EMBLAZE VCON

Videoconferencing Systems

Video Made Easy

Media Xchange Manager®

Version 4.5

Administrator's Guide

DOC01094 Rev. 12.0 07.06

Limited Warranty

Emblaze-VCON Ltd. warrants that SOFTWARE will perform according to accompanying user documentation for a period of 90 (ninety) days from the date of receipt; replacement SOFTWARE will be warranted for 90 (ninety) days from the date of receipt. This Limited Warranty shall not apply to any product that in the opinion of Emblaze-VCON Ltd. has not been installed or upgraded according to accompanying documentation from Emblaze-VCON Ltd. or been subject to misuse, misapplication, negligence or accident while in the hands of the purchaser.

GRANT OF LICENSE Emblaze-VCON Ltd. grants the Purchaser a non-exclusive and non-transferable license to use the SOFTWARE product and to make one copy solely for backup or archival purposes, which may include user documentation provided via online or other electronic form. Additional copies may not be made nor may anyone else be allowed to copy or otherwise reproduce any part of the licensed software without prior written consent of Emblaze-VCON Ltd.

About this Administrator's Guide

This Administrator Guide explains how to work with the Emblaze-VCON Media Xchange Manager (MXM) system. The following chapter summary briefly describes this guide's contents:

Emblaze-VCON Technical Support

This Administrator's Guide was designed to help you set up and work with your MXM easily so that you can enjoy its many features.

If a situation occurs that is not covered by the supplied documentation, contact your local Emblaze-VCON distributor, and request assistance from their Emblaze-VCON-trained technical support department. Please describe the problem, device, and PC operating system (if applicable), and any other relevant details.

Also, you may access the Technical Support section of the Emblaze-VCON website (http://www.emblaze-vcon.com/support/index.shtml) in order to check its knowledge base or initiate other customer support processes:

Page	Type of support
Support Notes	Troubleshoot or receive technical information about specific Emblaze-VCON products.
Downloads	Download a new software release or a free product evaluation.
Demo Numbers	Test your videoconferencing system.
License Key Requests	Request a permanent license key for your organization's MXM(s).

TABLE OF CONTENTS

1 WELCOME TO MEDIA XCHANGE MANAGER®

Congratulations on your entry into the revolutionary world of Emblaze-VCON's Media Xchange Manager® (MXM). The MXM centralizes the management of Video over IP communication within an enterprise-wide network.

1.1 About the MXM Server

The MXM provides centralized videoconferencing management services for corporate networks running on IP. It transfers many adminstration and configuration tasks from the individual computers, called *end points*, to the network, where they belong.

The MXM provides the following services:

- ❑ H.323 Revision 4-compliant Gatekeeper functions, including login and security:
  - — Auto-discovery and registration of nodes, such as videoconferencing end points, gateways, MCUs and their respective services.
  - — Address translation of IP addresses, H.323 aliases, E.164 numbers, e-mail addresses and URLs.
- ❑ Call Forwarding, Pickup, Transfer, Ad-hoc Conferencing and Hunting Groups
- ❑ Search capabilities for nodes in zones managed by other MXMs and gatekeepers
- ❑ Simplified gateway and MCU dialing for registered end points
- ❑ Control of the usage of gateway and MCU services by registered users
- ❑ Bandwidth management for allocating available bandwidth to registered nodes
- ❑ Compatibility with external online directory services (LDAP)
- ❑ IP-Nexus messaging and chat
- ❑ Network usage reports (Call Details Records and Asset Management Reports) - optional
- ❑ Integrated Videoconferencing Bridge (VCB5/VCB 2500) - optional.
- ❑ Integration with Emblaze VCON secure conferencing solutions (Frontier, ALG Proxy)

1.2 About the MXM Administrator

The Administrator application provides an interface for performing the management and monitoring of the MXM network. It may be installed on the same computer as the MXM Server as well as on additional computers, therefore providing remote management capability.

The Administrator application enables:

- ❑ Remote configuration and management of Emblaze-VCON HD, vPoint, MeetingPoint, Falcon, and VCB nodes
- ❑ Registration, configuration and management of H.323 end points, such as Emblaze-VCON's and other vendors' H.323 videoconferencing systems
- ❑ Registration, configuration and management of SIP User Agents, such as SIP phones and Windows XP Messenger applications.
- ❑ Registration, configuration and management of Gateways, MCUs and their respective services
- ❑ Configuration of videoconferencing policies between the local MXM and zones of nodes managed by other MXMs and gatekeepers
- ❑ Monitoring of connection states, login status, and events logging
- ❑ Creation of hunting groups (groups of end points that may be called through one common number)
- ❑ Creation of administrative groups that reflect the organization's corporate structure and enables efficient configuration of these groups' stations
- ❑ Setting limits on the permitted bandwidth usage
- ❑ Initiation and hangup of point-to-point calls between two end points
- ❑ Utility for upgrading the videoconferencing software of registered end points
- ❑ Testing for Least Cost Routing of gateway calls.

1.3 Glossary of MXM Terms

This section lists special MXM terms that are commonly used in this guide.

Ad-hoc conference	A videoconference that expands from a point-to-point session to a multipoint session while it remains open. Additional end points are "invited" by one of the parties.
Administrator	User whose responsibilities may include monitoring and managing the MXM network. Three levels of Administrator provide various rights for managing, controlling, monitoring, and viewing information.
Bandwidth Group	A group of nodes who belong within a specified IP address range, or who have been added manually, who have the same administrator-defined bandwidth usage policies.
End point	An H.323 terminal, Gateway, or MCU. An end point can call and be called. It generates and/or terminates information streams.
Firewall	A means of providing a network security from intruders. Firewalls may employ a single router or a combination of routers and servers that perform firewall processing of incoming and outgoing traffic.
Gatekeeper	Application that controls registration (login) into a computer or network, translates addresses, and manages bandwidth within a network.
Gateway	A network device that enables communication between two different types of networks, such as IP and ISDN telephony.
Hunting group	A group of users within an organization that may be reached through one common number.
LDAP	Lightweight Directory Access Protocol - used to access online directory servers, for registering and searching for other online users.
Login	The process of gaining entry, or registering, into a computer or a network.
MCU	Multipoint Control Unit - a device used to connect three or more end points in a single video meeting.
MXM Node	A node that is registered in the local MXM.
NAT	Network Address Translation - An IETF standard that allows an organization to present itself to the Internet with one address.

Neighbor Node	A node that is registered in a neighboring zone.
Neighboring Zone	A zone that is known and listed in the local MXM.
Node	A device on a LAN. For example, end points, gateways and MCUs are nodes.
Service	A configuration for the allocation of available bandwidth during videoconferences through gateways or MCUs.
Template	A complete set of default properties for new nodes.
Zone	A collection of nodes that MXMs and gatekeepers register and manage.

2 GETTING STARTED

2.1 Minimum System Requirements

The components of the MXM may be installed and operated on any computer that meets the following minimum requirements:

MXM Server

For optimum performance, install the MXM Server on a workstation or server that contains only the Windows 2003 or Windows 2000 operating system with Service Pack 4 or higher. We recommend that no other applications except MXM Administrator, Emblaze-VCON VCB, Conference Moderator or IP-Nexus be installed on it at any time. The presence of other applications (even if they are not open) may cause unpredictable operating results.

1. No other application may use the computer's default H.323 TCP/IP ports.
2. MXM installation program installs MDAC 2.8, which upgrades the ODBC driver, and MSDE 2000 with Service Pack 3a.

Basic Version

Operating System	Microsoft Windows 2003 or 2000 Server with Service Pack 4 or higher
Minimum CPU Speed	1 GHz
Recommended Memory	at least 512 MB
Minimum Free Disk Space	200 MB

With 2 VCB Session Support

Operating System	Microsoft Windows 2003 or 2000 Server with Service Pack 4 or higher
Minimum CPU Speed	2.4 GHz
Recommended Memory	at least 512 MB
Minimum Free Disk Space	300 MB

MXM Administrator Application

The MXM Administrator application may be installed on any workstation(s) on the network that meet the following specifications:

Operating System	Microsoft Windows 2003/98/XP/2000/NT 4.0 with Service Pack 5 or higher.
Minimum CPU Speed	166 MHz
Minimum Memory	64 MB
Minimum Free Disk Space	10 MB

Conference Moderator

The Conference Moderator must be installed on the same computer as the MXM Server.

Operating System	Microsoft Windows 2003 or 2000 Server with Service Pack 4 or higher.
Minimum CPU Speed	2.4 GHz
Minimum Memory	512 MB
Minimum Free Disk Space	300 MB
Already installed on same computer	MXM 4.2 or higher. Microsoft IIS 5.0 or higher. Internet Explorer 6.0 or higher.

2.2 Installing the MXM Server

The MXM server must be installed on a Windows 2003 or 2000 Server dedicated to the management of your organization's videoconferencing network.

➤ To install the MXM Server

1. Insert the MXM Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.

   Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file. The Installation program appears.
3. Select **MXM Server**.
4. Follow the instructions in the Setup Wizard, clicking **Next** to continue. The installation program installs the Server components.

If upgrading from a previous MXM version, the Installation program detects it. Click **OK** to continue. The Installation program saves the previous version's database settings, except for Call Details Records (CDRs) and the Event Log.

5. The Wizard asks where to install and use Microsoft SQL database. To install it on the same computer as the MXM (default setting), click **Next**. To install it on a different computer, click **Choose Location** and then enter the appropriate computer name or IP address.

   The installation program builds a system database, which requires a few minutes.
6. At another stage, the Enter Serial Number dialog box appears. Type the serial number that's on the supplied key code agreement and click **OK**.

   If you received a version for evaluation, click **Cancel**. To continue installing the evaluation version (limited no. of users for a short period), click **Yes** to confirm.

Whether this is a first-time installation or an upgrade, your initial key code is valid for 30 days. For instructions on making it permanent or increasing the permitted number of registered end points, see "Replacing the MXM License Key" on page 11.

7. When the Wizard informs that the installation is complete, click **Finish**.
8. To install the MXM Administrator application on the same computer, keep the Installation program open (see the next section).

   To exit the Installation program, click **Exit**.

2.3 Installing the MXM Administrator

The Administrator application may be installed on the same computer as the MXM Server and/or other workstations from which you may perform remote administration.

The new version of the MXM Administrator may be installed over a previous version of the application. You do not need to uninstall the previous version.

➤ To install the MXM Administrator

1. Insert the MXM Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Setup wizard will appear automatically.

   Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file. The Setup wizard appears.
3. Select **MXM Administrator**.
4. Follow the instructions in the wizard, clicking **Next** to continue.
5. The wizard provides a checkbox for installing the HD Upgrade Utility, which provides you with the ability to upgrade the software version of Emblaze-VCON HD3000/2000/1000/600 connected to your organization's network. If your organization has any of the above systems, we recommend that you install this application.

   Click **Next** to continue.
6. If you selected to install the HD Upgrade Utility, the wizard proceeds to its installation process. Follow the instructions in the wizard, clicking **Next** to continue to the next page.
7. When the Wizard informs that the installation is complete, click **Finish**.
8. To exit the Installation program, click **Exit**.

2.4 Installing Conference Moderator

The following procedure applies to Conference Moderator installations on computers that do not have a VCB5 set up on them (VCB5 includes a Conference Moderator application).

Microsoft® IIS 5.0 or higher must be already installed on the Server. To use the Web Sharing, the IIS must include its FTP Server.

Setup Parameters

Before installing Conference Moderator, set up the following (if not applicable to your organization, skip these instructions):

- ❑ If Microsoft Outlook® is your organization's e-mail application, install a Custom Installation of Outlook and include the following elements:
  - — **Collaboration Data Objects**
  - — **Electronic Forms Designer Runtime**
- ❑ If the server's operating system is Windows Server 2003, start *ASP.NET* manually.
  1. Right-click **My Computer** and choose **Manage**. Browse to *Services and Applications\Internet Information Services (IIS) Manager\Web Service Extensions*.
  2. In the right pane, select **ASP.NET [***version number***]** and choose **Allow** from the popup menu.

Running the Conference Moderator Installation Program

Conference Moderator must be installed on the same computer as the MXM Server.

➤ To install the Conference Moderator

1. Insert the MXM Setup CD-ROM in your computer's CD-ROM drive.
2. Click **Start** in the Windows taskbar and then click **Run**. Browse to the [CD-ROM drive]>*Moderator*>*Setup.exe* file. The Setup wizard appears.
3. Follow the instructions in the wizard, clicking **Next** to continue.
4. The Wizard asks for the location of the MXM SQL database. You may use a database installed on the same computer or click **Choose Location** and enter a different computer name or IP address. Click **Next** to continue.
5. When the Wizard informs that the installation is complete, click **Finish**.

Additional Configuration Issues

- ❑ In all Conference Moderator clients, enable the use of Active X controls and plug-ins. In Internet Explorer, enter the **Security** tab of the **Internet Options**, click **Custom Level**, and set all Active X settings to **Enable**.
- ❑ If Emblaze-VCON's Reporting Option is already installed, run its Restore program to restore its default configuration (the installation of Conference Moderator causes complications to the Reporting Option). The Restore program is located at *Program Files\VCON\Moderator\Setup\RestoreCtrlClient.exe*.
- ❑ To work with WebEx Data Sharing, enter the Conference Moderator's System>Data Sharing page and enter the following login details:
  - — URL of your organization's WebEx account
  - — User name
  - — Password

2.5 Replacing the MXM License Key

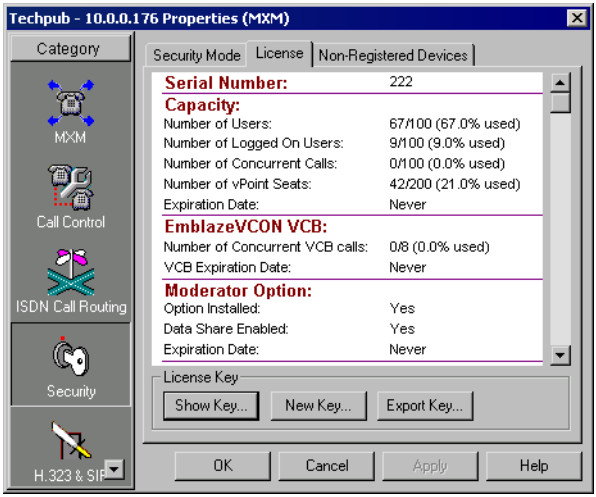
The following circumstances require replacement of your MXM license key:

- ❑ Replacing a temporary demo version with a permanent, purchased version. Your initial key code is valid for 30 days.
- ❑ Changing the number of permitted registered end points.
- ❑ Adding optional features to your MXM.

This process requires that an initial MXM is already set up. For instructions on setting up an MXM, see Chapters 4 and 5.

➤ To replace your MXM's license key

1. In the Administrator window, click the MXM entry or any of its managed objects.
2. In the *MXM* menu, choose *Show License Page*.
3. In the Properties dialog box's **License** tab, click **Export Key** to create a license file for the MXM on the host computer.



MXM System License Properties

4. Send the license file to your local Emblaze-VCON distributor. You will then receive a new key code from the distributor.
5. Save the new license code file to a location on your network.

6 After receiving a new license file from your Emblaze-VCON distributor, run the MXM Administrator application. Enter the MXM Properties **License** tab again.

7 Click **New Key**. The Open dialog box appears.

8 Browse to the location where you saved the license code file. Click **Open**.

9 When prompted to apply the license code, click **OK**.

10 To implement the license change and close the dialog box, click **OK** again.

2.6 Running the MXM

The MXM server opens automatically during the host computer's startup, and runs unseen as a service application.

➤ To run the MXM Administrator

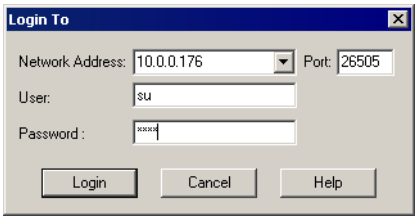
❑ In the Windows desktop, click **Start**, point to **Programs** and click **MXM Administrator**.

Starting the MXM Administrator

When you open the MXM Administrator application for the first time, you must open a new MXM object in the Main View.

➤ To open a new MXM

1 In the **MXM** menu, click **Log in to New MXM**.



Opening a New MXM

2 Enter the IP network address of the computer that it's installed on. Then, enter the default User name and default password during the startup. Afterwards, you may change these values to meet your own operating needs (see "Adding an Administrator" on page 25).

Default user	su
Default password	1234

3 Click **Login**. The new MXM is displayed in the Main View of the Administrator application. You can expand the MXM to see an initial system tree (see Chapter 3, "A Quick Tour of the MXM Administrator," for more details).

4 To save the administrator application configuration, open the **File** menu and click **Save As**. Save the configuration as a *.vca* file.

2.7 Basic MXM Operations

This section will list the various tasks required to set up the MXM for a typical video network. At the end of each description, the location of detailed explanations are provided.

1. Set up administrators.

   Enter the administrators and their various privileges into the system. The available privilege levels are Super User, Monitor System and View System Properties. See "Setting Up Administrators" on page 25.

2. Set up the MXM's configuration.

   Define the various properties of the system's configuration, such as connection details, open or closed mode for registering end points, and so on. See Chapter 5, "Setting MXM System Properties."

3. Define default settings for end points and other nodes in templates.

   A template includes the characteristic properties for a type of node or service. Any new created item in the system will initially have the default properties defined in the template. See "Setting Up Templates" on page 47.

4. Set up end point configurations.

   End points may be registered with the default properies defined in a template or be set following their login requests. See Chapter 6, "Defining End Point Nodes."

5. Create and set up bandwidth groups.

   Bandwidth groups enable administrators to control usage of bandwidth among a select group of nodes who belong within a specified IP address range. This feature makes it easier for administrators to organize the allocation of bandwidth limits throughout a whole organization. See "Bandwidth Groups" on page 49.

6. Create and set up hunting groups.

   A hunting group includes a series of nodes that may be grouped together within an organization for a variety of reasons, but may be reached through one common address. See "Adding Hunting Groups" on page 53.

7. Create and set up administrative groups.

   Administrative Groups of nodes in the Main View can help maintain a visual structure for nodes and the teams and departments to which they belong. This also makes it easier to control end point properties that need to be common within a team or department, such as limiting the available bandwidth for the group. See "Adding an Administrative Group" on page 59.

8. Set up a videoconferencing software upgrade process that includes all or most of the end points registered to the MXM (available for Emblaze-VCON vPoint, VCB and the MXM Administrator application).

   The software upgrade process enables you to place a new software version on a server location and then either schedule an upgrade time or run the upgrade program immediately for all the relevant end points. In this way, you can make sure that all end points (of specific models) in the organization are using the same and/or latest software. See Chapter 8, "Remote Upgrade of Videoconferencing Devices Software."

9. Prepare the MXM to provide gateway dialing services to ISDN connections for the registered end points.

   If gateways register with the MXM, you must set their MXM configurations and their services' configurations in the Administrator application. Then, you may define least-cost-gateway-dialing rules in order to reduce your organization's call costs. See Chapter 9, "Registering Gateways" and Chapter 10, "Least Cost Routing of Gateway Calls."

10. Set up the MXM configurations for Multipoint Control Units (MCU) that register with the MXM.

    MCUs are used for connecting registered end points with a number of other end points in a multipoint videoconference. MCU services are available after the particular MCU is granted login permission to the MXM. See Chapter 11, "Registering an MCU."

    Emblaze-VCON VCB provides multipoint conferencing and the expansion of point-to-point IP videoconferences into ad-hoc multipoint videoconferences. Set up the VCB services configurations, define VCB/MCU services for use in ad-hoc sessions, and control the use of ad-hoc session resources by creating ad-hoc service permission groups and associating end points to them. See Chapter 12, "Setting Up Multipoint Conferences Managed by a VCB."

11. If your network includes an Accord® MGC™, set up its configurations to provide gateway and MCU services to your MXM's end points.

    The MGC operates under a different configuration model than most other MCUs being used in the videoconferencing sector. For detailed instructions on setting up your MGC/MXM configurations, see Chapter 13, "Using Polycom® MGC™ with the MXM."

12 If your organization has more than one network of videoconferencing users, set up the MXM configurations for additional zones managed by other MXMs or gatekeepers on your MXM Administrator application.

The configuration of additional zones enables end points registered in the local MXM to engage in videoconferences with end points in these other zones. You can set bandwidth allocation, enable inter-zone Call Details Records (CDR) generation, and other inter-zone videoconferencing management policies. See Chapter 14, "Neighboring Zones."

13 Set up the MXM's configuration in an Lightweight Directory Access Protocol (LDAP) online directory server.

By listing MXM registered users in an LDAP server, they will be able to locate and call all other users listed in the same directory. The MXM supports several LDAP server applications. See Chapter 15, "Registering with LDAP Directories."

14 If your organization includes Session Initiation Protocol (SIP) User Agents, set up their configurations and manage communications among them and between registered H.323 end points.

The MXM provides similar services to SIP and H.323 systems. Administrators can initiate calls between two SIP user agents and between a SIP user agent and an H.323 end point. The MXM provides gateway-like services when connecting calls between H.323 and SIP networks. See Chapter 16, "Managing SIP Networks."

15 Set up a Cluster configuration to avoid interruptions of conferencing services resulting from temporary server problems.

A Cluster configuration provides continuity of conferencing services in case an MXM server goes down. The Emblaze-VCON Cluster application eliminates the downtime that occurs during server hardware and software interruptions. See Chapter 17, "Emblaze-VCON Cluster Module."

3 A Quick Tour of the MXM Administrator

Your work with the MXM takes place inside the Administrator application, which provides several elements and tools for performing the system management tasks.

In addition, the Administrator application provides various views and tables:

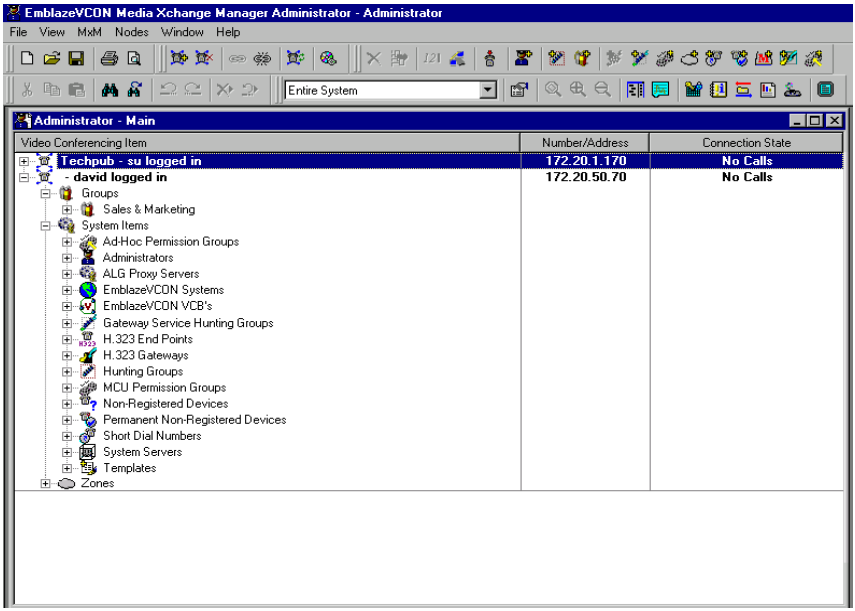
Main View	Displays a connected MXM and its registered nodes, hunting groups, and templates. From this window, you can view status, monitor activity, and configure properties of these registered users.
Node Status	Displays connection information about specific nodes that you want to monitor.
Login Status	Displays nodes that tried to register but were denied login - you can monitor registration and login procedures for nodes.
Event Log	Displays information about system events and operating conditions.
LDAP Servers	Displays information about the various online directories in which this MXM lists its registered nodes.
Frontier Server	Contains data about associated Frontier Servers. To enable registered end points to register and connect to a Frontier Server, you must first list the Server's details in the Frontier Server View

3.1 The Main View

Information about MXMs and their managed objects appears in the Main View. These include:

- Connected MXMs
- Administrators and their privileges
- Registered nodes and services, including user numbers and addresses, connection and call status
- Neighboring MXMs and Gatekeeper zones
- Software version indication for Emblaze-VCON vPoint end points and VCB nodes.

In addition to displaying an MXM's entire local and neighboring zones, viewing filters are available for showing smaller subsets of the registered nodes.



The Administrator Application Main View

Connected MXMs

An Administrator may log in multiple MXMs. Each logged-in MXM is represented in the Main View by an entry that has an expandable system tree. When this tree is expanded, you can view nodes (such as Emblaze-VCON users, gateways, MCUs, and other administrators) that have logged in to that particular MXM. In addition, associated hunting groups, templates, and neighboring zones are shown in the system tree.

The system tree also shows units that tried to register but were not accepted automatically. In these cases, you have to grant login permission and set up the units' MXM properties.

For each MXM, the Administrator application stores property information such as name/address, login settings, and various network settings (connection, timeouts, bandwidth management, etc.). For more information, see Chapter 5, "Setting MXM System Properties".

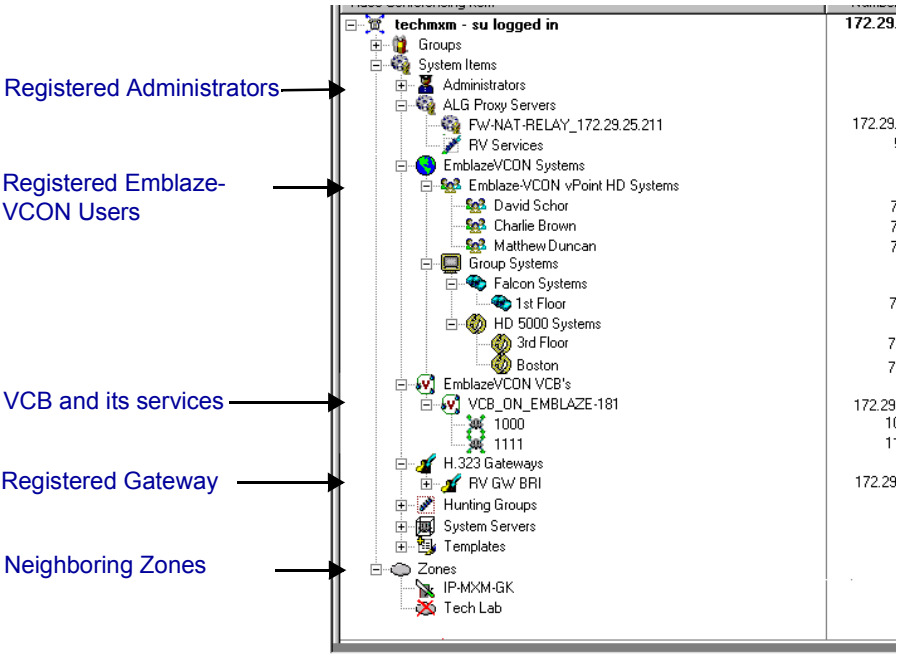
Registered Nodes

The MXM supports the registration of Emblaze-VCON and other H.323 end points, administrators, gatekeepers, gateways, MCUs, gateway services and MCU services. In this Administrator's Guide, registered nodes are also referred to as *MXM nodes*.

These nodes are visible when the system tree is expanded. For each of these items, the Administrator application stores property information such as name/address, bandwidth limits, online directory (LDAP) registration, and more.

Emblaze-VCON Group Systems with ISDN support

These are represented in the Main View by icons (for HD5000, for Falcon, for MediaConnect 9000) that display the status of the ISDN connections. Green indicates that the ISDN line is connected. Red indicates that the line is not connected.



Typical Main View

Displaying Call Status in the Main View

Neighboring MXMs and Gatekeeper Zones

If the local MXM is set to Open Mode for listing other MXMs and gatekeepers from the connected network, the MXM lists them in the Main View after it detects them. You can then set up the configurations for handling calls between each zone and the local MXM.

Nodes from a known neighboring zone may also be listed under their associated zone objects. In this way, neighboring nodes will be available for tasks such as call initiation and bandwidth management.

For more information about setting up and working with zones, see Chapter 14, "Neighboring Zones."

Software Upgrade Indication

The MXM Administrator application provides the ability to update software for registered vPoint end points, Video Conference Bridge (VCB) end points, or the MXM Administrator itself.

After an upgrade operation has been set up, an icon next to the relevant nodes indicates if they require upgrade to the latest available version. After successful installation of the latest version, the icon disappears.

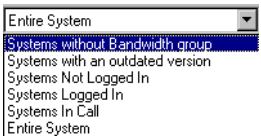
Filtering the Main View

You can control the amount of information that appears in the Main View by selecting filters according to the details that are important to you. You can set filtering according to the following criteria:

- Entire System
- Systems Not Logged In
- Systems Logged In
- Systems In Call
- Systems with an outdated (software) version

➤ To filter the main view

❑ In the Main View toolbar, open the Filter list and choose one of the options.



Main View Display Filters

3.2 The Node Status View

The Node Status View makes it easier to see the connection information only about specific nodes instead of viewing the entire system tree. You can monitor the following:

- End points
- Administrator nodes
- Gateways and services
- MCUs and services
- Neighboring zones
- Gatekeeper
- LDAP proxy
- SIP proxy.

Right-click the Node Name of the entry to open a shortcut menu that contains commands that relate to the selected item.

	Node Description	Node Number	Status	Connection State	Bandwidth (kbps)	Audio Codec	Video Codec	Video Codec2
	David3000	1060		Logged In	2*361	---	---	---
	Call #1			Talking to 1016	2*361	G.722 64k	H.263 QCIF	
	David Schor	1016		Talking to 1060	2*360	G.722 64k	H.263 CIF	
	DemoVP1	2101		Logged in to Management...	---	---	---	---
	Matthew D..	1002		Logged In	---	---	---	---
	Charlie Br..	1029		Logged In	---	---	---	---

Node Status Table

3.3 The Login Status View

The Login Status View lists nodes that tried to register, but were not given login and registration permission. This table makes it easier to monitor registration and login procedures for specific nodes instead of viewing the entire system tree.

Administrator:2 - (172.20.10.205) - Login Status

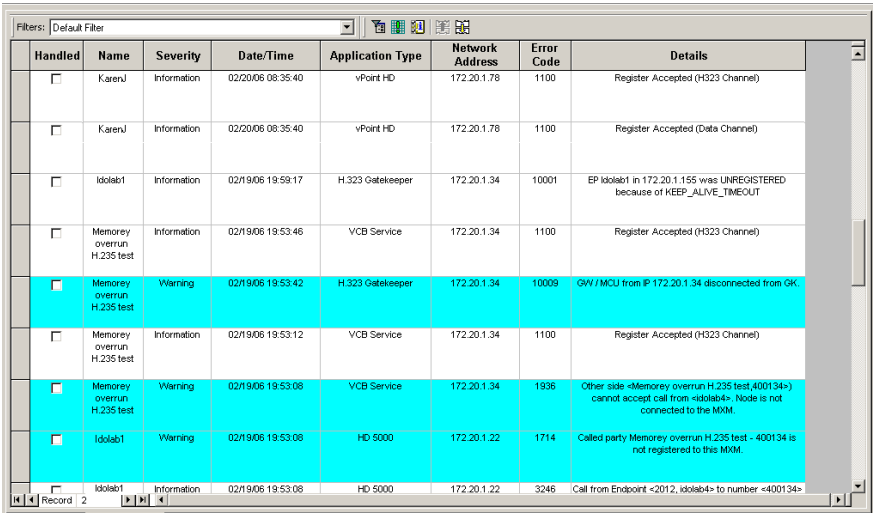
Login Category	Network Address	Alias	Login Name	Login Status
vPoint HD	172.20.10.21	davids	davids	Login Permission Requested

Login Status View

3.4 The Event Log

The Event Log displays information about system events and operating conditions. You can refer to it for troubleshooting and isolating a problem.

The following illustration shows all the types of information (according to column) that the Event Log provides. If you want to display only a few important details, you can define filters that reduce the amount of displayed records according to various criteria.



Filters: Default Filter

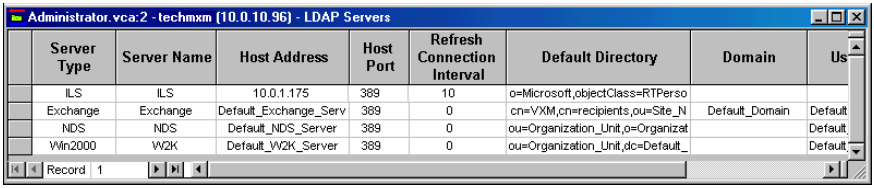
Handled	Name	Severity	Date/Time	Application Type	Network Address	Error Code	Details
☐	KarenJ	Information	02/20/06 08:35:40	vPoint HD	172.20.1.78	1100	Register Accepted (H323 Channel)
☐	KarenJ	Information	02/20/06 08:35:40	vPoint HD	172.20.1.78	1100	Register Accepted (Data Channel)
☐	Idolab1	Information	02/19/06 19:59:17	H.323 Gatekeeper	172.20.1.34	10001	EP Idolab1 in 172.20.1.155 was UNREGISTERED because of KEEP_ALIVE_TIMEOUT
☐	Memorey overrun H.235 test	Information	02/19/06 19:53:46	VCB Service	172.20.1.34	1100	Register Accepted (H323 Channel)
☐	Memorey overrun H.235 test	Warning	02/19/06 19:53:42	H.323 Gatekeeper	172.20.1.34	10009	GW / MCU from IP 172.20.1.34 disconnected from GK.
☐	Memorey overrun H.235 test	Information	02/19/06 19:53:12	VCB Service	172.20.1.34	1100	Register Accepted (H323 Channel)
☐	Memorey overrun H.235 test	Warning	02/19/06 19:53:08	VCB Service	172.20.1.34	1936	Other side <Memorey overrun H.235 test,400134>) cannot accept call from <idolab4>. Node is not connected to the MXM.
☐	Idolab1	Warning	02/19/06 19:53:08	HD 5000	172.20.1.22	1714	Called party Memorey overrun H.235 test - 400134 is not registered to this MXM.
☐	Idolab1	Information	02/19/06 19:53:08	HD 5000	172.20.1.22	3246	Call from Endpoint <2012, Idolab4> to number <400134>

Record 2

Event Log

3.5 LDAP Servers

The LDAP Servers View provides information about the MXM's connection and registration in an LDAP (Lightweight Directory Access Protocol) online directory. The administrator may list the MXM and its registered nodes in any one of these online directories.



Administrator.vca:2 - techmxm (10.0.10.96) - LDAP Servers

Server Type	Server Name	Host Address	Host Port	Refresh Connection Interval	Default Directory	Domain	Us
ILS	ILS	10.0.1.175	389	10	o=Microsoft,objectClass=RTPerso		
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=VXM,cn=recipients,ou=Site_N	Default_Domain	Default
NDS	NDS	Default_NDS_Server	389	0	ou=Organization_Unit,o=Organizat		Default
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default

Record 1

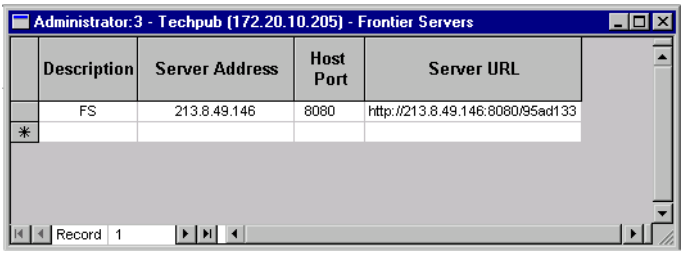
LDAP Servers View

3.6 The Frontier Server View

Emblaze-VCON's Frontier Server allows your organization's personnel to engage in videoconferences, yet still maintain your required level of security. The Frontier Server applies secure firewall traversal, network address translation and encryption. To enable registered end points to register and connect to a Frontier Server, you must first list the Server's details in the Frontier Server View.

➤ To add Frontier Server details

1 In the **View** menu, point to **Views** and click **Frontier Servers**. The Frontier Servers View opens.



Frontier Servers View

2 In the table, enter the following information:

Description Name for the Frontier Server - it may be its alias or any other arbitrary name.

Server Address IP address of the Frontier Server.

Host Port Port used for communicating with the Frontier Server unit configuration management.

Server URL The web page of the Frontier Server's User List, where the addition and deletion of nodes to the Server's database takes place.

After being added to this table, this Server is available for selection in the vPoint HD and HD5000 **Network>LAN** Properties.

4 MANAGING THE MXM

This chapter provides instructions for organizing your MXM Administrator system so that you can manage your organization's videoconferencing network. The tasks include:

- Setting Up Administrators
- Editing Nodes
- Status Monitoring
- Setting Up Templates
- Bandwidth Groups
- Adding Hunting Groups
- Adding an Administrative Group
- Adding a Short Dial Number

4.1 Setting Up Administrators

Adding an Administrator

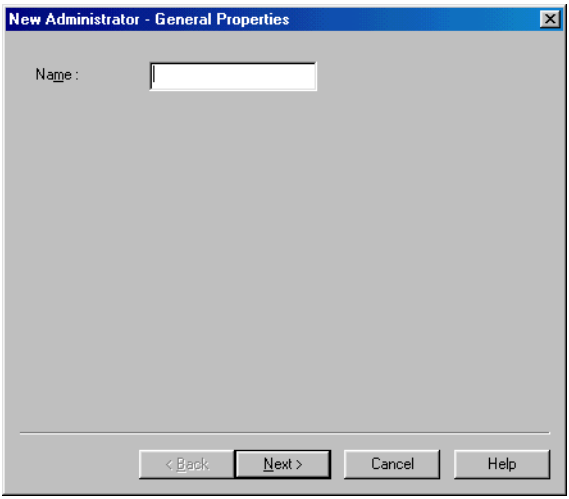
At any time, you can register additional administrators to the MXM. Each administrator must have an administration level (privileges) and a password.

In addition, you can change the privileges and other properties of the registered administrators at any time.

➤ To add an Administrator

1 Click the **New Administrator** button. The New Administrator Properties dialog box appears.

2 Type the Administrator's **Name**. Click **Next**.



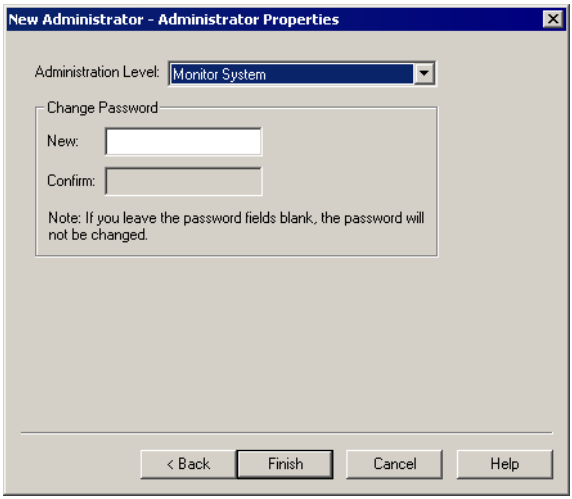
New Administrator - General

3 Enter the following privileges and security information:

Administration Level Defines the level of activity allowed for the selected Administrator. The available options are:

- **Monitor System** - The Administrator may only observe the Main View and the Node Status View, and initiate videoconferences between known end points.
- **View System Properties** - The Administrator may only observe the Main View, the Node Status View, view other nodes' properties, and initiate videoconferences between known end points.
- **Super User** - The Super User may change node and system configurations, in addition to the activities allowed for the other options.

Change Password In the **New** box, type a new password for the new Administrator. In the **Confirm** box, type the new password again.



New Administrator - Administrator Properties

4 Click **Finish** to complete the setup. A new administrator appears in the Main View under the **Administrator** icon.

Changing Administrator Properties

If necessary, you may change the properties of existing administrators.

➤ To change an administrator node's properties

1 In the Main View, expand the Administrator group to view a list of Administrators.

2 Double-click an Administrator to open the Properties dialog box.

3 Change the appropriate properties. For a description of them, see "Adding an Administrator" on page 25.

4 Click **OK** to complete the change. If you want to discard the change, click **Cancel**.

4.2 Editing Nodes

Adding Nodes

After a node connects to the MXM, it is added to the MXM's database. The MXM may automatically accept the registration attempt, require manual registration by the administrator, or reject the attempt.

Granting Login Permission

To receive login requests, the MXM may be in Open Mode for certain types of nodes, and/or in Closed Mode for all other nodes.

Open Mode

Emblaze-VCON end points allows automatic login to all Emblaze-VCON end points that register with the MXM (Escort, Cruiser 150/384, ViGO, MediaConnect 6000/8000, Falcon, VCON Conference Bridge).

Non-Emblaze-VCON end points allows automatic login to any non-Emblaze-VCON H.323 videoconferencing end point that registers.

MCUs allows automatic login to any MCU that registers.

Neighboring Gatekeepers (Zones) allows the MXM to list any neighboring zones management device (MXM or gatekeeper) that contacts it (see Chapter 14, "Neighboring Zones.").

SIP User Agents allows automatic login to any SIP end point that registers.

Closed Mode

The administrator can manually grant login permission to nodes or reject them by ignoring their requests.

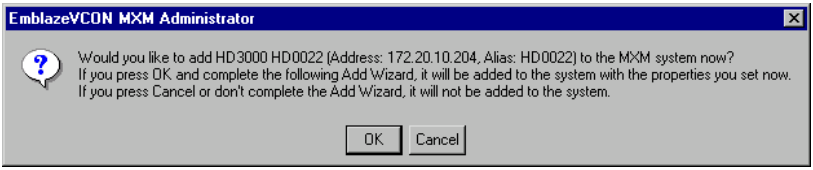
For nodes registering in Closed Mode (or nodes that cannot be registered automatically, such as gateways), a Login Request entry appears on the system tree in the Main View.

Login Request Indication

➤ To grant login permission

1. Expand the Login Request item.
2. Right-click the item name and then click **Grant Login Permission**.

   A message appears, asking if you want to register the node now.



Node Registration Request

3. Click **OK** if you want to manually set the node's properties, such as directory number or call forwarding. The Add Wizard appears (for definitions of the node properties, see "Setting End Point MXM Properties" on page 91). The original property values are the default values defined in the node type template (see "Setting Up Templates" on page 47).

   If you click **Cancel**, the node will not log in, but remains under the Login Requests object until you delete it (and the node stops trying to log in). See the next section, "Deleting a Login Request".

4. Change properties according to your specifications, or keep the default settings. When you finish each page of the wizard, click **Next**.
5. When you finish the last page, click **Finish**.

   The node is registered. It appears as an entry in an appropriately labelled location of the system tree.

If the registering node is an Emblaze-VCON Personal system (MeetingPoint 4.5 or higher) or vPoint system, the login process does not continue automatically after you click **Finish**. Instruct the node to log in again (user must click **Connect**) in order to complete the registration.

Deleting a Login Request

You may choose to reject any login requests that require you to grant permission manually.

➤ To delete a login request

❑ Right-click the Login Request item and then click **Delete Login Request**. Click **Yes** to confirm.

If the node continues trying to register, ask the user to try logging in to another gatekeeper or to operate stand-alone.

Setting a Node's Properties

The MXM and all of its registered nodes have definable properties, or characteristics, which define their functionality and operation. Setting up and maintaining these properties is the key to efficient videoconferencing network management. At any time, an Administrator with Super User privileges can change properties of a registered node.

In addition, the videoconferencing configurations of vPoint HD, vPoint, HD2000/3000/4000/5000, MeetingPoint 4.5 (and higher), and Falcon end points may also be edited. See the appropriate appendix for the product you need to configure. For MeetingPoint and Falcon end point properties configuration, see *MeetingPoint® End Point Properties* or *Falcon™ End Point Properties* from the MXM CD-ROM or the Documentation>Manuals page of the Emblaze-VCON website.

➤ To set a node's properties

1. In the Main View, browse the system tree until you find the node that you want to edit. If necessary, click a category's plus sign to expand the tree and display additional items.
2. Right-click the node, point to **Property**, and then click the specific property type. The node's Properties dialog box opens to the property type that you clicked.

   -or-

   Double-click the node. The node's Properties dialog box opens to the **General** tab.

3 Change any appropriate properties.

If you want to continue to another property group, click that group's tab. In dialog boxes with many tabs, you may have to click the right or left arrow on the tab row to access all of them.

4 Click **OK** to implement all the changes and close the dialog box.

Finding Nodes and Objects in the Administrator

The Find and Find Next utilities help you search for specific items in the MXM Administrator. This feature is very useful if your enterprise's network is large and not all nodes are visible in the Administrator application window.

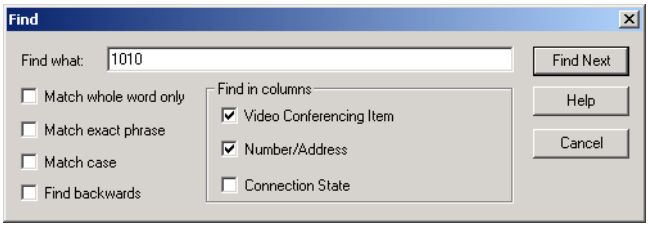
Find in Main View

In the Main View, you can search for any words, phrases or numbers in all of the columns.

➤ To find nodes and objects in the Main View

1 To search the whole system tree, click at the top of the Main View.

2 Click the Find button. The Find dialog box appears.



Find Dialog Box

3 In the **Find What** box, type a name and/or number.

4 If necessary, define additional search parameters:

Match whole word only — Select this option to match only complete words or phrases. For example, if you enter **Gate**, the search ignores the word, "Gateway".

If you want to find characters that may be part of a longer word or part of a phrase, deselect this option.

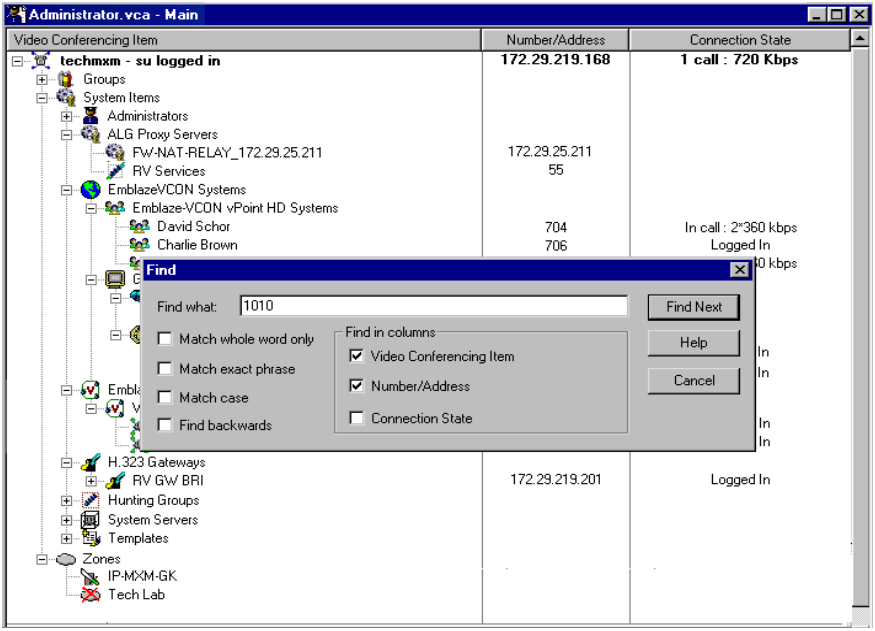
Match exact phrase — Select this option to match only complete phrases. For example, if you enter **Gateway Hunting Group**, the search ignores any items including only the word, "Gateway".

Match case — Select this option to match items whose capitalization is identical to the item in the **Find What** box. For example, if you enter **GW**, the search ignores any items that include “gw” or “Gw”.

To find all matching items, regardless of capitalization, deselect this option.

Find backwards — Select this option to search up the tree from the selected location. To select down the tree, deselect this option.

5 Click **Find Next**. The first matching item in the Main View is selected. To search for more matching items, click **Find Next** again.



Finding an Item in the Main View

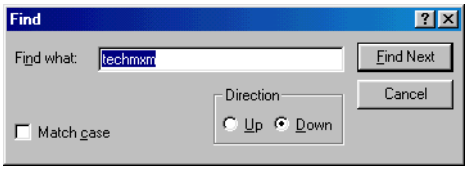
Find in Other Views

In the MXM Administrator application's other Views, you can search for the names of entries. The search covers the first column of the table.

➤ To find entries in other Views

1. Open the View in which you want to work.

2. Click the Find button. The Find dialog box appears.



Find Dialog Box

3. In the **Find What** box, type the name of the entry.
4. If necessary, define additional search parameters:

Match case — Select this option to match items whose capitalization is identical to the item in the **Find What** box. For example, if you enter **GW**, the search ignores any items that include "gw" or "Gw".

To find all matching items, regardless of capitalization, deselect this option.

Direction — Select the direction from the selected entry to search in the View, **Up** or **Down**.

5. Click **Find Next**. The first matching entry in the View is selected. To search for more matching entries, click **Find Next** again.

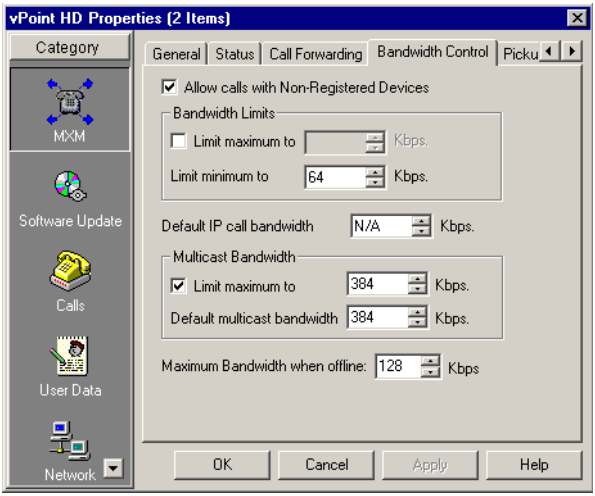
Editing Multiple Nodes

You can select more than one node at the same time and define certain properties with identical values. If the selection of nodes contains more than one node type, only the common properties among them may be changed. Other properties will be unavailable.

➤ To edit multiple nodes

1. Select the nodes that you want to change, using the standard Windows object selection techniques:
   - To select consecutive nodes, click the first node, press <Shift> and click the last node in the series that you want.
   - To select non-consecutive nodes, click the first node, hold down <Ctrl> and click all the other nodes that you want.
2. Right-click one of the selected nodes, and then click **Properties**.

   The Properties dialog box appears. Only common properties among the selected nodes are available for change.
3. Change the appropriate properties. Remember that this change affects all the selected nodes.
4. Click **OK** to complete the change.



Sample Properties Dialog Box - Multiple Nodes

Changing Directory Numbers

All end points, services, hunting groups, and other registered items are assigned an internal directory number (also called *E.164 number*). Any registered node can call another registered item simply by dialing the destination's directory number. This number is usually only a few digits, and can be adopted from the node's IP address, telephone extension number, or randomly.

The administrator may change the directory numbers of one or a range of several registered nodes.

➤ To change the directory number of a single node

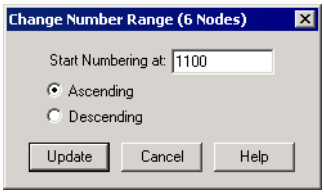
1. Double-click the node. The **General** tab of the node's Properties dialog box appears.
2. In the **Directory Number** box, type the new number. Press **OK**.

➤ To change a range of directory numbers

1. In the Administrator window, find the nodes whose numbers you want to change. If necessary, click a category's plus sign to expand the tree and display additional items.

   Select the relevant nodes.

2. In the toolbar, click the **Change Numbers** button. The Change Number Range dialog box appears. The title bar shows the number of nodes in the selected range.



Changing Node Numbering

3. In the **Start Numbering At** box, type the new number for the start of the range.

4 Select **Ascending** for the numbering range to go up from the number that you typed (for example, 60, 61, 62, 63, ...). This new assignment affects the numbers for all other selected nodes.

   Select **Descending** for the numbering range to go down from the number that you typed (for example, 63, 62, 61, 60, ...).

5 Click **Update** to implement the number change. On the Administrator tree, the new numbers for the selected nodes appear. From this point, a registered node must dial the new number to complete a call to the respective node.

Deleting a Node

If a node is not relevant to the network anymore, you can delete it from the MXM.

➤ **To delete a node**

❑ Click the node and then click the **Delete** button.

Click **Yes** to confirm.

4.3 Status Monitoring

The Administrator application provides a number of views for monitoring the operations of the MXM and its registered nodes:

- Main View
- Login Status View
- Node Status View
- Event Log.

Monitoring Nodes in the Main View

The Main View's Connection State column (right side of table) provides status information about the current activity of registered nodes. This column may display nodes' login status, or if nodes are currently in a videoconference and the amount of bandwidth being used.

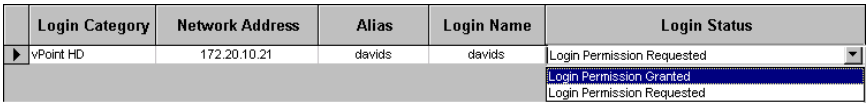
Indication of Nodes in a Videoconference

Viewing the Login Status

Use the Login Status View to monitor registration and login procedures for nodes. The table lists nodes that tried to register, but were not given login and registration permission. This table makes it easier to see the login information only about specific nodes instead of viewing the entire system tree.

➤ To open the Login Status table

❑ Click the **Login Status View** button.



Login Status View

The Login Status table provides the following information:

Login Category	The type of node that tried to register.
Network Address	Address of this node.
Alias	Name of this node.
Login Name	The node's user name, as entered during the login procedure. If the node cannot provide a user name to the MXM, this space remains blank.
Login Status	Describes what happened when the node last tried to log in to the MXM.

In the Login Status table, you can grant login permission by clicking the node's Login Status column and then selecting **Login Permission Granted** (see the preceding figure). The node login process continues (see "Adding Nodes" on page 28).

Viewing the Node Status

The Node Status View makes it easier to see the connection information only about specific nodes instead of the entire system tree. You can monitor the following:

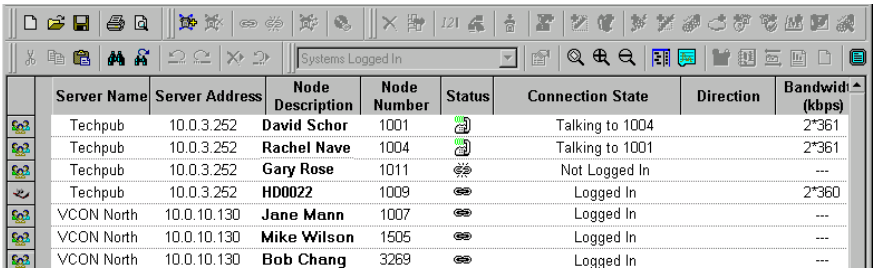
- End points
- Gateways
- MCUs
- VCBs
- Neighboring Zones

➤ To monitor nodes in the Node Status View

1. Click the **Node Status View** button. The Node Status View appears.
2. In the main Administrator window, select any number of nodes.
3. Drag the nodes into the Node Status View window. The information about the selected nodes appears in the table.

Node Description	Node Number	Status	Connection State	Direction	Bandwidth (kbps)	Audio Codec	Video Codec	T.120	MLP	HMLP	LSD
HD50003dFf	1011		In Call	Outgoing	384	G.728 16k (...	[in: H.261 Q...	Unkn...	6400	Off	Off
Line #1 (9507260)			Synchronized with 001512...		---	---	---				
Line #2 (9507260)			Synchronized with 001512...		---	---	---				
Line #3			Idle		---	---	---				
Line #4			Idle		---	---	---				
Line #5			Idle		---	---	---				
Line #6			Idle		---	---	---				
DavidSchor	1002		Talking to 2205		2*360	G.722 64k	H.263 CIF				
HD0022	2205		Talking to 1002		2*360	G.722 64k	H.263 CIF				
MC6000West	2802		Not Logged In		---	---	---				

Node Status Table



Server Name	Server Address	Node Description	Node Number	Status	Connection State	Direction	Bandwidth (kbps)
Techpub	10.0.3.252	David Schor	1001		Talking to 1004		2*361
Techpub	10.0.3.252	Rachel Nave	1004		Talking to 1001		2*361
Techpub	10.0.3.252	Gary Rose	1011		Not Logged In		---
Techpub	10.0.3.252	HD0022	1009		Logged In		2*360
VCON North	10.0.10.130	Jane Mann	1007		Logged In		---
VCON North	10.0.10.130	Mike Wilson	1505		Logged In		---
VCON North	10.0.10.130	Bob Chang	3269		Logged In		---

MXMs Displayed in Node Status Table

4. To go back to the Main Administrator View, click the **Administrator** tab at the bottom of the window.

Multiple Node Status Tables

You can make more than one Node Status Table to view different groups of nodes.

➤ To create a new Node Status table

1. At the bottom of the Node Status View, click the **Add New Tab** button.
2. Double-click the tab name.
3. Press the <Delete> key as many times as required until the default name is deleted.
4. Type a new tab name and press <Enter>.

➤ To delete a Node Status table

1. Click the tab of the table.

2. At the bottom of the Node Status View, click the **Remove Tab** button.

   The tab is deleted.

Node Status Table Information

The Node Status View provides the following information:

Server Name	Name of the MXM in which the node is registered. Applicable if more than one MXM is connected.
Server Address	IP address of the MXM in which the node is registered. Applicable if more than one MXM is connected.
Node Name	Name for the node - it may be the node's alias or any other arbitrary name.
Node Number	MXM directory number of the node.
Status	Connection status as indicated by icon.
Direction	Applicable to ISDN calls. Indicates if the node initiated (**Outgoing**) or received the call (**Incoming**).
Connection State	Describes the current connection or activity status of the node. For example, this column may indicate that a node is currently in a videoconference.
Bandwidth	Amount of bandwidth that is consumed by the node during the current call. If the node (such as an MCU) is engaged in more than one session, both total and per-session bandwidths appear.

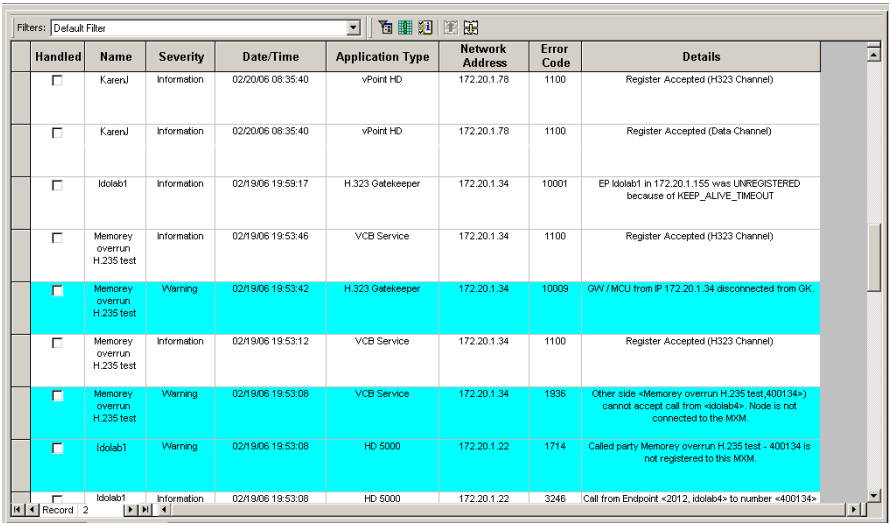
Audio Codec	If the node is in a call, this column indicates the audio transmission standard being used.
Video Codec	If the node is in a call, this column indicates the video transmission standard being used.
T.120	Data sharing specification that lets users share documents and applicants during an H.323 videoconference.
MLP	Multilayer Protocol. T.120 must use the MLP or HMLP channel for transmitting data. MLP data and audio can only be placed in the first 64 kbps channel of a connection.
HMLP	High-speed Multilayer Protocol. T.120 systems use this standard for high-speed data transmission. HMLP channels are multiples of 64 kbps.
LSD	Low Speed Data. During ISDN calls, this describes the transmission of video, audio and data in a single 64 Kbps channel.

Event Log Monitoring

The Event Log displays information about system events and operating conditions. You can view all network events during a time period, events involving a specific node, specific types of events, events of a certain severity level, and more. Refer to it if you need to troubleshoot and to isolate a problem.

➤ To view the Event Log for the MXM

1 Click the **Event Log** button.



Event Log View

2 To see events that occurred before those in the table, click the **Prior Events** button.

To see events that occurred after those in the table, click the **Next Events** button.

To update the table and display new events, click the **Refresh** button.

➤ To view the Event Log for a specific node

1 Right-click the node and then click **View Events**.

2 The Event Log opens for the specific node only.

Changing Record-Keeping Periods

From the Event Log View, you can change the periods of time that the MXM keeps records of specific types of events.

➤ To change the record-keeping period

1. In the Event Log View, click the Event Log Settings button. The MXM's **Event Log** properties tab appears.
2. Change the appropriate record-keeping periods (see "Event Log" on page 88).

Event Log Information

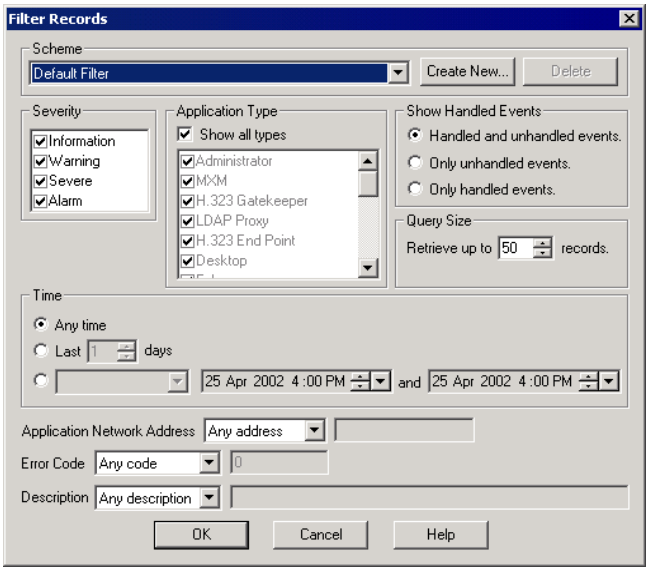
The Event Log provides the following information:

Handled	Indication if the event no longer needs administrator attention.
Name	Name of the node associated with the event.
Severity	Classification of the type of event that occurred. This can determine the level of attention that's required from the administrator.
Date/Time	Date and time that the event occurred.
Application Type	Type of node or group in which the event occurred.
Network Address	IP address of the node or group shown in the Application Type column.
Error Code	Indication of the type of error or event.
Details	Description of the event.

Filtering the Event Log

You can control the level of information that appears in the Event Log by defining filters according to the details that are important to you. You can set filtering according to all or any combination of the following criteria:

- Severity level
- Application (node type)
- Handled/unhandled events
- Number of displayed records
- Date and time
- IP Address range
- Error code
- Event description.



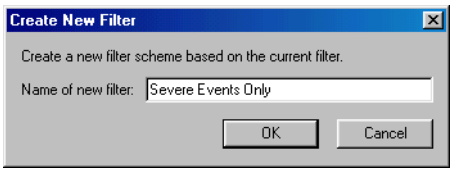
Filtering the Event Log

➤ To set Event Log view filters

1. In the Event Log, click the **Filter** button. The Filter Records dialog box appears.
2. Define the particular filters according to the specific criteria that you require for reducing the possible accounts that you want to check (for definitions of the categories, see "Filtering Criteria" on page 45).
3. Click **OK**.

➤ To save a filter for future use

1. In the Event Log, click **Create New**.
2. In the Create New Filter dialog box, type a name for the new filter scheme.
3. Click **OK**.



Saving a Filter Scheme

The scheme name now appears in the **Scheme** list.

To delete a scheme, select it from the **Scheme** list and click **Delete**.

Filtering Criteria

This section provides explanations for the various Event Log filtering categories (for definitions of the categories, see "Event Log Information" on page 42):

Severity — Set the log to display only certain types of events which affect the network's functioning.

Application Type — Set the log to display only events that occur in specific types of nodes.

Select **Show All Types** to include all node types in the Event Log.

Show Handled Events — Show events that are defined as handled (or fixed) or unhandled or both. This category helps you indicate if events no longer need administrator attention.

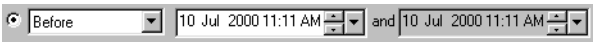
Query Size — Set the log to display a maximum number of records on the screen. If the log contains more than this number of records, you can click **Prior Events** and/or **Next Events** to display them.

Time — Set the log to display only records within a specific time range. Select one of the following options:

- ❑ Any time
- ❑ Up to 60 days before the current day
- ❑ A time range according to the following criteria:

  After, **Before**, **Between**, **On or after**, **On or before** a specific date and time.

If you select **Between**, you have to set an earliest and latest time limit.



Setting a Time Range Filter

Time (cont.)	To specify the time limit, click the large down arrow to open a calendar in which you can browse and choose an exact date and year. In addition, you can select one-by-one the date, month, year, hour, minute, and/or AM/PM. Then, click the small up or down arrows until the value that you want appears.
Application Network Address	Filters the event log to display events only from nodes whose IP addresses meet the criterion defined here. In the adjacent box, type the address range that fits the phrase selected from the list. For example, clicking **Begins with** and then typing **100.100.100.** will display records for accounts whose IP address is in the range greater than 100.100.100.0.
Error Code	Indicates the type of error or event that occurred.
Description	Set the log to display only records whose Details contains, does not contain, ends or begins with (and other criteria) a specific text string.

4.4 Setting Up Templates

When you manually grant permission to a new node to register, or if you add a new service, you have to confirm or change the item's properties before the item is added to the MXM's tree and database. The original default properties were set at Emblaze-VCON's production facility.

An administrator with Super User privileges may change various default properties by setting up a template. A template includes the characteristic properties for a type of node or service. Any newly created item in the system will initially have the default properties defined in the template.

Any changes to a template only affect new nodes that you create afterwards - they do not affect existing nodes.

Editing a Template

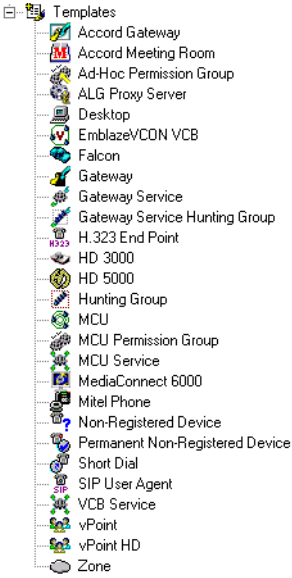
Templates are provided for the following items. For explanations about a template's properties, see the referred section. Other referred guides may be found on the MXM CD and the Documentation>Manuals page of the Emblaze-VCON website.

- ❑ Accord Gateway — See pages 228 to 232.
- ❑ Accord Meeting Room — See pages 212 to 215.
- ❑ Ad-hoc Permission Group — See pages 164 to 166.
- ❑ ALG Proxy Server — See the *SecureConnect Getting Started Guide*.
- ❑ Desktop systems — See pages 91 to 106 and the *MeetingPoint® End Point Properties Guide*.
- ❑ Emblaze-VCON VCB — See pages 173 to 178.
- ❑ Falcon — See pages 91 to 106 and the *Falcon End Point Properties Guide*.
- ❑ Gateway — See pages 132 to 138.
- ❑ Gateway Service — See pages 139 to 140.
- ❑ Gateway Service Hunting Group — See page 141 to 142.
- ❑ H.323 (non-Emblaze-VCON) End Point — See pages 91 to 106.
- ❑ HD3000 — See pages 91 to 106 and App. C.
- ❑ HD5000 — See pages 91 to 106 and App. D.
- ❑ Hunting Group — See pages 53 to 58.
- ❑ MCU — See pages 151 to 155.
- ❑ MCU Permission Group — See pages 160 to 162.
- ❑ MCU Service — See pages 155 to 159.

- ❑ MediaConnect 6000 — See pages 91 to 106.
- ❑ Permanent Non-registered Device — See pages 91 to 106.
- ❑ Short Dial — See pages 61 to 62.
- ❑ SIP User Agent — See pages 91 to 106.
- ❑ VCB Service — See pages 179 to 198.
- ❑ vPoint systems — See pages 91 to 106 and App. B
- ❑ vPoint HD systems — See pages 91 to 106 and App. A
- ❑ Zones (neighboring) — See pages 236 to 248.

➤ To edit a template

1 In the Main view, expand the **Templates** group to display all available templates.



List of Templates

2. Right-click a template, and then click **Properties**.

   The Properties dialog box appears.

3. Change the appropriate properties (see the list on the previous page for the locations of the relevant properties explanations). If applicable, click on other tabs in the dialog box to change more properties.

4. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.

4.5 Bandwidth Groups

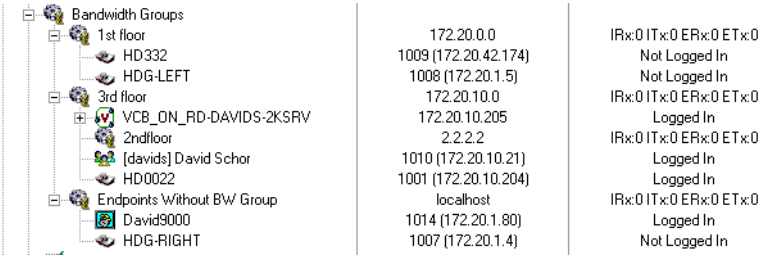
Bandwidth groups enable administrators to control usage of bandwidth among a select group of nodes who belong within a specified IP address range. An aggregate amount of bandwidth is made available to all nodes within a group at a single time. If enough bandwidth is available (within the aggregate), the MXM allows any node in the group to make a call. If there is not enough bandwidth remaining, the MXM does not allow any group member's calls to connect, unless enough bandwidth becomes available again.

Every registered node, except neighboring zones, automatically belongs to the bandwidth group which matches its IP address. A system-generated group, "Endpoints Without BW Group," is intended for nodes which do not meet the address specifications of the bandwidth groups that you create.

After you create a bandwidth group, it appears under the "Bandwidth Groups" object in the Main View. Nodes whose IP address falls within the defined range are placed in the appropriate group.

1. A node may belong to only one bandwidth group.
2. A bandwidth group may be a child of another bandwidth group.
3. You may force a node into a bandwidth group other than its "natural," address-determined group by using the Pin to Bandwidth Group command.
4. Multicast calls are not included in the bandwidth group summations.
5. Running the Delete command on a node under a bandwidth group object deletes the node and all its details from the MXM's database.

The illustration below shows an example of bandwidth groups.



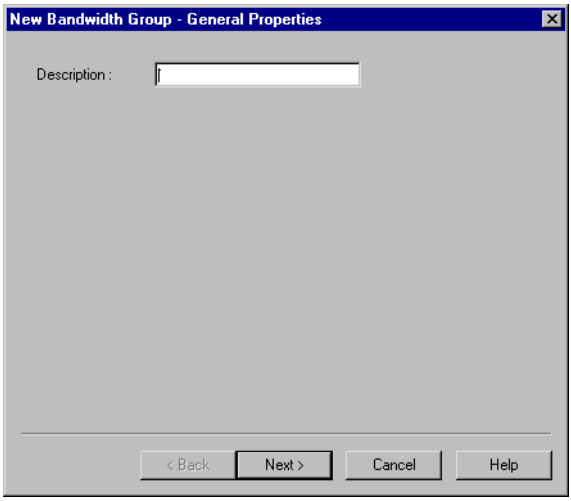
Bandwidth Groups in Main View

➤ To create a Bandwidth Group

1. In the Main View, right-click the Bandwidth Group object and then click **New Group**. The New Bandwidth Group wizard opens.
2. Define the properties (IP address range for nodes, bandwidth limits) according to your requirements (see). Click **Next** to go to the next page in the wizard.
3. Click **Finish** to add the entry to the Main View.

General Properties

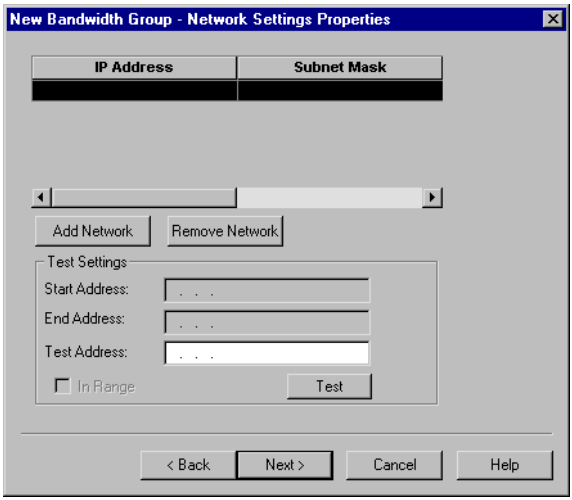
In the General page, give an identity to the bandwidth group. This name appears in the Main View under the Bandwidth Groups object.



Bandwidth Group - General Properties

Network Settings Properties

In the Network Settings page, define the permitted IP address ranges for the nodes belonging to this specific bandwidth group.



Bandwidth Group - Network Settings Properties

➤ To define the IP address range

1. Click **Add Network**. A new row in the Network Settings table appears.
2. Add the following:

Network Address — Define the host ID range for nodes in this group.

Subnet Mask — The subnet mask, helping to identify the available IP address range.

3. Add as many rows as your network requires.
4. To test whether a specific node is within a defined range, enter its IP address in the Test Address range. Click **Test**. In the Test Settings area, the following information appears:

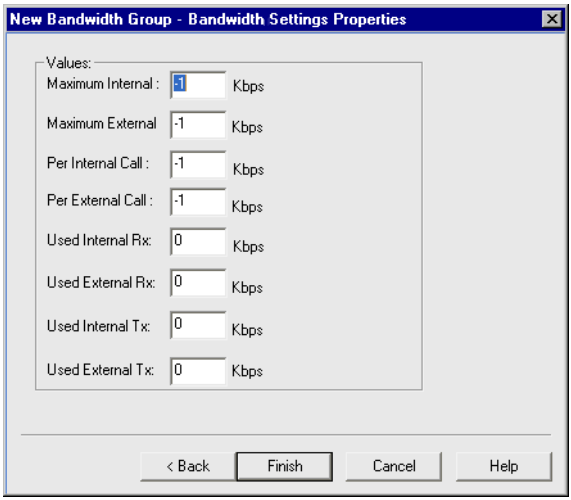
Start Address — The minimum IP address of the defined range.

End Address — The maximum IP address of the defined range.

In Range — If the tested address is within the defined range, a checkmark appears next to **In Range**.

Bandwidth Settings

In the Bandwidth Settings page, define the total bandwidth available to this bandwidth group at a single time.



Bandwidth Group - Bandwidth Settings Properties

In the Bandwidth Settings, define the following information:

Maximum Internal	The total bandwidth available, at a single time, for calls among nodes of this group.
Maximum External	The total bandwidth available, at a single time, for calls between nodes of this group and nodes outside of this group.
Per Call	Maximum bandwidth allowed during a single call.
Used Internal/ External Rx/Tx	Shows the amount of bandwidth being used at the current time by all the nodes of this group.

Pinning a Node to a Bandwidth Group

Every node registered to the MXM automatically belongs to a bandwidth group which is associated with the node's IP address. If you want to force a node to belong to a different bandwidth, you can use the Pin To Bandwidth Group command to accomplish this.

➤ To create a bandwidth group

❑ In the Main View, right-click the node, point to **Pin into Bandwidth Group**, and then choose the target group. The node then appears under the target group under the Bandwidth Group object.

If you choose **Return To Default Group**, the MXM automatically places the node into the bandwidth group matching its IP address.

4.6 Adding Hunting Groups

A hunting group includes a series of nodes that may be grouped together within an organization for a variety of reasons, but may be reached through one common number. When the common number is dialed, the MXM searches for a free node.

For example, if the first node is busy, the system tries to contact the next node, and so on. If all nodes are engaged, the MXM rejects the call.

The most important characteristic of a hunting group is the order in which calls are routed to members of the group. When you create a hunting group, you can determine the "hunting" order and method (see "Hunting Group Properties" on page 56).

Gateway Service hunting groups operate under a similar principle. You can set the order in which gateway services are requested when the hunting group's access number is dialed (see "Gateway Service Hunting Groups" on page 141).

➤ To create a hunting group

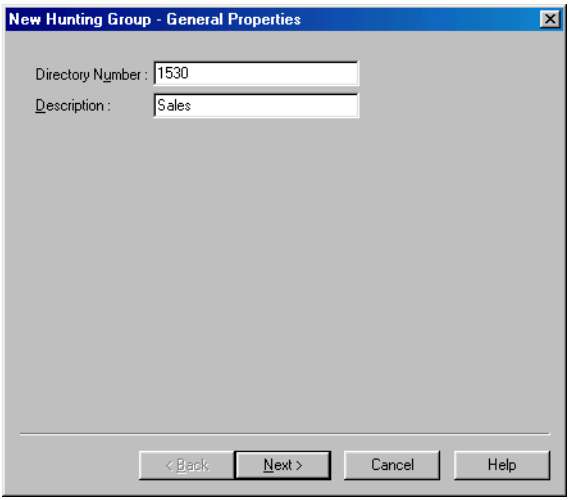
1 Click the **New Hunting Group** button. The New Hunting Group Properties wizard opens.

2 Change properties according to your hunting group requirements. To move to the next properties page, click **Next**. For explanations about the various properties, see pages 54 to 58.

3 Click **Finish**. In the Main View, the new hunting group appears under the Hunting Group object.

General Properties

The **General** page appears when you open the Hunting Group wizard. It contains identity information about the hunting group.



Hunting Group - General Properties

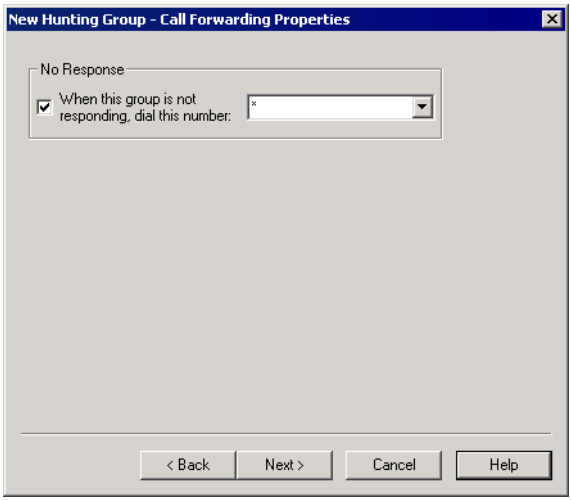
Set the following **General** Properties:

Directory Number — The number to be dialed in order to call this hunting group.

Description — Description or name for the group. This name appears in the Main View under the Hunting Groups object.

Call Forwarding Properties

In the Hunting Group Properties **Call Forwarding** page, set an alternate destination for the MXM to route calls.



Hunting Group - Call Forwarding Properties

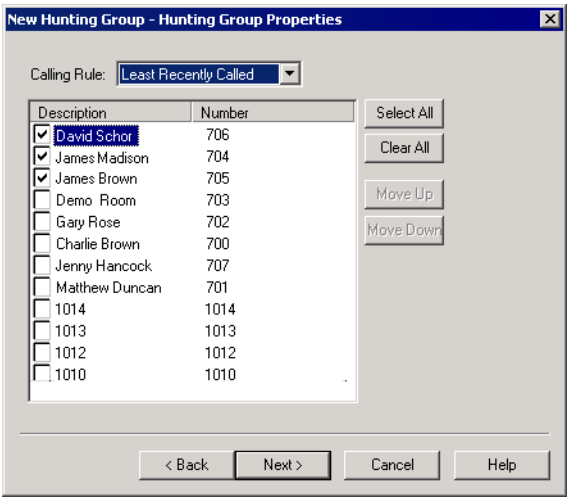
No Response

When this group is not responding, dial this number

Set an alternate destination for a call if none of the group members answers after a specified time. From the list, select the alternate destination.

Hunting Group Properties

In the Hunting Group Properties page, you can set the default hunting method, place specific nodes in the hunting group, and set the preferred order of hunting.



Hunting Group Properties

Set hunting group properties as follows:

Calling Rule — Default "hunting" method

Least Recently Called - Calls are routed first to the node which has not received a call in the longest time.

Circular - Calls are routed first to the node in the hunting group list that follows the last node that was called.

Fixed Order - The search starts at the first node in the hunting group list, then the second node, third node, and so on, until a free node is found.

Simultaneous - Simultaneous calls go to every member of the hunting group. Upon the first acceptance of a call, all the other calls disconnect.

Description/ Number — Select the nodes that will belong to this hunting group.

- To place all nodes in the hunting group, click **Select All**.
- To clear all the selections, click **Clear All**.

Setting the Hunting Order

In the New Hunting Group Properties dialog box, selected nodes are automatically placed in the top part of the list. You can then move them to different places in the hunting order. Their locations in the list, together with the Calling Rules setting, determines the hunting order.

➤ To set the hunting order of the selected nodes

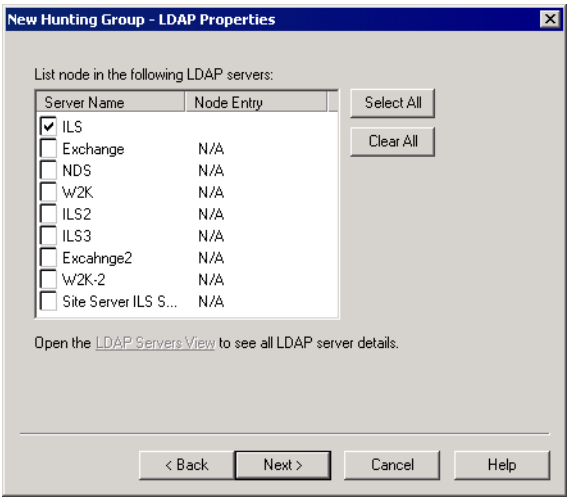
1. Click the name (*not* the checkbox) of a selected node. To move the node up and down the list to its designated place, click **Move Up** or **Move Down** as many times as necessary.

   Repeat this step for as many nodes as necessary.

2. Click **OK** to implement the settings and close the dialog box.

Hunting Group LDAP Properties

In the LDAP page, you can define the hunting group's registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server.



Hunting Group - LDAP Properties

List node in the following LDAP servers

Select LDAP servers that can contain the subdirectory in which the hunting group should be listed. Hunting groups may be registered in all LDAP servers in which the MXM is registered.

If the hunting group has been previously registered in an LDAP server, its entry name or number (node entry) appears in the list.

- To be listed in all LDAP servers (depending on MXM registration in them), click **Select All**.
- To clear all the selections, click **Clear All**.

Additional ID Properties

In addition to its directory (E.164) number, a hunting group may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 ID. In the **Additional ID** page, you may enter these, if applicable. For example, the Description entered in the **General** page will appear as an Additional ID as an H.323 ID.

For more information about adding Additional IDs, see "Additional IDs" on page 106.

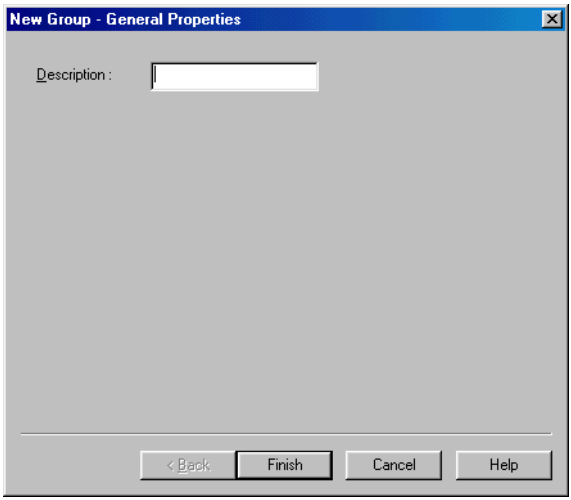
4.7 Adding an Administrative Group

You can create Administrative Groups of nodes that reflect the needs of the enterprise's organization. Administrative groups in the Main View can help maintain a visual structure for nodes and the teams and departments to which they belong. This also makes it easier to set common end point properties within a team or department, such as limiting the available bandwidth for the group.

For example, you can create groups for Management, Sales, Finance, R&D, or others and place end points accordingly.

➤ To create an administrative group

1 Click the **New Administrative Group** button. The New Group wizard appears.



New Administrative Group Properties

2 In the **Description** box, type a name for the group and click **Finish**. This name will appear on the system tree.

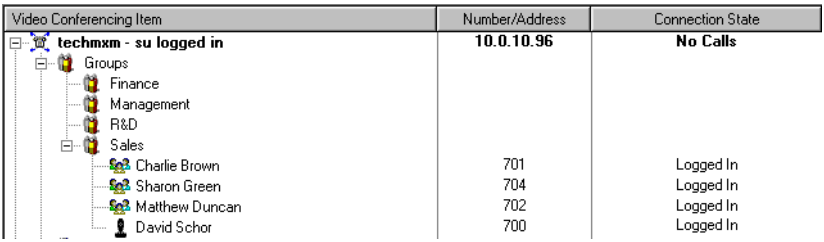
3 To create more groups, repeat steps 1 and 2.

4 To see the created groups in the Main View, expand the Groups object.

You can also add administrative subgroups as branches under other created groups. To do this, select an existing administrative group before clicking the Add Administrative Group button.

➤ To place nodes into an administrative group

1. In the Main View, select one or more nodes.
2. Drag the nodes to the administrative group.



Sample Administrative Group

Changing Group Member Properties

Administrative groups make it easier to control end point properties that need to be common within a team or department, such as limiting the available bandwidth for the members of a group.

➤ To change common properties for all group members

1. Right-click the group name, point to **Member Property**, and click the specific property type.

   A Properties dialog box for all group members opens to the property type that you clicked. Common properties among the group members are available for change.
2. Change the appropriate properties. Remember that this change affects all the group members.
3. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.

4.8 Adding a Short Dial Number

A Short Dial Number is a number, that when dialed, is routed to another specific registered user. It ideally is used as an easy-to-remember number intended to dial an ISDN number through a gateway, or reach a department or a location instead of a specific user.

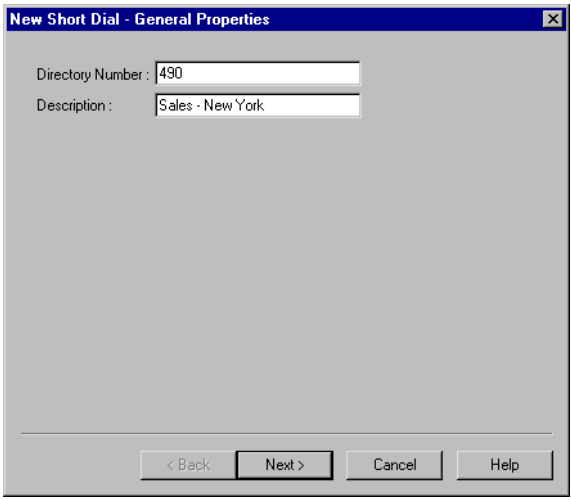
For example, you can set up a Short Dial Number, “490”, that automatically dials “90017185557890” through a gateway.

➤ To add a Short Dial number

1. In the Main View’s toolbar, click the New Short Dial button. The New Short Dial Wizard appears.
2. Change properties according to your short dial requirements. To move to the next properties page, click **Next**. For explanations about the various properties, see the following subsections.
3. Click **Finish**. In the Main View, the new Short Dial entry appears under the Short Dial Numbers object.

General Properties

The **General** page appears when you open the New Short Dial wizard. It contains identity information about the entry.



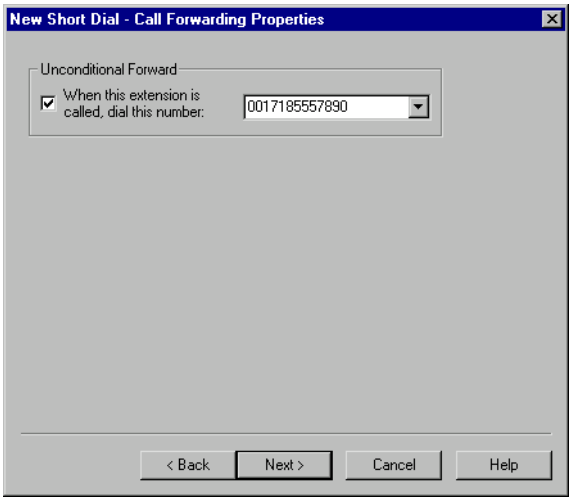
Short Dial - General Properties

Set the following **General** Properties:

Directory Number	The number to be dialed in order to call the user that this entry represents.
Description	Description or name for the entry. This name appears in the Main View under the Short Dial Numbers object.

Call Forwarding Properties

In the **Call Forwarding** tab, select the user who will receive any videoconference calls dialed to the Short Dial number.



Short Dial - Call Forwarding Properties

LDAP Properties

The **LDAP** tab provides information about the Short Dial number's registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes' LDAP Properties, see "LDAP" on page 104.

Additional ID Properties

In addition to its directory (E.164) number, a Short Dial number may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** page, you may enter these, if applicable. For more information about adding Additional IDs, see "Additional IDs" on page 106.

5 SETTING MXM SYSTEM PROPERTIES

MXM servers have system properties that define their operation. In the MXM Properties dialog box, the properties are divided into various categories:

MXM	Connection, System Information, Dial Plan, LDAP Settings See page 64.
Call Control	System Bandwidth Control, Call Settings, Ad-hoc Resources See page 72.
ISDN Call Routing	System Location, Dialing Prefixes See page 77.
Security	Security Mode, License, Non-registered Devices See page 79.
H.323 & SIP	Zone Settings, Advanced Settings See page 84.
Reporting	Billing, Event Log See page 87.

➤ To define MXM Server system properties

1. In the Administrator window, right-click the MXM node at the top, point to **Property** (opening another menu), and click the specific property type.

   -or-

   Click the MXM node and then click the **Display Properties** button.

2. In the Properties dialog box, change properties according to the system's specifications. To set different types of system properties, click the appropriate category icon on the left side of the dialog box, and then click the tab at the top of the dialog box. For explanations about the various properties, see the above list for their locations.
3. To implement the change and proceed to another set of MXM properties, click **Apply** and then the appropriate category icon and tab.
4. To implement all the changes and close the dialog box, click **OK**.

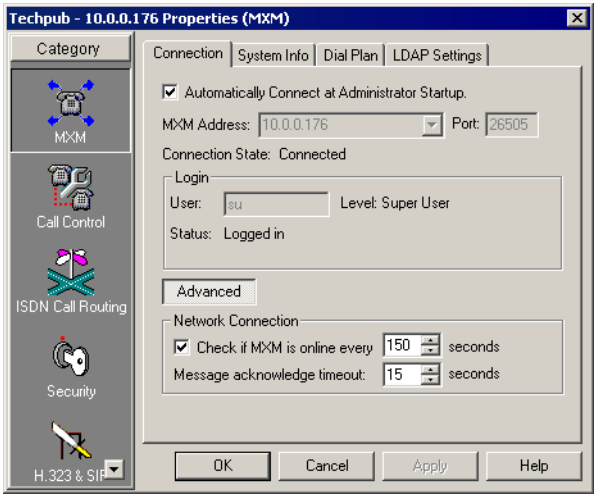
5.1 MXM Properties

In the MXM system Properties dialog box, click the **MXM** icon to access the following property pages:

- Connection
- System Info
- Dial Plan
- LDAP Settings

Connection

The **Connection** tab contains information about the MXM Administrator application's connection to the MXM.



MXM Connection Properties

Set the connection properties as follows:

Automatically Connect at Administrator Startup	Select this option if you want to connect to this MXM automatically whenever you start the Administrator application.
MXM Address	IP address or DNS name of the MXM.
Port	TCP/IP port number. Automatically provided by the system.
Connection State	Informs you if the MXM Administrator application is connected and available for management, trying to connect, or not trying to connect to the MXM.
Login	Provides information about the current login state:
User	The administrator name.
Level	Level of administration privileges permitted to the User.
Status	Current state of the login attempt.

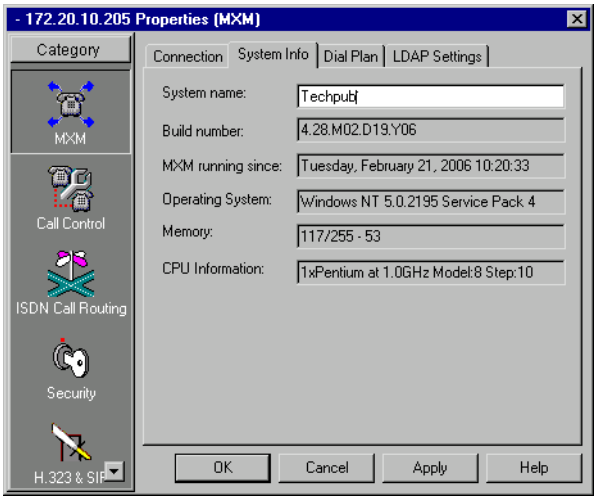
Clicking **Advanced** displays the following properties:

Network Connection

Check if MXM is online	Select if you want the Administrator application to periodically check that the MXM is still connected, when there is no traffic over the connection. Next to that property, select the number of seconds between checks if there is no activity over the connection.
Message Acknowledge Timeout	Select the number of seconds that the Administrator application waits to receive an update response from the MXM. After this interval, a message states that the MXM did not respond.

System Info

The **System Info** tab provides information about the current MXM version. Provide this information if you contact Emblaze-VCON's Technical Support.



MXM System Information

System Name — The identifying name for the MXM. This name does not affect the operation of the system.

Build Number — The number and date of the MXM software version.

MXM Running Since — Date and time when the MXM started operating.

Operating System — Operating system and version of the MXM server's host.

Memory — Shows the MXM server's host computer's memory usage at the time of the program's startup, written in the following syntax:

a/b - c

where:

a = amount of memory in use (MB).

b = total memory in the computer (MB).

c = percentage of memory which is free.

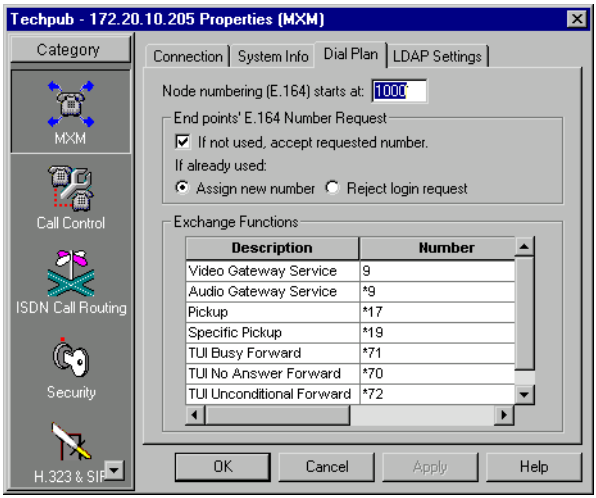
CPU Information — Decscription of the MXM server's host computer's processor.

Dial Plan

In the **Dial Plan** tab, define how the MXM assigns directory numbers (E.164-type) to registered end points and other nodes. Entering directory numbers are a convenient way for registered users to dial other nodes.

This tab also includes the names of the supplemental exchange functions and the default Telephony User Interface (TUI) numbers that the end point may dial to activate each of them. You may change the number for any of the functions.

For more information about how end points use exchange functions, see the MXM's Online Help's *Telephony Exchange Functions* topics.



Dial Plan Properties

Set directory numbering as following:

Node numbering (E.164) starts at

This number is the starting point for assigning directory numbers to registering nodes. You can provide for two, three, four, etc. digits for numbering nodes.

For example, if this number is "700", new nodes will receive the first 3-digit number available between 700 and 999. To increase the numbering capacity (according to the license key code's specification), you can specify a larger 3-digit range or add a fourth digit.

End Points' E.164 Numbering Request

If not used, accept requested number

Select to grant any E.164 number requests, if available, by registering end points.

If deselected, the MXM assigns directory numbers only according to the Node numbering definition above, and rejects all user E.164 numbering requests.

If already used

Assign new number

Select to accept the login request, but to assign a directory number according to the Node numbering definition above.

Reject login request

Select to reject the login request if the specified E.164 number is already assigned to another node.

The Exchange Functions table lists the available functions and their corresponding TUI numbers.

➤ To change the TUI number of an exchange function

❑ Click in the **Number** column of the entry that you want to change.

Delete the previous number and type a new number.

To replace other numbers, repeat this step as many times as necessary.

vPoint HD, vPoint, HD5000/4000, HD3000/2000, Falcon, and MeetingPoint 4.6 provide access to the various exchange functions (call pickup, forwarding, invite and transfer) from their interfaces.

The available functions are:

Video Gateway Service

For starting an ISDN videoconference over a gateway. The end point must enter this number, followed by the ISDN channel numbers, and then click **Dial**.

The default value is **9**.

Audio Gateway Service

For starting an ISDN audio conference over a gateway. The end point must enter this number, followed by the ISDN channel numbers, and then click **Dial**.

The default value is ***9**.

Pickup

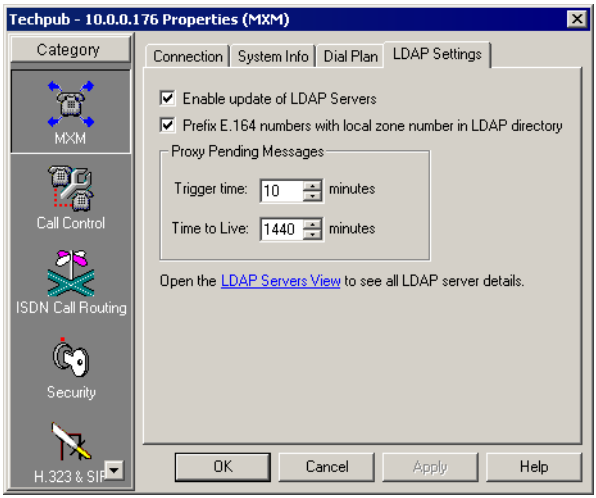
For picking up a call that's intended for any destination for which the end point has pickup permission. The end point enters this number and then clicks **Dial**.

The default value is ***17**.

Specific Pickup	For picking up a call that's intended for a specific destination (for which the end point has pickup permission). The end point enters this number, followed by the directory number of the destination end point, and then clicks **Dial**. The default value is ***19**.
TUI Busy Forward	If the end point is busy in a videoconference, the MXM forwards all incoming calls for it to an alternate destination. To activate, the end point enters this number, followed by the directory number of the alternate destination, and then clicks **Dial**. The default value is ***71**.
TUI No Answer Forward	If the end point does not answer, the MXM forwards a call to an alternate destination. To activate, the end point enters this number, followed by the directory number of the alternate destination, and then clicks **Dial**. The default value is ***70**.
TUI Unconditional Forward	The MXM forwards ALL calls intended for the end point to an alternate destination. To activate, the end point enters this number, followed by the directory number of the alternate destination, and then clicks **Dial**. The default value is ***72**.
Ad-hoc Conference	For inviting additional users to an open point-to-point videoconference. The end point enters this number, followed by the directory number of the target end point, and then clicks **Dial**. The default value is *77.
Transfer	For transferring an open videoconference to another end point (and disconnecting from the transferring end point). The transferring end point enters this number, followed by the directory number of the target end point, and then clicks **Dial**. The default value is ***45**.

LDAP Settings

In the **LDAP Settings** tab, enable the MXM to periodically update its registered users in connected LDAP (Lightweight Directory Access Protocol) online directories. For more information about LDAP, see Chapter 15, "Registering with LDAP Directories."



LDAP Settings Properties

Set LDAP Settings as follows:

Enable Update of LDAP Servers	Select to enable the MXM to update its registered users information in the LDAP directories.
Prefix E.164 numbers with local zone number	If neighboring zones are included in your online directories, select this option to append zone numbers to the directory numbers of all listed nodes.

Proxy Pending Messages

If no communication was received from the LDAP directory after a certain interval, the MXM asks the LDAP Proxy server if its directory list (for the MXM registered users) requires updating.

Trigger Time	Enter the interval between update request messages sent by the MXM to the LDAP Proxy server.
Time to Live	Enter the interval for discarding an update request message that is not received by the LDAP Proxy server.
LDAP Servers View	For information about the available LDAP servers, click this link. The LDAP Servers table appears, displaying location and access information about the available servers.

If you update the MXM's LDAP settings, you must also update the same configuration settings in the LDAP server (see Chapter 15, "Registering with LDAP Directories").

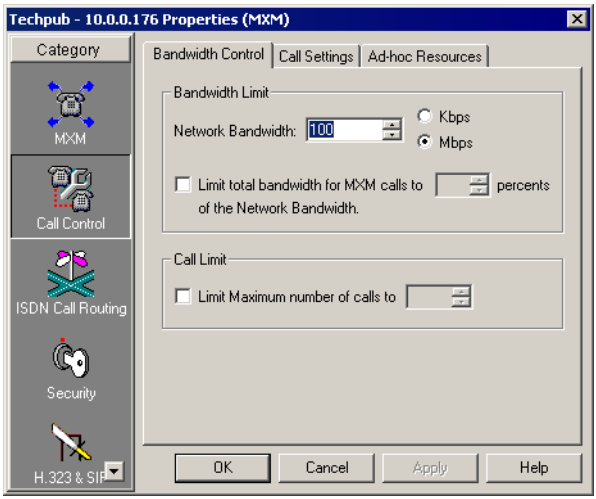
5.2 Call Control Properties

In the MXM system Properties dialog box, click the **Call Control** icon to access the following property pages:

- ❑ Bandwidth Control
- ❑ Call Settings
- ❑ Ad-hoc Resources
- ❑ Number Manipulation

Bandwidth Control

In the **Bandwidth Control** tab, define how the MXM manages the available bandwidth within its zone.



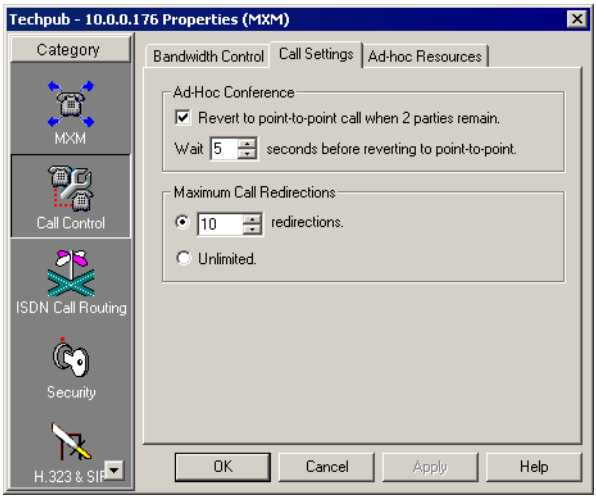
Local MXM's Bandwidth Control Properties

Set bandwidth control properties as follows

Network Bandwidth	Total amount of bandwidth available to the LAN.
Limit total bandwidth of MXM calls	Select to define the percentage of total network bandwidth to be allocated for calls managed by the MXM.
Limit maximum number of calls to	Select to define the maximum number of conferences managed by this MXM, that can carry on at the same time. The amount of open conferences cannot exceed the bandwidth limit defined above.

Call Settings

The **Call Settings** tab includes properties defining call connection throughout the videoconferencing network.



Call Settings Properties

Set Call Settings properties as follows:

Ad-hoc Conference

Revert to point-to-point call when 2 parties remain — Select to return to a point-to-point call when only two parties remain in an ad-hoc videoconference.

Wait __ seconds before reverting to point-to-point — After a third party disconnects, the videoconference will revert to a point-to-point session after this interval.

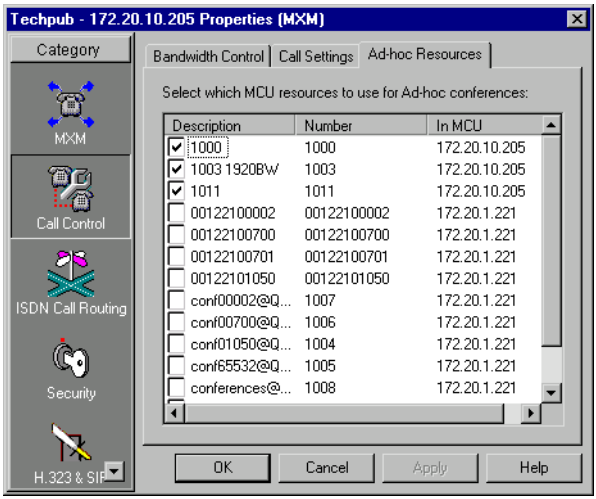
Maximum Call Redirections

___ redirections — Select the maximum number of times that a call can be forwarded sequentially to other nodes before the call is cancelled.

Unlimited — Select to allow calls to be forwarded to as many destinations as necessary until they are answered.

Ad-hoc Resources

The Ad-hoc Resources table contains a list of MCU and VCB services registered with the MXM, together with the MCU or VCB with which they are associated. Select the services that the MXM may use to initiate an ad-hoc videoconference.



Available Ad-hoc Resources

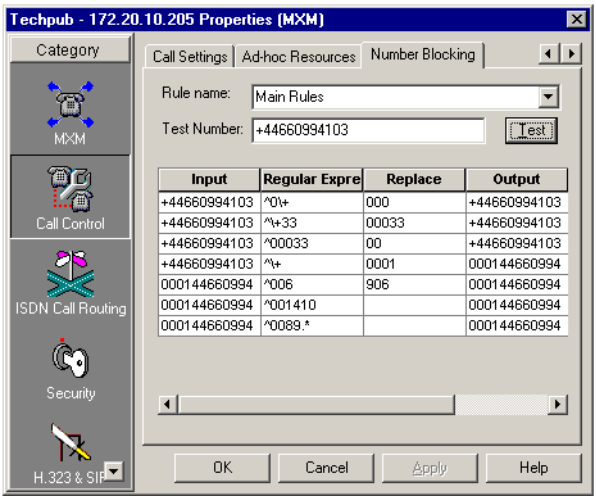
Number Manipulation

Number manipulation is a set of rules for translating blocks of dialed digits and/or characters into other formats, such as a gateway prefix or an area code, which enables the MXM to send the call towards its destination.

When a user dials a string covered by any of the rules, the program identifies the dialed digits/characters, and uses regular expressions to convert them into a target string which complies with standard dialing convention.

For more information about working with regular expressions, please go to the following sites:

- www.snapfiles.com/get/regexcoach.html
- www.weitz.de/regex-coach/



Rules for Number Manipulation

➤ To enter number manipulation rules

1. In the Main View, click the MXM node at the top and then click the **Display Properties** button.

2. In the Properties dialog box, click the **Call Control** icon and scroll to the **Number Manipulation** tab.
3. In the **Rule Name** box, enter a name for the set of rules.
4. In the table's **Regex** column, type the expressions which need a translation rule.
5. In the **Replace** column, type the resulting target string for the translation.

➤ To test the application of the rules on a dialing number string

1. In the **Test Number** box, type the string you want to dial.
2. Click **Test**.

   In the table, the Test Number appears in the **Input** column and the resulting dialed number appears in the **Output** column for all the rules.

Examples

Convert	Regex	Replace	Dialing
International calls starting with a "+" sign to standard dialing convention ("0001")	\+	0001	+44660994103 converts to 000144660994103.
Calls for a specific country into local calls	\+44	00044	+44660994103 converts to 00044660994103.
Converting internal calls into 5-digit PBX calls	001410		00141041050 converts to 41050.
Blocking calls to a particular prefix	\0089.*		00899876543 fails to connect.

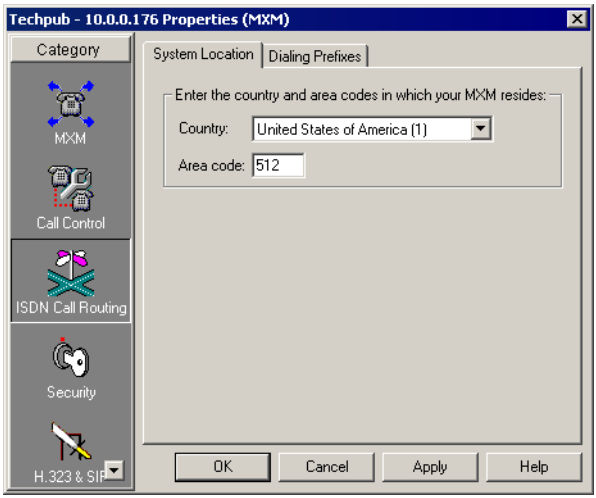
5.3 ISDN Call Routing Properties

In the MXM system Properties dialog box, click the **ISDN Call Routing** icon to access the following property pages:

- System Location
- Dialing Prefixes

System Location

In the **System Location** tab, enter the country and area code in which the local MXM is located. This information is used when the MXM computes ISDN and gateway call rates.



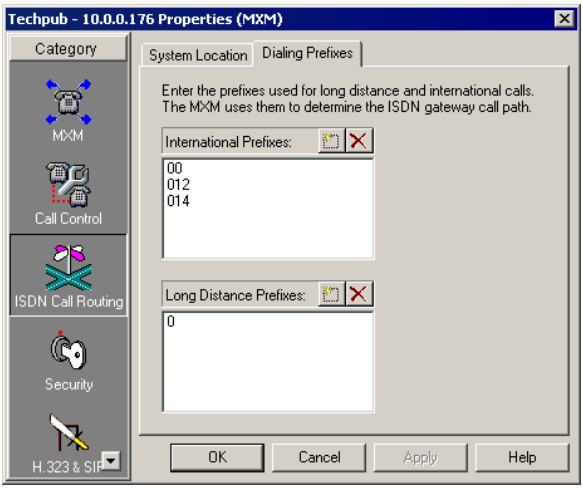
Local MXM Location

Dialing Prefixes

In the **Dialing Prefixes** tab, enter the prefixes which are required for dialing international and long-distance videoconferencing calls. If the call requires routing through a gateway, the MXM uses this information when it determines the optimum gateway and service (see "Testing for the Optimal Gateway Service" on page 147.

For example, international calls may require that you add a prefix such as 00 or 1 before dialing a country code. This number is provided by the local telephone company or other ISDN provider.

Long distance calls within a country also may require a prefix such as 0 or 1 before the remainder of the ISDN number.



Gateway Dialing Prefixes for Local MXM Network

➤ To add prefixes

1. Click the New Prefix button.
2. Type the prefix and press <Enter>.
3. To add more prefixes, repeat steps 1 and 2 as many times as required.
4. Click **Apply** to implement the settings while remaining in the dialog box.

   -or-

   Click **OK** to implement the settings and close the dialog box.

➤ To delete prefixes

1. Select the prefix that you want to delete.

2. Click the Delete button.
3. Click **Apply** to implement the settings while remaining in the dialog box.

   -or-

   Click **OK** to implement the settings and close the dialog box.

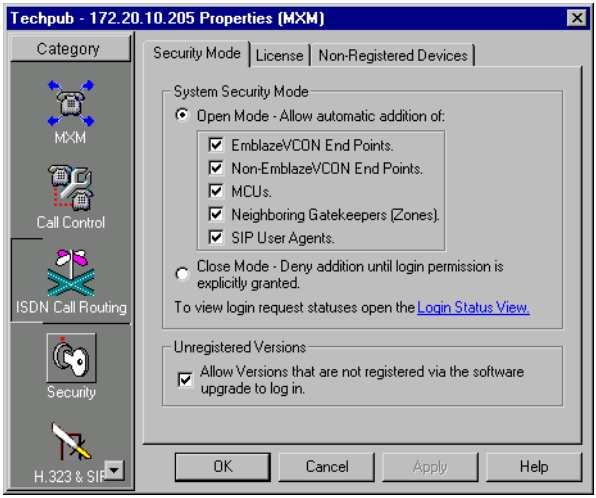
5.4 Security Properties

In the MXM system Properties dialog box, click the **Security** icon to access the following property pages:

- Security Mode
- License
- Non-Registered Devices

Security Mode

In the **Security Mode** tab, set the properties for restricting login to specific users. You can set up the MXM in any or all of the available Open Modes, or in Closed Mode to all nodes.



MXM's Security Mode

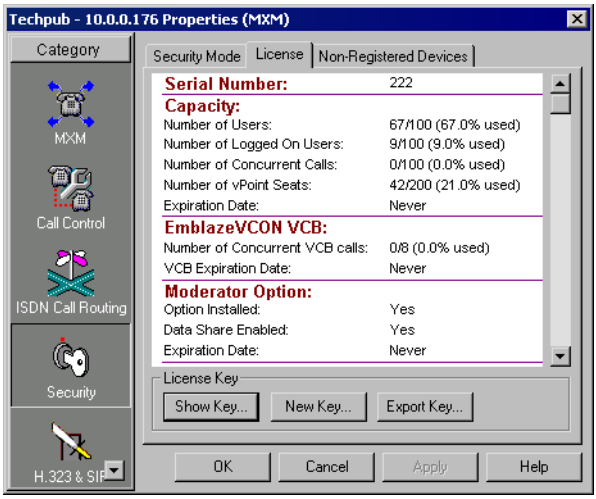
Set the security mode as follows:

System Security Mode

Open Mode	Select to allow automatic login privileges to various types of nodes, which are listed below this option. A deselected type must be manually granted or refused login permission by the administrator
Emblaze-VCON end points	Select to automatically accept Emblaze-VCON systems that register (Escort, Cruiser 150/384, ViGO, MediaConnect 6000/8000, Falcon, VCON Conference Bridge).
Non-Emblaze-VCON end points	Select to automatically log in any non-Emblaze-VCON H.323 videoconferencing node that registers.
MCUs	Select to automatically log in any MCU that registers.
Neighboring Gatekeepers (Zones)	Select to automatically list other MXMs and Gatekeepers that the local MXM calls or that contact it. In addition, this selection enables registered MXM nodes to receive calls from other zones. These zones appear automatically in the Main View.
SIP User Agents	Select to automatically log in any SIP user agent that registers.
Closed Mode	Select to restrict login privileges. All nodes that attempt to register must be granted login permission manually or rejected by the administrator.
Login Status View	Click this link to display the Login Status Table. The far right column of the table shows the login status for specified nodes. For more details about the Login Status Table, see "Viewing the Login Status" on page 37.
Allow versions that are not registered via the software upgrade to log in	Select this option to grant registration and login to nodes that are using a videoconferencing application version not defined in a Software Upgrade task (see "Selecting a Software Version" on page 115). If this option is deselected, the MXM refuses to grant login to these nodes until their software matches a Software Upgrade task.

License

The **License** tab shows the number of registered users that the MXM is licensed to service. If you need to change these numbers, contact your local Emblaze-VCON distributor.



License Properties

Serial Number The license number of your MXM system.

Capacity

Number of Users Actual and maximum numbers, respectively, of non-vPoint Software-only end points that this MXM is permitted to register, according to its current license.

Number of Logged On Users Actual and maximum numbers, respectively, of non-vPoint software-only end points that are logged in at the current time.

Number of Concurrent Calls Actual and maximum numbers, respectively, of registered nodes that can be engaged in calls at one time.

Number of vPoint Seats Actual and maximum numbers, respectively, of vPoint software-only end points that this MXM is permitted to register, according to its current license.

Expiration Date Depending on your license, this will be either **Never** or the date that your MXM license expires. If your license is temporary, see "Replacing the MXM License Key" on page 11 for information about updating your license.

Emblaze-VCON VCB

Max. Number of VCB Conferences	The number of simultaneous ad-hoc videoconferences managed by the VCB allowed.
Expiration Date	Depending on your license, this will be either **Never** or the date that this license expires.

Moderator Option

Option Installed	Indicates if Conference Moderator has been installed on the same server as the MXM.
Data Share Enabled	Indicates if data sharing is allowed in conferences managed through the Conference Moderator.
Expiration Date	Depending on your license, this will be either **Never** or the date that this license expires.

IP-Nexus Server

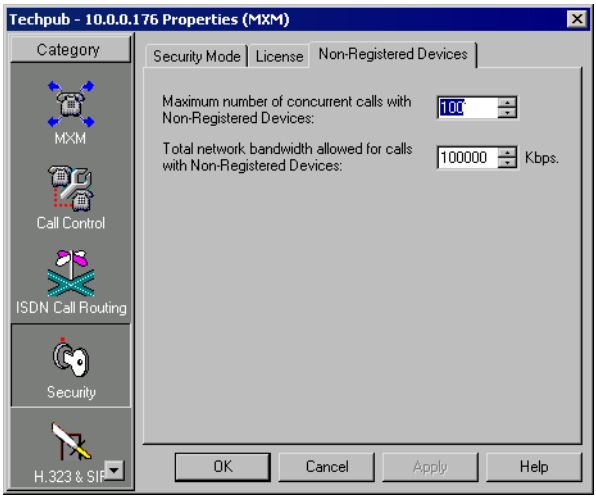
Option Installed	Indicates if your MXM includes the IP-Nexus Server option, which provides instant messaging, application sharing, file transfer, and other services to users who register with the IP-Nexus Server.
Expiration Date	Depending on your license, this will be either **Never** or the date that this license expires.
Max. Number of Concurrent Users	The maximum number of users that can be logged in at one time.

License Key

Export Key	Your initial key code is valid for 30 days. To purchase a license for a different number of ports, click **Export Key** to create a license file for the MXM on its host computer. Send the file to your local Emblaze-VCON distributor. You will then receive the appropriate key without time restrictions.
Show Key	Click to view the key code for the current MXM Server installation.
New Key	After receiving a new license file from your Emblaze-VCON distributor, click this button, browse to select the file and click **Open**. When prompted to apply the license code, click **OK**. To implement the license change and close the dialog box, click **OK** again.

Non-Registered Devices

In the **Non-Registered Devices** tab, define how the MXM allows registered end points to engage in videoconferences with nodes that are unable to register with the MXM.



Non-Registered End Point Settings

Set the properties as follows:

Maximum Number of Concurrent Calls with Non-registered Devices — Maximum number of simultaneous calls involving non-registered end points that the MXM may handle.

Total Network Bandwidth Allowed for Calls with Non-registered Devices — Select the limit on the amount of bandwidth (in Kbps) that may be allocated to these videoconferences. The value must be a multiple of 100 (such as 200, 5000, 999000).

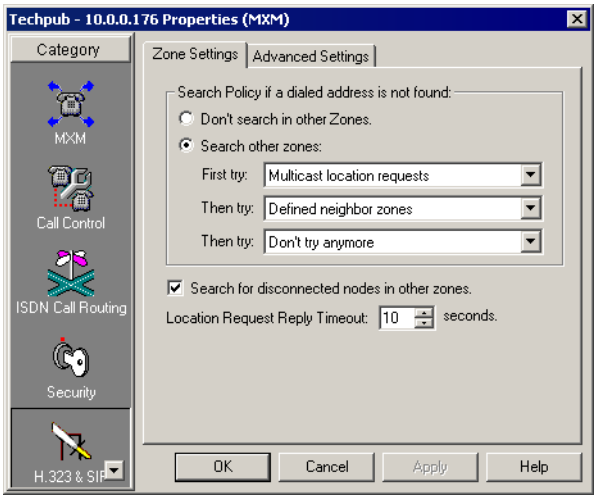
5.5 H.323 & SIP Properties

In the MXM system Properties dialog box, click the H.323 & SIP icon to access the following property pages:

- Zone Settings
- Advanced Settings

Zone Settings

In the **Zone Settings** tab, define the method of search that the MXM uses when a registered end point dials a party in a different zone (*neighbor node*).



MXM Gatekeeper Zone Settings

Search Policy

If a dialed address is not found, the MXM will continue (or not) to search for that address according to one of the following policies:

Don't search in other zones The MXM will reject the call without searching in other zones.

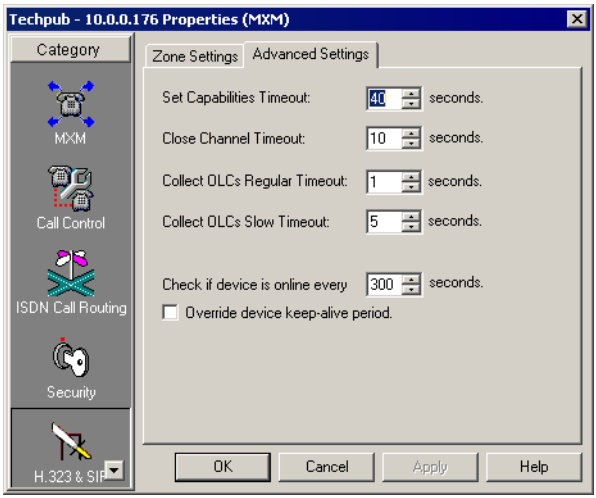
Search other zones

If the dialed address is unknown to the local MXM, the MXM will send out Location Requests (LRQs) to other MXMs and gatekeepers, according to the policy defined here.

First Try/Then Try	In the **First Try** list, select the search method that the local MXM employs first. In the first and second **Then Try** lists, select alternative search methods in case the first method fails to find the dialed node.
Multicast Location Requests	The MXM sends out identical LRQs to all detected zones. The call is connected to the first zone that sends a positive response (party found) to the MXM.
Defined Neighbor Zones	The MXM only sends LRQs to zones that are listed in the MXM Administrator, or "known" to the MXM. The call is connected to the first zone that sends a positive response (party found) to the MXM.
Directory Gatekeepers	The MXM sends LRQs only to directory gatekeepers known to it.
Don't Try Anymore	At this stage, the MXM stops sending LRQs.
Search for disconnected nodes in other zones	If a call is dialed to an MXM node that is currently not logged in, the MXM continues to search for that node in other known zones.
Location Request Reply Timeout	Select the maximum interval for the MXM to receive a reply from the dialed destination's gatekeeper. If this interval passes before the MXM receives this reply, the call is disconnected.

Advanced Settings

In the **Advanced Settings** tab, set the intervals at which the MXM activates various timeouts.



MXM Gatekeeper Advanced Settings

Set Capabilities Timeout Select the maximum interval for registered end points to receive the H.323 capabilities of the dialed destination. If this interval passes before the end point receives this information, the MXM disconnects the call.

Close Channel Timeout Select the maximum time for H.323 logical channels to close when a videoconference ends.

Collect OLCs Regular Timeout The maximum period that the MXM collects information transmitted by H.323 devices (except gateways) in order to synchronize a SIP-H.323 conversation.

Collect OLCs Slow Timeout The maximum period that the MXM collects information transmitted by H.323 gateways in order to synchronize a SIP-H.323 conversation.

Check if device is online Select the interval for checking if all registered nodes are connected to the MXM. At this time, the MXM polls the devices. If it does not receive a response from a node, the node is logged off.

Override device keep-alive period Select to use the MXM's polling interval instead of any intervals that may have been defined in individual nodes.

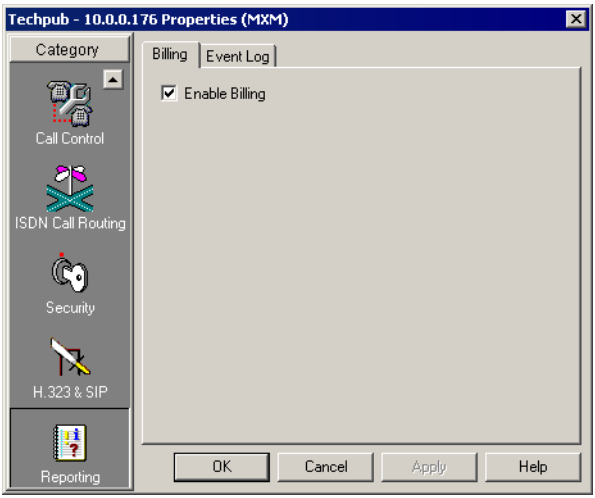
5.6 Reporting Properties

In the MXM system Properties dialog box, click the Reporting icon to access the following property pages:

- Billing
- Event Log

Billing

In the **Billing** tab, select **Enable Billing** to list all calls within the local zone in a Call Details Record (CDR).

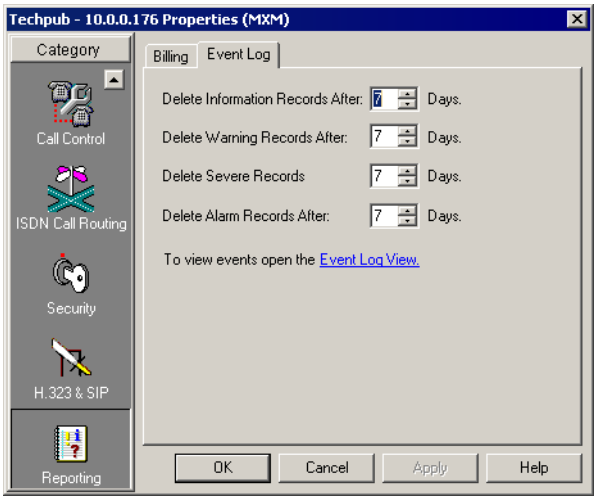


Billing Properties

For more information about CDRs and call accounting, see **Working with the MXM>Reporting Option>Call Accounting** in the MXM's online help.

Event Log

In the **Event Log** tab, define the length of time that the MXM keeps records of specific types of events.



Event Log Properties

Set record-keeping periods as follows:

Delete Informatory Records After	Amount of time until informative records are deleted from the log.
Delete Warning Records After	Amount of time until warning records are deleted from the log.
Delete Severe Records After	Amount of time until severe error records are deleted from the log.
Delete Alarm Records After	Amount of time until alarm records are deleted from the log.
Event Log View	To view the event log, click this link.

6 Defining End Point Nodes

End point nodes can represent several different types of users who log in to the MXM and require its services. This chapter provides explanations for defining the MXM management configuration for registered Emblaze-VCON HD, vPoint, MeetingPoint, Group System end points, or other videoconferencing applications.

The videoconferencing system configurations of registered Emblaze-VCON HD (vPoint, 2000/3000, 5000) end points, vPoint end points (ViGO, software only), MeetingPoint 4.6 end points (ViGO, Escort, Cruiser, MediaConnect 8000/9000) and Falcon may be viewed and changed from the MXM. Descriptions of the Properties for some Emblaze-VCON end points are located in Appendixes A to D.

6.1 Setting Up an End Point

In order to register, an end point contacts the MXM (see "Granting Login Permission" on page 28). If login permission is granted automatically (Open Mode), the end point retains the default MXM properties. These default properties may be viewed or changed in the relevant end point configuration templates (see "Setting Up Templates" on page 47).

When you grant login permission manually, you can register the node with the default MXM properties or set the properties during the login process.

➤ To set up an end point's properties

1 After login permission is granted:

Open Mode — In the Administrator window, registered Emblaze-VCON end points appear under the **Emblaze-VCON Systems** group. Non-Emblaze-VCON end points appear under the **H.323 End Points** group. Double-click the new end point to set up its properties.

Closed Mode — The New End Point Wizard appears.

2 Change properties according to your system specifications. To set different types of end point properties, click the appropriate tab at the top of the dialog box (in the New end point Wizard, click **Next** to advance to the next properties page). For explanations about the various properties, see "Setting End Point MXM Properties" on page 91.

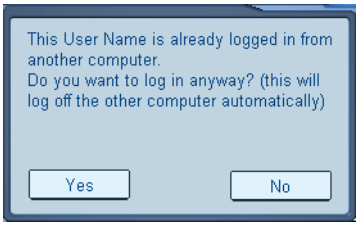
3 To implement all the changes and close the dialog box, click **OK** (in the last page of the New end point Wizard, click **Finish**).

Login Attempt by Duplicate Users

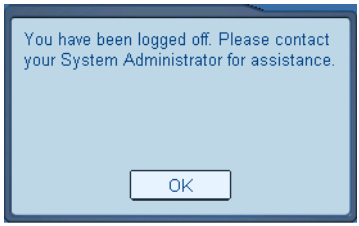
The same User Name may not be logged in to the MXM from more than one end point at the same time.

In case of a duplicate login attempt from vPoint HD, vPoint, and MeetingPoint 4.5 (or higher) end points, the user is given the choice of:

- Continuing to log in using the same name, causing the other end point to be disconnected from the server.
- Logging in using a different User Name.



Duplicate User Login Message



Message on Disconnected End Point

For other Emblaze-VCON and non-Emblaze-VCON end points, duplicate login attempts are rejected without explanation from the MXM.

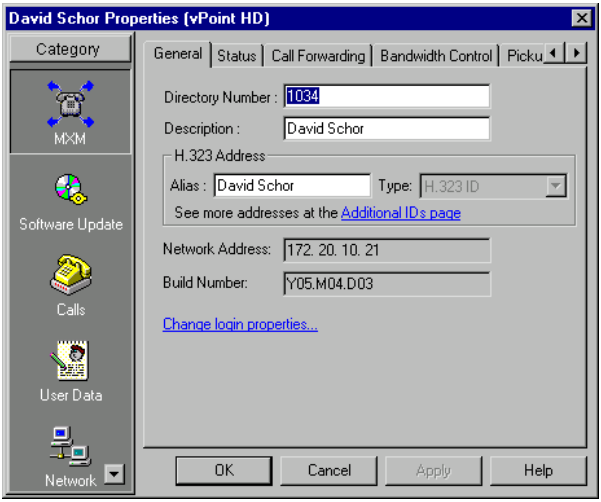
6.2 Setting End Point MXM Properties

The administrator can set MXM properties for all videoconferencing end points. MXM end point properties define how the end points operate as parts of the MXM videoconferencing network.

1. If an end point logs in during Closed Mode, the administrator can set these properties during the initial registration process or keep the default values.
2. The properties described in this section are applicable also to SIP User Agents (see Chapter 16, "Managing SIP Networks" on page 315).

General

The **General** tab contains identity information of the selected end point.



Typical Emblaze-VCON End Point - General Properties

The **General** Properties tab contains the following properties:

Directory Number	Internal directory number (E.164 number) assigned to the end point. Any other end point registered with this MXM can call this end point by dialing this number.
Description	Identity or description for the end point. This name will appear in the Main View after the login process is finished.
Alias	The end point's alias name.

Type The type of address used by the end point for registering with the MXM.

Additional IDs page Click this link to view any additional IDs that have been configured for this end point.

Network Address IP address of the end point.

The following settings are available for some types of end points.

Build Number Version information for the end point's videoconferencing application.

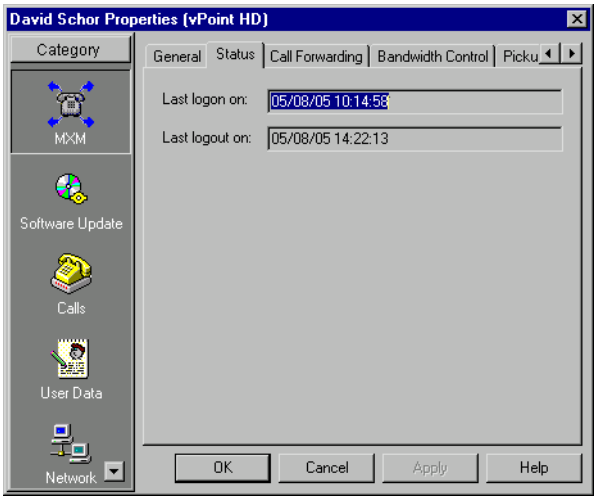
Change Login Properties For changing the end point's MXM login password. This change takes effect the next time the end point logs in.

1. In the **New** box, type a new password for the end point.
2. In the **Confirm** box, type the new password again.

Status

The **Status** tab displays the most recent dates that the selected node logged in and out of the MXM.

If the Last Login date is later than the Last Logout date, the selected node is currently logged into the MXM.

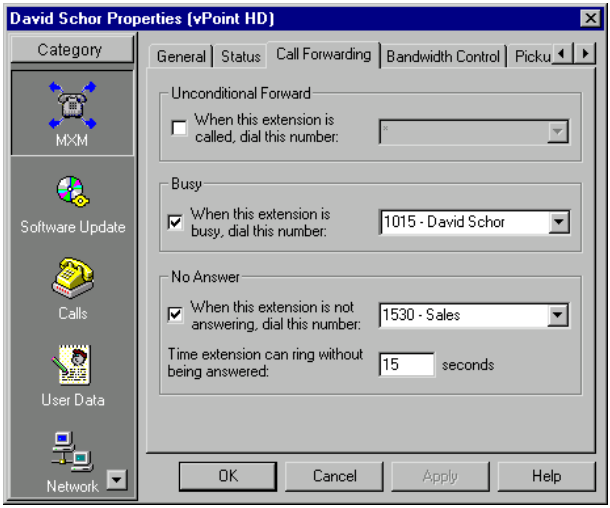


Typical Emblaze-VCON End Point - Status Properties

Call Forwarding

In the **Call Forwarding** tab, set alternate destinations for the MXM to route calls. Call forwarding for a specific node may be performed:

- ❑ At all times (unconditionally)
- ❑ If the node is busy in another videoconference
- ❑ If the call is not answered by the node.



Typical Emblaze-VCON End Point - Call Forwarding Properties

Set alternate destination numbers for the following conditions:

Unconditional Forward

When this extension is called, dial this number

Select this option to set an alternate destination for every call to this end point. In the list, choose the alternate destination. The forwarding occurs unconditionally and immediately.

If this option is selected, the **Busy** and **No Answer** options are not available.

Busy

When this extension is busy, dial this number

Select this option to set an alternate destination for a call if this end point is engaged in another call at the same time. In the list, choose the alternate destination. The forwarding occurs immediately.

No Answer

When this extension is not answering, dial this number

Select this option to set an alternate destination for a call if this node does not answer after a specified time. In the list, select the alternate destination.

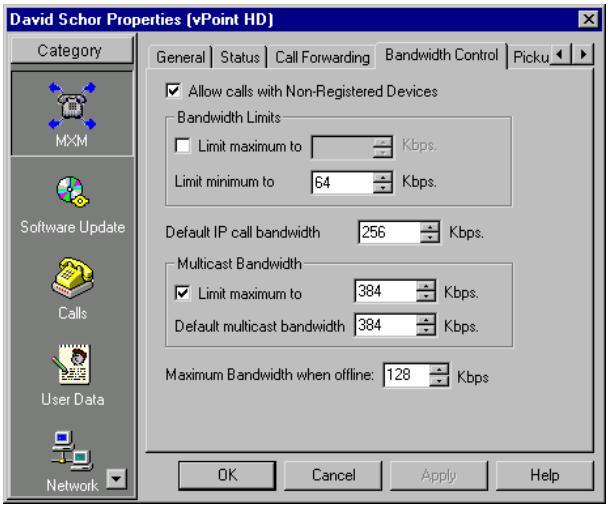
Time extension can ring without being answered

Type the number of seconds before the system forwards unanswered calls.

A "*" entry indicates that the particular forwarding setting is not active.

Bandwidth Control Properties

In the **Bandwidth Control** tab, you can define the permitted amount of bandwidth that the end point can use when communicating with others.



Typical Emblaze-VCON End Point - Bandwidth Control

Set bandwidth properties as follows:

Allow calls with Non-registered Devices — Select to enable this end point to engage in videoconferences with parties that are not listed or cannot register with the local MXM.

Limit Number of Concurrent Calls to — Select the number of calls that can go to or from the end point at the same time. This feature is available only to end points that support concurrent videoconferences.

Bandwidth Limits

Limit Maximum to — Select this option to define the highest amount of bandwidth that the end point may use. In the list, choose the bandwidth.

Limit Minimum to — Choose the lowest amount of bandwidth that the end point may use.

Default IP Call Bandwidth — This feature is applicable in vPoint and Falcon end points only.

Set the default bandwidth for calls initiated by this end point. Unless the bandwidth is changed before dialing, the outgoing call will use this bandwidth.

Multicast Bandwidth

This feature is applicable in vPoint 5.1 or higher, Desktop and MediaConnect 9000 end points only.

Limit Session to — Select this option to define a bandwidth limit for the end point's participation in an Interactive Multicast videoconference. The end point is not permitted to take part in a multicast session that exceeds this limit.

In the list, choose the bandwidth limit.

Default Multicast Bandwidth — The default bandwidth for Interactive Multicast sessions. The actual bandwidth will depend on the amount of available bandwidth during the session.

Maximum Bandwidth when Offline — Select this option to limit the amount of bandwidth that the selected end point may use if it's not logged in to the MXM. In the list, select a bandwidth.

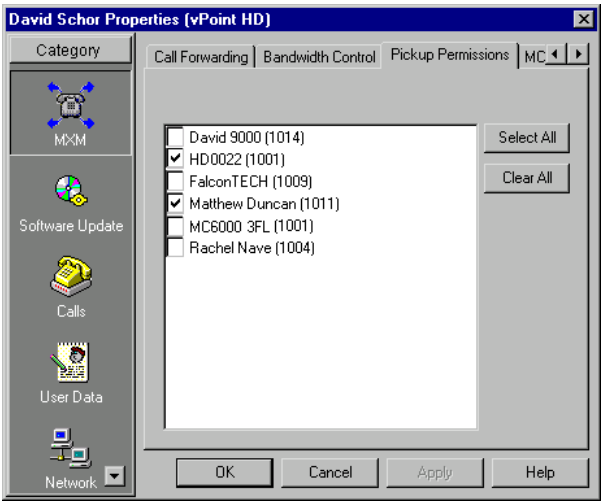
Pickup Permissions

In the **Pickup Permissions** tab, you can authorize other end points to answer a video meeting call to the selected end point. Only end points that are registered with the same MXM may receive pickup permission for each other.

For example, suppose Rachel is a video meeting call's destination. If David has pickup permission for Rachel's calls, he can answer this video meeting call.

In the list, select any number of end points that may pick up a call to this specific end point.

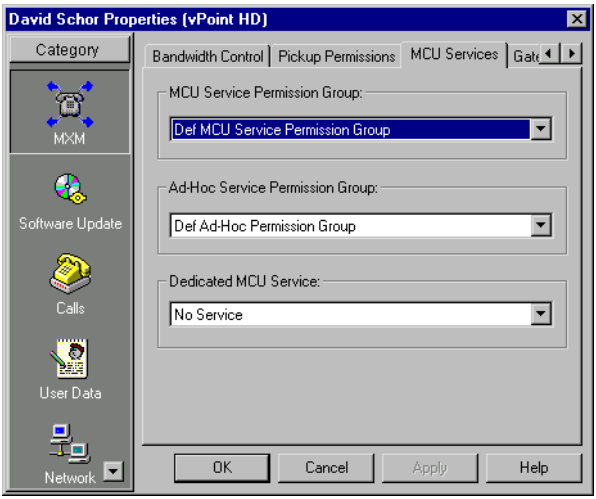
- To grant pickup permission to all end points in the list, click **Select All**.
- To clear all the selections, click **Clear All**.



Typical Emblaze-VCON End Point - Pickup Permissions

MCU Services

In the **MCU Services** tab, define bandwidth allocation policy for any multipoint conferences that this end point engages in.



Typical Emblaze-VCON End Point - MCU Services Properties

MCU Service Permission Group

Select the name of the MCU Service Permission group from which this end point can receive services. The available options are all MCU Service Permission groups that are listed in the Main View.

Ad-hoc Permission Group

Select the name of the Ad-hoc Permission Group from which this end point can choose a service for initiating an ad-hoc conference.

Dedicated MCU Service

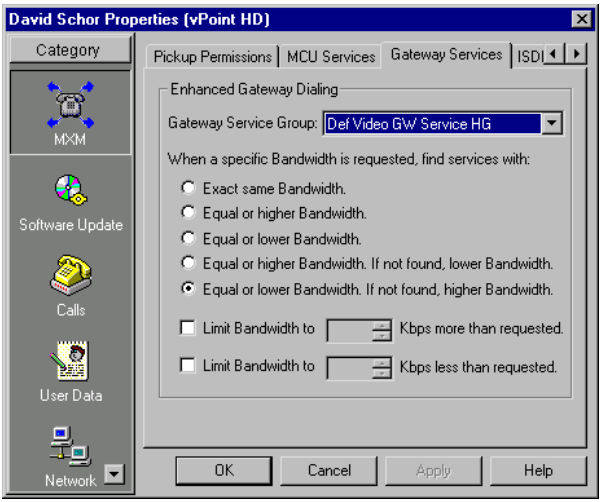
An ad-hoc service resource that may be used only if a specific end point is one of the parties of the resulting ad-hoc conference (either one of the original two end points of the conference or the invited end point).

If you want to dedicate a specific MCU or VCB service for this end point, select the service from the list.

To be a dedicated service, the service must be set up as an ad-hoc resource. See "Session" on page 158.

Gateway Services

In the **Gateway Services** tab, you can define bandwidth allocation policy for any MCU conferences or calls through a gateway that this end point engages in.



Typical Emblaze-VCON End Point - Gateway Services Properties

Set the Services properties as follows:

Gateway Service Group — Select the name of the gateway service hunting group from which this end point can receive services. If the end point dials the defined gateway access number (default is "**9**"), it may use any of the included services within that particular Service group.

The available options are all gateway service hunting groups that are listed in the Main View.

Some calls through the gateway may specify a required bandwidth. The following options define how the MXM allocates bandwidth in this situation:

Exact same bandwidth — Provide a choice only among services that provide the exact bandwidth required.

Equal or higher bandwidth — Provide a choice only among services that provide the exact bandwidth required or more.

Equal or lower bandwidth — Provide a choice only among services that provide the exact bandwidth required or less.

Equal or higher bandwidth - if not found, lower bandwidth	Provide a choice among services that provide the exact bandwidth required or more. If none exist, then offer services allocating lower than required bandwidth.
Equal or lower bandwidth - if not found, higher bandwidth	Provide a choice among services that provide the exact bandwidth required or less. If none exist, then offer services allocating higher than required bandwidth.
Limit bandwidth to ___ Kbps more (or less) than requested	Select the appropriate option to enable only a specific amount of deviation (higher or lower) from the requested bandwidth. From the appropriate list, choose the amount of deviation (in Kbps) allowed. For example, if you want to allow no more than an additional 128 Kbps, then choose **128** from the appropriate list.

ISDN Call Routing

In the **ISDN Call Routing** tab, define how the MXM decides how to route calls through gateways. The MXM can prioritize between several sets of gateway routing rules:

- Least Cost Routing Rules (see "Testing for the Optimal Gateway Service" on page 147)
- Bandwidth Rules (nodes' Properties **Services** tab - see "Gateway Services" on page 99)

Set ISDN Call Routing properties as follows:

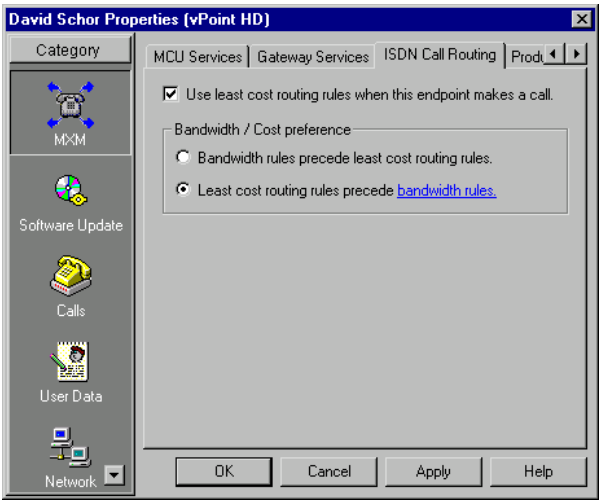
Use least cost routing rules when this end point makes a call	Select to allow the MXM to apply least cost routing to the end points' gateway calls.

Bandwidth/Cost Preference

Select one of the following:

Bandwidth rules precede least cost routing rules — When initiating a gateway call, the MXM chooses a gateway service based on the rules defined in the initiating end point's Service properties.

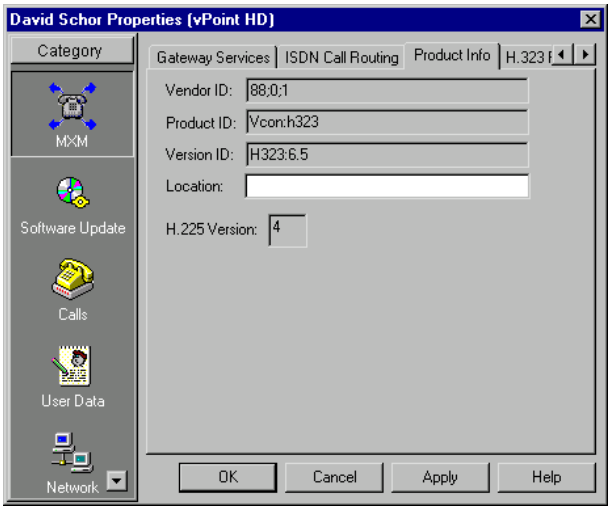
Least cost routing rules precede bandwidth rules — When initiating a gateway call, the MXM chooses the most efficient gateway service based on the application of the least cost routing rules.



Typical Emblaze-VCON End Point - ISDN Call Routing Properties

Product Info

The **Product Info** tab shows identification information about the end point's videoconferencing system's manufacturer and model.



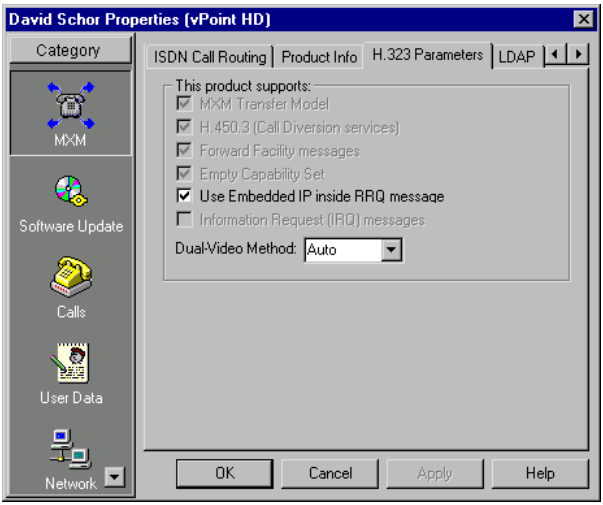
Typical Emblaze-VCON End Point - Product Information Properties

The tab provides the following information:

Vendor ID	Identity of the end point manufacturer
Product ID	Identity of the conferencing tool used by the end point.
Version ID	Version number of the videoconferencing tool, for identification purposes.
Location	Physical location of the end point.
H.225 Version	Protocol for control signaling in an H.323 conferencing environment.

H.323 Parameters

The **H.323 Parameters** tab shows which H.323 features are enabled in the selected end point.



Typical Emblaze-VCON End Point - H.323 Parameters Properties

Use Embedded IP Inside RRQ Messages

In response to registration requests (RRQ) from this end point, the MXM will send response to the IP address specified in the RRQ.

Dual-Video Method

Define the permitted method for transmitting dual video streams from this end point.

The H.239 standard enables end points to convert data into a separate media stream and transmit it parallel to the video stream. Video systems supporting H.239 display shared data and live video in separate windows. Systems not supporting H.239 display only the shared data in a single window.

- Choose **None** to block all dual video transmission.
- Choose **Non-H.239** to allow dual video transmission from this end point, although not using H.239.

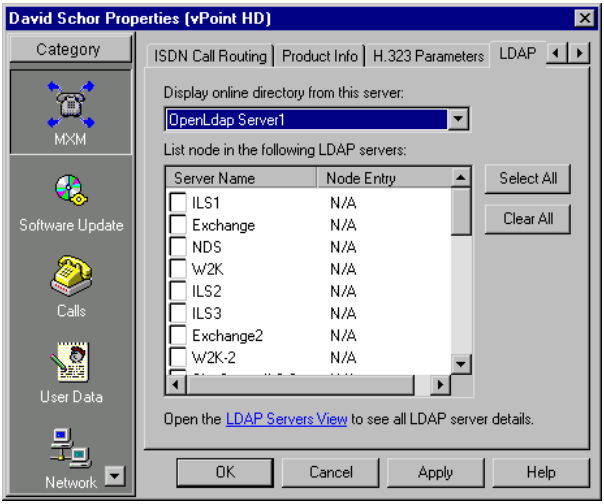
Dual-Video Method (cont.)

- ❑ Choose **Only H.239** to allow dual video transmission only if the end point supports H.239.
- ❑ Choose **Auto** to allow this end point to choose the method.

LDAP

The **LDAP** tab provides information about the end point's registration, if applicable, in LDAP (Lightweight Directory Access Protocol) servers based on the X.500 standard for directory services. LDAP servers (also known as online directories) are lists of contacts whose videoconferencing systems are online and registered with that directory.

End points may be registered in more than one LDAP server, on condition that the MXM is registered and configured in them.



Typical Emblaze-VCON End Point - LDAP Properties

Set the end point's LDAP configuration as follows:

Display Online Directory from this Server
The online directory that is available for this end point. The end point can dial any other videoconferencing user listed in this online directory.

List node in the following LDAP servers
Select LDAP servers that can contain the subdirectory in which the end point should be listed. End points may be registered in all LDAP servers in which the MXM is registered.

If the end point has been previously registered in an LDAP server, its entry name or number (node entry) appears in the list.

- To be listed in all LDAP servers (depending on MXM registration in them), click **Select All**.
- To clear all the selections, click **Clear All**.

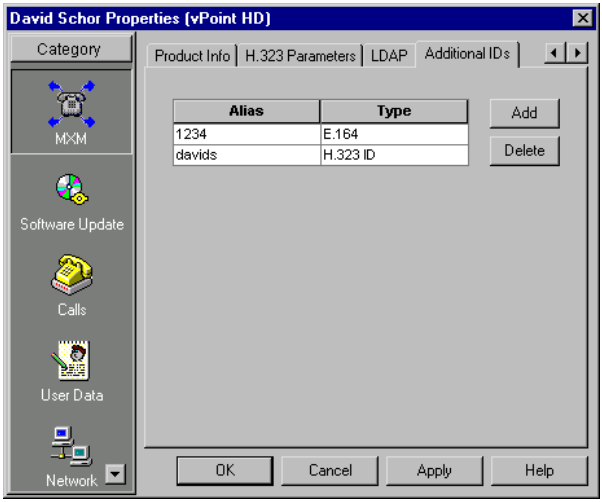
LDAP Servers View
Click this link to see location and access information about the available LDAP servers.

For more information about registering in LDAP servers, see Chapter 15, "Registering with LDAP Directories".

Additional IDs

In addition to its directory (E.164) number, a node may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** tab, you may enter these, if applicable.

For example, this feature supports the Multiple Subscriber Network (MSN) service, which assigns multiple phone numbers to one ISDN line. MSN is supported by some ISDN switches.



Typical Emblaze-VCON End Point - Additional IDs Properties

➤ To add additional IDs for a node

1. Click **Add** to display a table row.
2. In the **Alias** column, type the node's additional E.164 number, H.323 alias, URL, or e-mail address.
3. In the **Type** column, click and select the address type.

To delete an entry, click in its row and then click **Delete**.

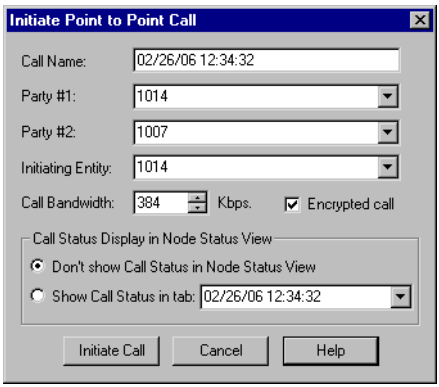
7 Initiating Videoconferences From the MXM Administrator

7.1 Administrator-Initiated LAN Dialing

As a system administrator with Super User or Monitor/View privileges, you can initiate a point-to-point videoconference by connecting two end points listed in the Administrator's Main View. Calls may also be initiated to end points in neighboring zones.

➤ To initiate a point-to-point call through the Administrator

1. Select the parties for the videoconference.
2. Right-click and then click **Initiate point-to-point call**.
3. Make any changes required in the call properties. Otherwise, leave the default settings. For a description of the properties, see "Setting Point-to-Point Videoconference Properties" on page 108.
4. Click **Initiate Call**.



Initiating a Point-to-Point Videoconference

Setting Point-to-Point Videoconference Properties

If necessary, change point-to-point videoconference properties before connecting the two end points.

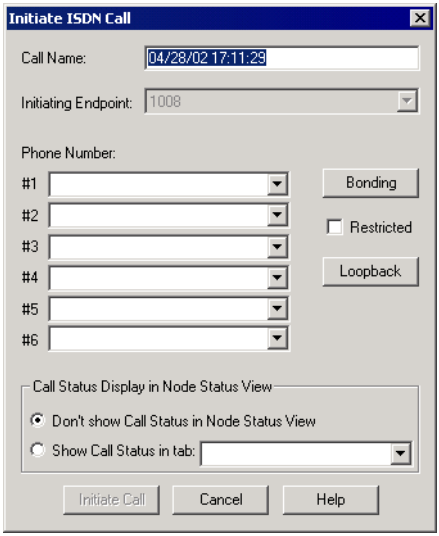
Call Name	Name of the videoconference. This name will identify this call in the CDR.
Party #1; Party #2	The two end points in the videoconference.
Initiating Entity	End point that dials to initiate the videoconference.
Call Bandwidth	Maximum bandwidth allocated for the videoconference
Encrypted Call	All Emblaze-VCON HD systems support the H.235 encryption standard. For calls involving two systems supporting H.235, this option is selected by default. If at least one of the end points do not support H.235, disable this option. Otherwise, the call will fail to connect.
Call Status Display in Node Status View	Select **Show Call Status in Tab** to display the call status in the Node Status View in a specific tab. The name or description listed here is also listed on the tab. Select **Don't show Call Status in Node Status View** if you don't want to monitor the videoconference in the Node Status View.

7.2 Administrator-Initiated ISDN Dialing

➤ To initiate an ISDN videoconference through the Administrator

1. Select the initiating party of the videoconference.
2. Right-click and then click **Initiate ISDN call**.
3. Set the call properties, including the ISDN numbers of the receiving party. For a description of the properties, see "Setting ISDN Videoconference Properties" on page 110.
4. Click **Initiate Call**.

If the call is successful, a notification, "**In ISDN Call: [*n*] kbps**" appears in the Main View next to the calling station's entry, where *n* indicates the call's bandwidth.



Initiating an ISDN Videoconference

Setting ISDN Videoconference Properties

Set ISDN videoconference properties before initiating the call.

Call Name	Name of the videoconference. This name will identify this call in the CDR.
Initiating End Point	End point that dials to initiate the videoconference.
Phone Numbers	The ISDN phone numbers to dial. Enter numbers corresponding to the number of lines and amount of bandwidth that the call will require.
Bonding	Click to make this conference a Bonding call. Bonding combines multiple ISDN lines into a single channel, effectively strengthening the signal.
Restricted	Select if the connection is over a Restricted network, which uses 56K switches (instead of 64K).
Loopback	Click to initiate a call to the end point's own ISDN lines. A loopback tests if the ISDN lines are functioning normally.
Call Status Display in Node Status View	Select **Show Call Status in Tab** to display the call status in the Node Status View in a specific tab. The name or description listed here is also listed on the tab. Select **Don't show Call Status in Node Status View** if you don't want to monitor the videoconference in the Node Status View.

7.3 Administrator-Initiated Hang Up

As a system administrator with Super User privileges, you can hang up open calls that include selected users or users within a selected group. For example, if more than one user in the Sales Administrative group are involved in videoconferences but you have to terminate all of that group's calls, select the Sales Administrative group object.

Although administrators with Monitor/View privileges may initiate videoconferences, they cannot hang up calls.

➤ To hang up calls through the Administrator

1. Select the end point(s) or group object that includes the users that you want to disconnect.

2. In the toolbar, click the Hang Up Calls button.

   All calls involving the selected users are therefore disconnected.

8 Remote Upgrade of Videoconferencing Devices Software

After your organization receives new versions or patches of certain Emblaze-VCON videoconferencing software applications, you can then install them on all registered end points that require the specific applications. The MXM's Remote Software Upgrade utility supports the following software products:

- vPoint HD, HD5000, HD4000
- vPoint 5.1
- Emblaze-VCON VCB
- MXM Administrator

The definition of a software upgrade progress requires the setting of five sets of properties. The Software Upgrade Wizard's steps enable you to:

- ❑ Select the application and version - Versions page (see "Selecting a Software Version" on page 115).
- ❑ Copy the upgrade to a target location in your network or on an FTP server - Upload page (see "Setting a Target Location for the Upgrade" on page 116)
- ❑ Set temporary alias and password for end points to access the upgrade file (for users not defined as "Administrators" on their computers) - Login page (see "Setting Up User Login" on page 118)
- ❑ Schedule the time for upgrading all or selected end points - Run page (see "Setting the Upgrade Schedule" on page 119)
- ❑ Confirm the upgrade task's properties and initiate the upgrade - Confirmation page (see "Confirm Upgrade Definition" on page 121).

The MXM enables you to monitor the software versions status for applicable end points throughout the network, making sure that all end points are working with the latest or most suitable software versions.

8.1 Defining a Software Upgrade

The Software Upgrade Wizard enables you to define properties such as application version, upload location, and scheduling.

➤ To set up the software upgrade

1. Make sure that the upgrade file is in an accessible location, such as a CD-ROM.
2. In the MXM Administrator, open the **MXM** menu and choose **Update Software**. The Software Update Wizard appears.
3. On the Versions page, click **Browse**. Locate and select the upgrade file.
4. Set properties according to your upgrading specifications. When you finish each page of the wizard, click **Next**. For explanations about the various Property pages, see "Setting Software Upgrade Properties" on page 114.
5. When you finish the last page, click **Finish**.

   The Software Upgrade task is set up and the upgrade process will proceed as defined.

8.2 Setting Software Upgrade Properties

The Software Upgrade Wizard guides you through the task of defining the upgrade process. The Wizard's steps enable you to:

- ❑ Select the application and version
- ❑ Upload the upgrade to an accessible target location in your network or on an FTP server
- ❑ Set login parameters for providing access to the software upgrade file
- ❑ Schedule the time for upgrading all or selected nodes that require the specific software application
- ❑ Confirm the upgrade task's properties.

Selecting a Software Version

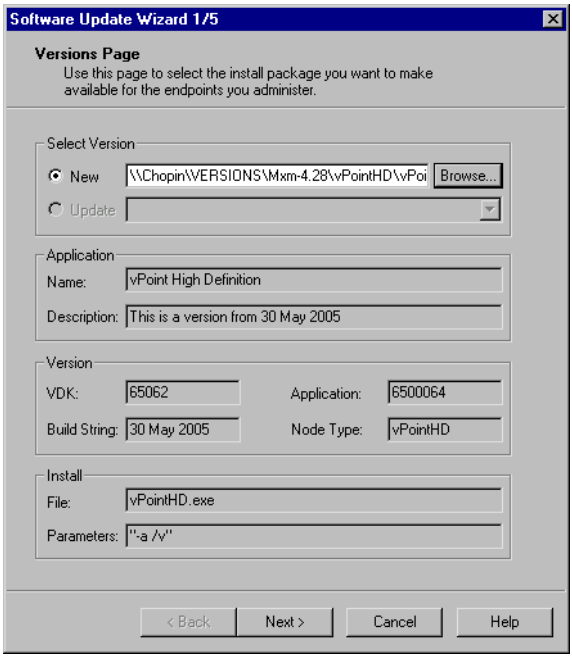
When you open the Software Upgrade Wizard, the Version page opens first.

Define whether this upgrading task will be New or an Update:

New — Click **Browse** to locate and select the application+version upgrade file. Emblaze-VCON supplies an XML file with its upgrades that define its version identification, installation requirements, and other information.

Update — If an update was previously performed, select the appropriate application description from this list. The description provides identification information for the required application version.

After selecting the upgrade file, the installation information appears on the Version Page.



Selecting Software Upgrade Application

Setting a Target Location for the Upgrade

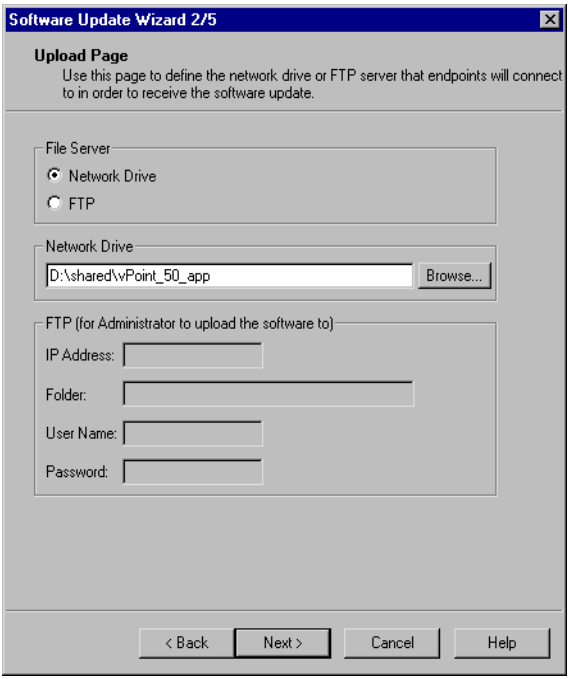
In the Software Upgrade Wizard's Upload page, set the location from which the upgrade is accessible for the relevant registered nodes.

File Server — Select to upload the upgrade file to either a **Network Drive** or **FTP** location. Depending on your choice, specify the exact access information in the relevant areas in the dialog box.

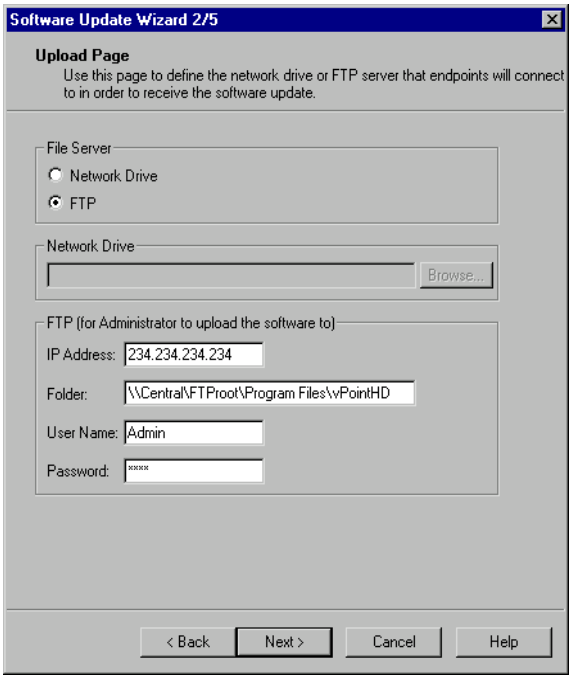
Network Drive — Select a folder on your organization's network for the upgrade file. Click **Browse** in the Network Drive area, then locate and select the location.

FTP — Type the path of a folder on an FTP server for the upgrade file.

Enter the login information (**Name**, **Password**, and **IP Address**) that the administrator must enter to upload the upgrade file to the FTP location.



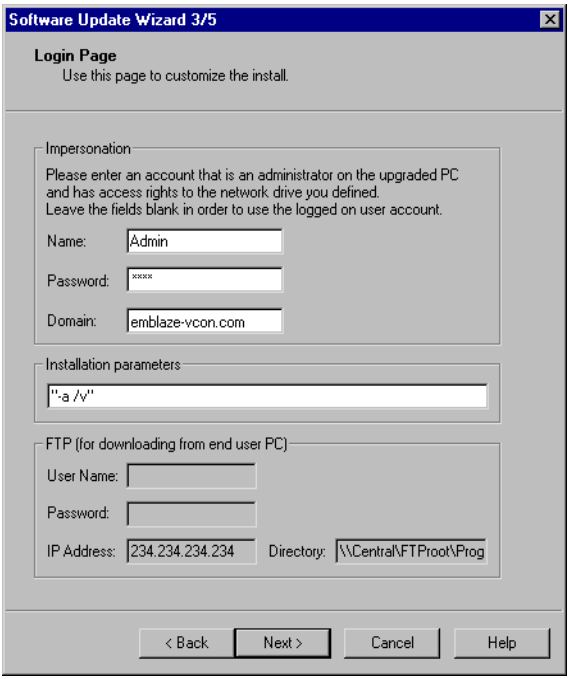
Setting Network Location for the Upgrade



Setting FTP Location for the Upgrade

Setting Up User Login

In the Login page, set the login parameters for providing access to the software upgrade file.



Setting Up User Login

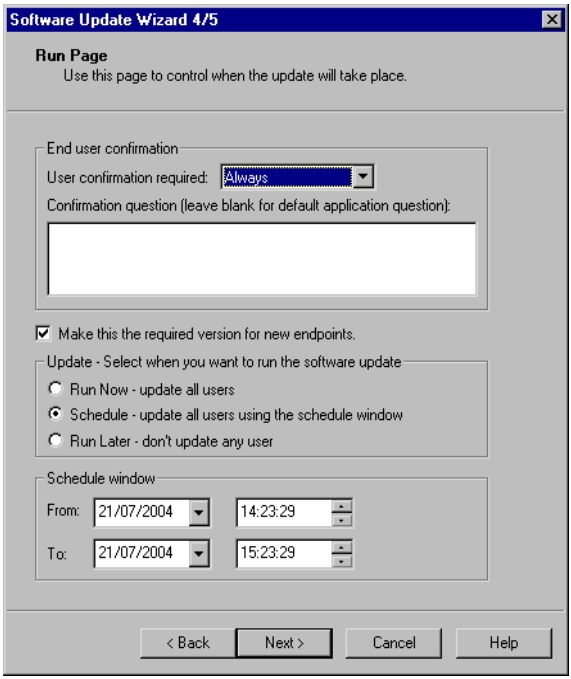
Impersonation Provide a **Name**, **Password**, and **Domain** of a Windows 2000/XP user that has Administrator privileges. This allows the server to perform the upgrade for client users that do not have sufficient privileges on their computers or the network.

Parameters Switches used to modify the installation command.

FTP ***For upgrading through an FTP server***
Provide a **Name** and **Password** for the MXM to use on behalf of the nodes in order to access the upgrade file.

Setting the Upgrade Schedule

In the Run Page, define the time for upgrading all registered nodes that require the specific software application.



Setting the Upgrade Schedule

End User Confirmation

User Confirmation Required

- Select **Always** to notify the node user that a newer version of the application is available, and to ask if the MXM should perform the upgrade now.
- Select **Only When In a Call** to wait for users engaged in videoconferences to hang up before notifying them that the software upgrade is available.
- Select **Never** to perform the upgrade without asking for the node user's permission.

Confirmation Question	Type the text that should appear in the Upgrade request on the node's screen (for example, "**Do you want to upgrade to the newest software version?**"). If this box is blank, a default text appears.
Make this the default version when a new end point logs in	Select to make this upgrade task the default for all new nodes (of the relevant node type) that register with the local MXM.

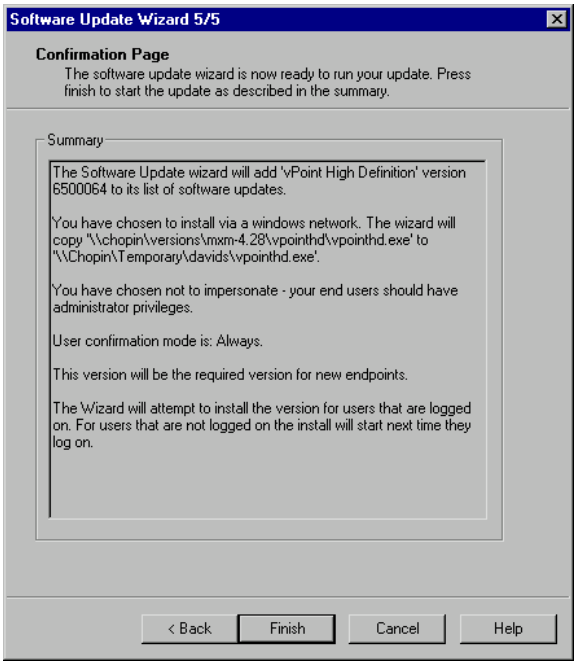
Update

Set the time to run the upgrade process.

Run Now (all users)	Select to initiate the upgrade process immediately after you finish defining it. The MXM starts the task of upgrading the software of all relevant logged in nodes. For offline nodes, their upgrade will be available the next time they log in to the MXM.
Schedule (all users)	Select to set a time period for initiating the upgrade process on all logged-in nodes (of the relevant node type). If offline nodes log in during this period, their applications will be updated too.
Run Later	Select if you want to run this upgrade process at a later, undefined time. When you exit the last page of this Wizard, this upgrade task, although defined, will not run until you initiate it a later time.
Schedule Window	This area is available if you selected **Schedule (all users)** above. In the **From** and **To** lines, set the time period for performing the upgrade process. In the Date box, choose a date. In the Time box, highlight the hour, minute, and/or seconds, and then press the up or down arrow buttons until the correct time appears.

Confirm Upgrade Definition

In the Confirmation page, confirm the upgrade task's properties. A summary describes the Property values that you set in the previous pages of the Software Upgrade Wizard.



Summary of Upgrade Task Definition

Click **Finish** to activate the upgrade task in the MXM's zone. If you defined a new upgrade task (see "Selecting a Software Version" on page 115), the MXM copies the upgrade file to the target location (defined in the Upload page - see page 116).

8.3 Selecting Nodes to Upgrade

If you schedule the software upgrade to Run Later (see "Setting the Upgrade Schedule" on page 119) at an undefined time, you can select specific nodes at a convenient time and run the upgrade process.

➤ To select nodes and run the upgrade process

1. In the Main View, select the specific nodes.
2. Right-click and then click **Update Software**. The Update Software Wizard appears.
3. Set the Upgrade properties according to your specifications. For descriptions of the properties, see the next section, "Node Software Upgrade Properties".
4. Click **OK** to start the upgrade process on the selected nodes.

Node Software Upgrade Properties

For node types whose software may be updated through the MXM, you can view and set upgrade properties for individual nodes.

➤ To access the Software Upgrade properties of individual nodes

1. In the Main View, select the specific end points.
2. Right-click the node(s), point to **Property** and **Software Update**, and then click the specific properties. The node's Properties dialog box opens to the property type that you clicked.

   -or-

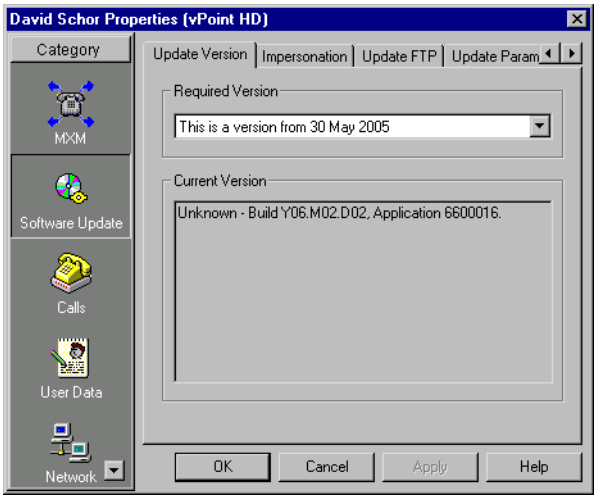
   Double-click the node, and then browse to the Software Update properties. Click the specific properties that you need.

The Software Upgrade Property pages are:

- Update Version
- Impersonation
- Update FTP
- Update Parameters
- Update Run

Update Version

The **Update Version** tab displays the name(s) of the required videoconferencing application for the end point and the currently installed videoconferencing application.



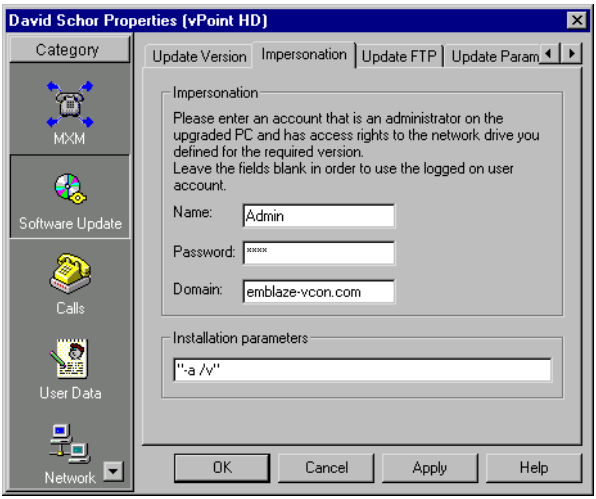
Software Upgrade Properties - Update Version

Required Version The version (as defined in the Software Upgrade task) that the end point will receive when an upgrade takes place. To change the version or the defined upgrade task, select it from the list.

Current Version Version currently running in the end point.

Impersonation

In the **Impersonation** tab, set the login parameters for providing access to the software upgrade file.



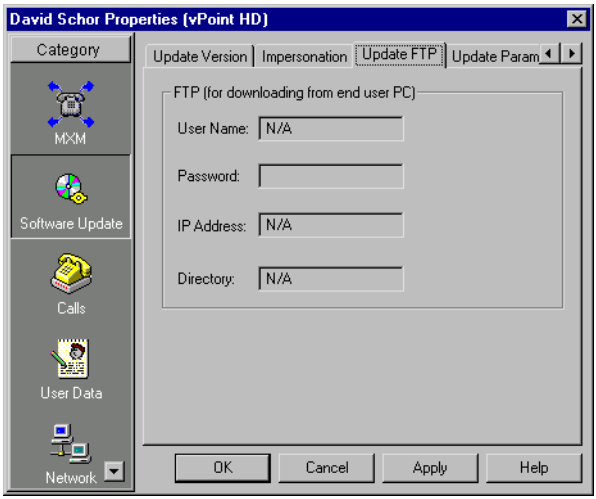
Software Upgrade Properties - Impersonation

Name, Password, Domain — The Name, Password, and Domain of a Windows 2000/XP/2003 user that has Administrator privileges. This allows the server to perform the upgrade for client users that do not have sufficient privileges on their computers or the network.

Installation Parameters — Switches used to modify the installation command.

Update FTP

The **Update FTP** tab contains the login parameters for providing access to the software upgrade file if it's located on an FTP server.



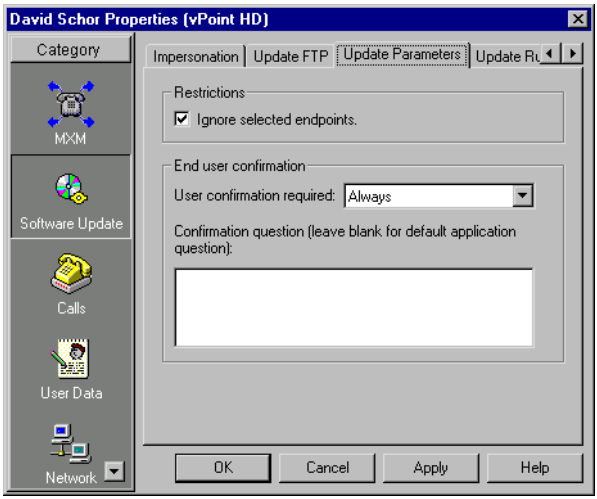
Software Upgrade Properties - Update FTP

Name, Password — The MXM uses these to log onto the FTP server, on behalf of the end points.

IP Address, Directory — Location of the upgrade file.

Update Parameters

In the **Update Parameters** tab, define node-specific properties for software upgrade procedures.



Software Upgrade Properties - Update Parameters

Restrictions

Ignore Selected End Points Select to prevent the software upgrade of the selected nodes.

End User Confirmation

User Confirmation Required

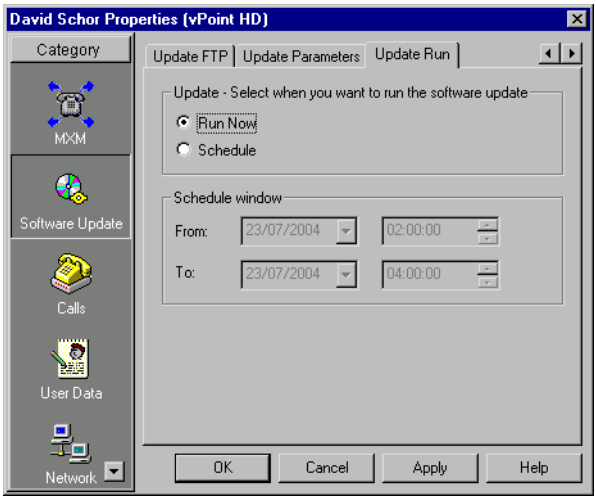
- ❑ Select **Always** to notify the node user that a newer version of the application is available, and to ask if the MXM should perform the upgrade now.
- ❑ Select **Only When In a Call** to wait for users engaged in videoconferences to hang up before notifying them that the software upgrade is available.
- ❑ Select **Never** to perform the upgrade without asking for the node user's permission.

Confirmation Question The text box displays the text that should appear in the Upgrade request on the end point's screen (for example, "**Do you want to upgrade to the newest software version?**").

If this box is blank, a default text appears.

Update Run

In the **Update Run** tab, define the time for upgrading the selected node's videoconferencing software.



Software Upgrade Properties - Update Run

Update

Run Now — Select to initiate the upgrade process after you finish defining it.

The MXM starts upgrading the software in all relevant logged in nodes. For nodes engaged in calls, their upgrade occurs after hangup. For offline nodes, their upgrade occurs the next time they log in to the MXM.

Schedule — Select to set a time period for initiating the upgrade preocess on all logged-in end points (of the relevant node type). If offline end points log in during this period, their applications will be updated too.

Schedule Window

This area is available if you selected **Schedule** above.

From, To — In these lines, set the time period for performing the upgrade process.

In the Date box, choose a date.

In the Time box, highlight the hour, minute, and/or seconds, and then press the up or down arrow buttons until the correct time appears.

8.4 Monitoring Software Upgrade Status

In the Main View, you can see which end points received the upgrades and which ones did not.

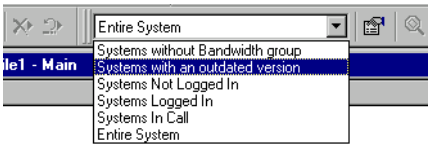
- Next to each applicable end point, an icon indicates if that end point is working with the latest available software version.

- The Event Log shows if the end point's software was upgraded.

Error Code	Details
1	Software agent will now run install, process=C:\DOCUME~1\
3103	Sending software upgrade message to Endpoint . Endpoint N
3111	Unrecognized Version for logged Endpoint. Endpoint Number

Event Log Details

- The Main View's "**Systems with an outdated version**" filter displays only end points that have not been upgraded yet (see "Filtering the Main View" on page 21).



"Systems with an Outdated Version" Filter

9 REGISTERING GATEWAYS

The MXM supports the use of H.323 gateways for connecting calls from registered end points to remote parties over ISDN networks. A gateway works as mediator between the two systems, translating between IP and ISDN protocols.

Each type of gateway has its own access number and dialing syntax. The dialing syntax usually includes the gateway's access number and the ISDN number of the remote party. For greater dialing flexibility, the syntax may also include delimiters.

Gateway services are also added to the MXM while gateways are granted login permission to the MXM. A gateway service defines the amount of available bandwidth and the type of information transmitted (such as voice only, video\voice, video\voice\data). One Gateway Service access number is created for each service type. At any time, you can add or edit available service entries from the Main View.

You can also organize sets of services within *Gateway Service Hunting Groups*. By associating end points with Gateway Service Hunting Groups, you can allocate available bandwidth to your organization's end points according to a certain resources allocation policy or geographic considerations. When an end point dials the Gateway access number, the MXM searches in the end point's Gateway services hunting group for an available service.

The registration and configuration procedures differ for Accord Gateways. For more details, see"Adding an Accord Gateway" on page 215.

9.1 Logging in a Gateway

A gateway cannot register automatically to the MXM. To accept the initial login attempt, the administrator must manually grant permission and then define its MXM properties.

➤ To register a gateway to the MXM

1. In the Gateway's configuration application, enter the IP address of the MXM and complete the appropriate commands to register.

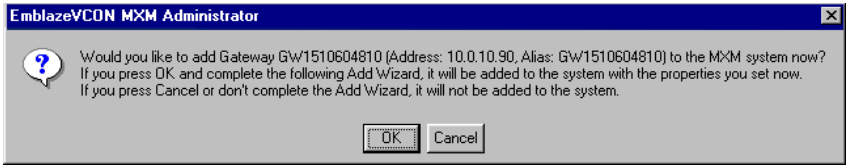
   In the MXM Administrator application, a Login Request notification appears on the Administrator tree.

2. Expand the Login Request item.

Login Request Notification for Gateway

3 Right-click the Gateway name and then click **Grant Login Permission**.

A message appears, asking if you want to register the gateway now.



Gateway Registration Request

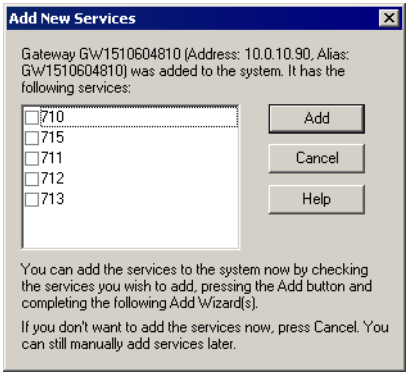
4 Click **OK** if you want to manually set the gateway's properties. The New Gateway Wizard appears. The original property values are the default values defined in the H.323 gateway template (see "Setting Up Templates" on page 47).

If you click **Cancel**, the gateway does not log in, but remains under the Login Requests object until you delete it (and the gateway stops trying to log in). See "Deleting a Login Request" on page 30.

5 Change properties according to your system specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see "Setting Gateway Properties" on page 132.

6 When you finish the last page, click **Finish**.

The Add New Services dialog box displays a list of all gateway services configured in the new gateway.



Adding Gateway Services

7 Select the services that will be available in the MXM's zone, and click **Add**.

The New Gateway Services wizard appears.

8 Define the gateway service properties according to your system and gateway specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see "Setting Gateway Service Properties" on page 139.

The wizard is repeated for each service that you selected in the previous step.

When logging in a Radvision viaIP gateway, the MXM takes service descriptions as they're defined in the viaIP's configuration program. Do not define descriptions for the services in the wizard or in the MXM afterwards.

In the viaIP configuration program, it is recommended to define service descriptions that include configuration information, such as the bandwidth.

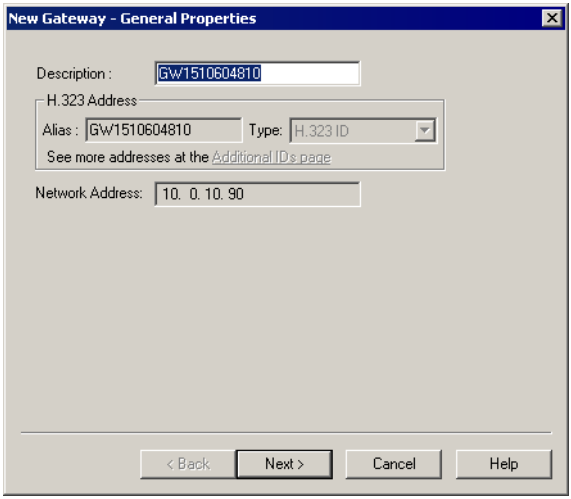
9 When you finish the last page, click **Finish**.

9.2 Setting Gateway Properties

In step 5 of "Logging in a Gateway" on page 130, the New Gateway Wizard provided the chance to change various gateway properties. This section describes these properties.

General

The **General** page contains identity information of the new gateway.



New Gateway - General Properties

The following information appears:

Description — Identity of the gateway. This name will appear in the Main View after the login process is finished.

H.323 Address

Alias — The gateway's alias name.

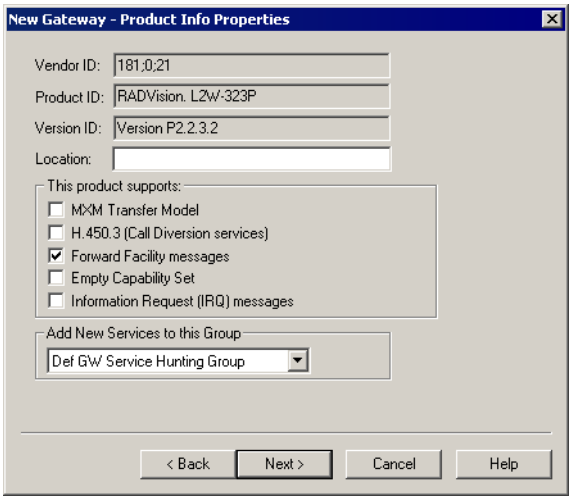
Type — The type of address used by the gateway for registering with the MXM.

Network Address — IP address of the gateway.

Changing the gateway's IP address must be done through its configuration utility. The address cannot be changed from the MXM.

Product Info

The **Product Info** page provides information about the gateway's manufacturer and model. In addition, you can enable or disable the exchange functionalities supported for videoconference calls through the gateway.



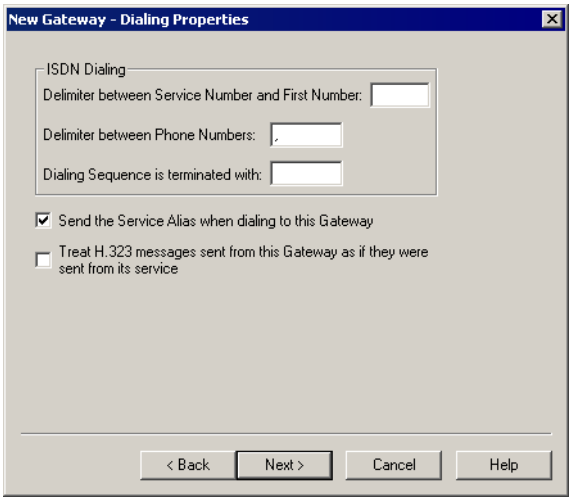
New Gateway - Product Information Properties

Vendor ID	Identity of the manufacturer.
Product ID	Manufacturer's identity of the gateway product.
Version ID	Manufacturer's version identification of the gateway product.
Location	Physical location of the gateway.
MXM Transfer Model	If selected, videoconferences through this gateway may be transferred to another end point.
H.450.3 (Call Diversion services)	If selected, calls through this gateway may be forwarded according to the capabilities of H.450.3. It provides additional information about forwarded calls than Forward Facility does, such as the original destination of the call.
Forward Facility messages	If selected, calls through this gateway may be forwarded according to Forward Facility capabilities. A forwarded call does not provide information about the redirection.
	If the selected gateway supports both H.450.3 and Forward Facility, we recommend enabling H.450.3.

Empty Capability Set	If selected, video and audio stream channels in a call are temporarily closed while a call transfer takes place. This option helps increase the speed of call transfer and ad-hoc videoconferences.
Information Request Messages (IRQ)	An IRQ is a request for status information from gatekeeper to terminal. If selected, the MXM can send IRQ messages checking if the gateway is online.
Add New Services to this Group	If a new gateway service is added to this gateway's configuration, it will automatically be included in the hunting group selected here. To avoid adding services to hunting groups automatically, select **No Group**.

ISDN Dialing

Dialing conventions vary among gateways, according to the vendor. Refer to your gateway's documentation for the specific delimiters or other characters that are required in order to access the gateway's services.



New Gateway - ISDN Dialing Properties

In the **Dialing** page, define the following information: .

ISDN Dialing

Delimiter between Service Number and First Number	Type the character, if applicable, that the MXM adds before the first ISDN number.
Delimiter between Phone Numbers	Type the character, if applicable, that the MXM adds between each ISDN number to be dialed.
Dialing sequence is terminated with	Type the character, if applicable, that the MXM must enter at the end of the dialing string.

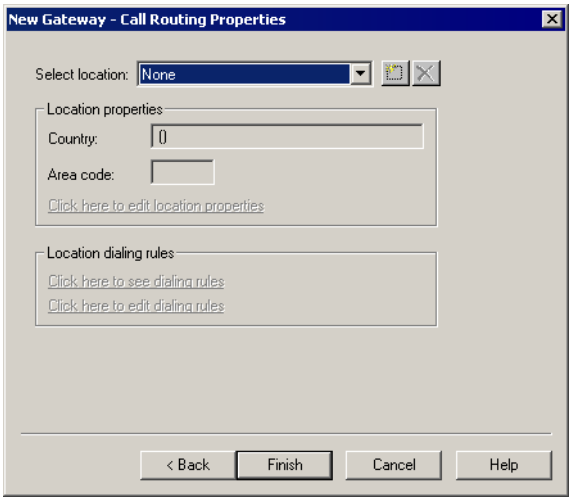
All of the above values must be identical to the dialing configuration of the Gateway

Send the Service Alias when dialing to this gateway	Video gateways support multiple services. If the gateway dialing syntax requires the inclusion of a service number, select this option.
Treat H.323 messages sent from this gateway as if they were sent from its service	Select this option if the new gateway does not define services. The MXM will handle messages sent through the gateway as H.323 64K Voice messages.

Call Routing

In the **Call Routing** page, enter the physical location of the gateway and define the cost rates for using the gateway's services.

When you run a Least Cost Routing test to find available gateway services and costs for a gateway call to a certain location, the resulting cost estimates will be based on the cost rates defined here (see "Testing for the Optimal Gateway Service" on page 147).

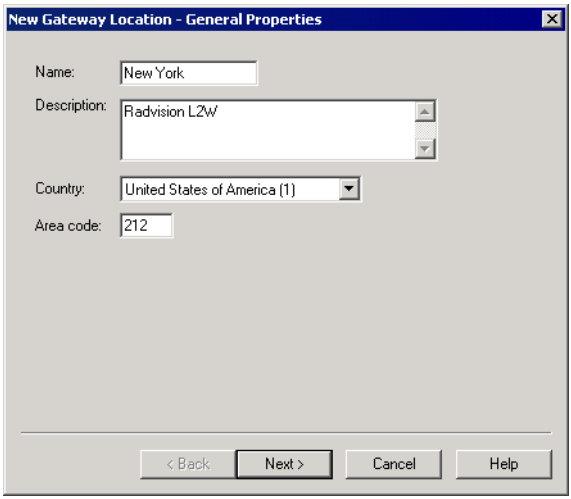


New Gateway - Call Routing Properties

➤ To add a gateway location

1. If the location does not appear in the **Select Location** list, click the **Add New Location** button. The New Gateway Location Wizard appears.

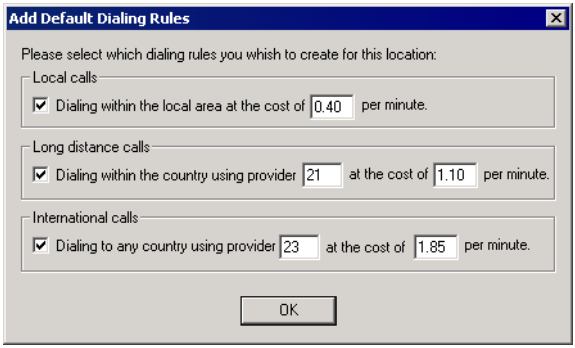
2. Enter a **Name** of the location and a **Description** (optional). Select a **Country** and enter the location's local **Area Code**.



New Gateway Location - General Properties

To go to the next page, click **Next**.

3 In the Add Default Dialing Rules dialog box, define the costs for calls through this gateway that originate in the MXM's zone.

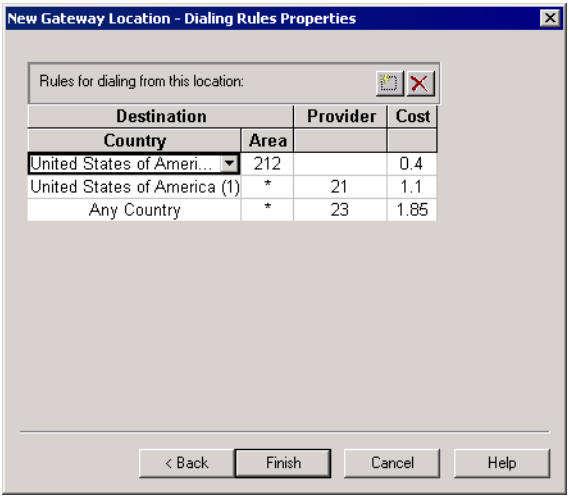


Select if MXM nodes may use this gateway for **Local**, **Long Distance**, and **International** calls, respectively.

Enter the rate (cost per minute) for each call type.

To go to the next page, click **OK**.

4 In the Dialing Rules page, a table lists the information that you provided in the previous step.



New Gateway Location - Dialing Rules

To add another rule, click the Add New Rule button and choose the appropriate call type (**Local**, **Long Distance**, and **International**).

To delete a rule, select that entry and click the Remove Rule button.

5 Click **Finish**. The gateway location now appears in the gateway's Call Routing Properties.

9.3 Setting Gateway Service Properties

Gateway services are added to the MXM during the gateway registration process. A gateway service defines the amount of available bandwidth and the type of information transmitted (video or voice - set in the gateway device's configuration).

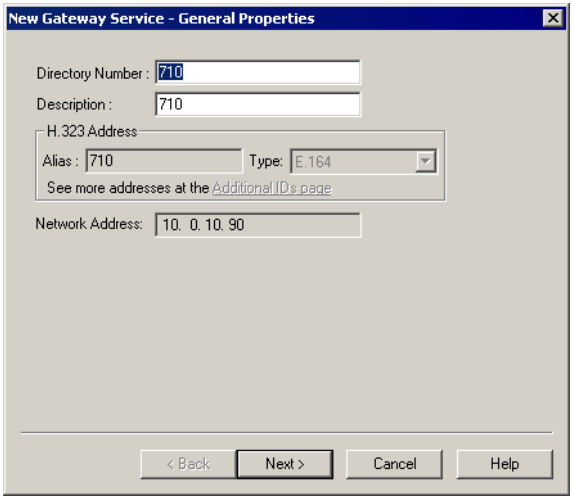
General

The **General** page contains identity information of the new gateway service.

When logging in a Radvision viaIP gateway, the MXM takes service descriptions as they're defined in the viaIP's configuration program. Do not define descriptions for the services in the wizard or in the MXM afterwards.

In the viaIP configuration program, it is recommended to define service descriptions that include configuration information, such as the bandwidth.

For all other gateways' services, you still have to manually define their descriptions in the MXM.



New Gateway Service - General Properties

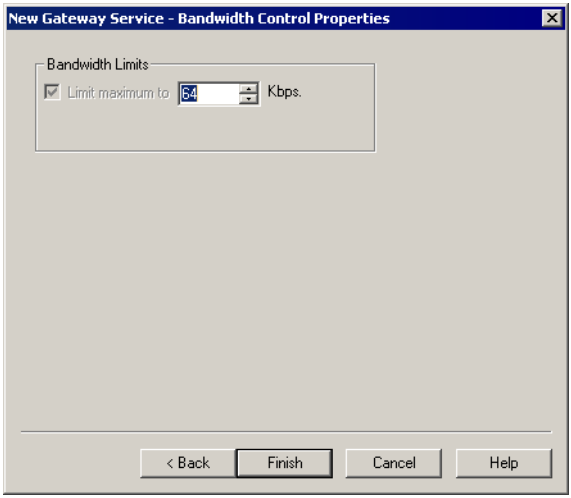
Define the following information:

Directory Number	Directory number of this service. This number will appear in the Main View after the login process finishes.
Description	Identity of the service.

Alias	The service's alias.
Type	The type of alias or address.
Network Address	IP address of the gateway.

Bandwidth Control

In the **Bandwidth Control** page, enter the exact bandwidth defined in the gateway's configuration.



New Gateway Service - Bandwidth Control Properties

9.4 Gateway Service Hunting Groups

A Gateway Service hunting group contains multiple gateway services that are available to particular end points when they start LAN to ISDN videoconferences. One Gateway Service Hunting Group can contain different bandwidths and different Gateway devices.

Every registered end point may be associated with a gateway services hunting group (see "Gateway Services" on page 99). When an end point dials the gateway access number, the MXM searches for the services available to its associated group.

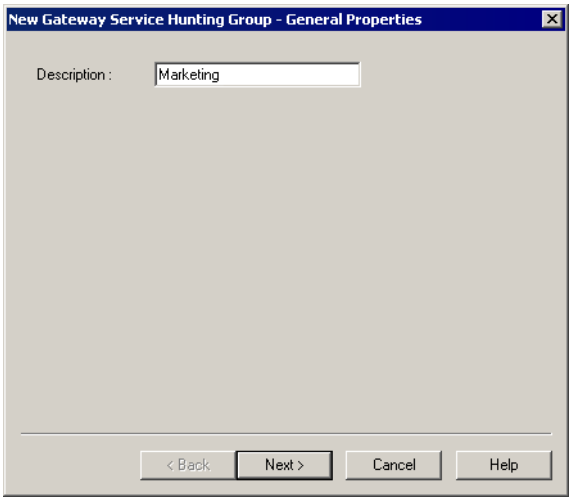
For example, if an end point specifies 384 Kbps bandwidth, the MXM checks in the associated hunting group if a gateway service providing 384 Kbps is permitted for the end point. If not, the MXM searches for the closest available service (in accordance to the end point's Service properties).

This ability can help you allocate available ISDN resources to various end points according to a certain resources allocation policy or geographic considerations.

➤ To set up a hunting group of gateway services

1 Click the **New Gateway Service Hunting Group** button.

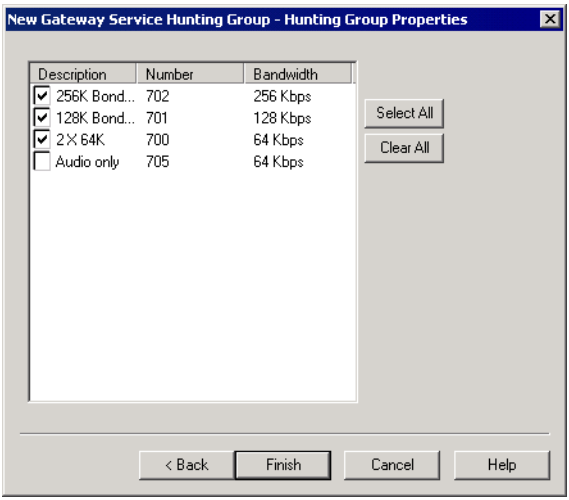
The New Gateway Service Hunting Group wizard opens to the General Properties dialog box.



Gateway Services Hunting Group - General Properties

2 In the **General** page, type a name for this hunting group in the Description box. This description appears in the MXM Administrator under the Gateway Service Hunting Group object.

Click **Next**. The Hunting Group Properties dialog box appears.



Gateway Services Hunting Group - Hunting Group Properties

3 Select any number of services from the list to be in the hunting group. The selected services will be the only ones available to associated end points.

— To place all services in the hunting group, click **Select All**.

— To clear all the selections, click **Clear All**.

4 Click **Finish** to implement the settings and close the dialog box.

10 Least Cost Routing of Gateway Calls

Least cost routing automatically connects an outgoing ISDN or IP-to-ISDN call with the least expensive gateway service to the target location at that time of day. Depending on the locations of the registered gateways, long-distance calling costs can be reduced significantly.

For example, suppose that a user in Hong Kong wants to videoconference with someone in Canada. If the call is initiated over a LAN through a registered gateway located in the USA, the initiator in Hong Kong is charged for a call from the USA to Canada, instead of from Hong Kong to Canada.

If the most efficient service is not available, least cost routing will try to pass the call through the next most-efficient service, or it will give the caller a busy signal.

In the MXM Administrator, you can check and compare the costs of IP-to-ISDN calls from the MXM's zone to destinations using registered gateway services. This allows you to apply the most cost-efficient connections for these calls.

Setting up and using least cost routing requires a combination of procedures in the MXM Administrator:

1. In the MXM's ISDN Call Routing Properties, set the location of the MXM and define the prefixes required for dialing (see "Setting ISDN Call Routing Properties" on page 144).
2. In the appropriate Gateway's Call Routing Properties, set the location of the gateway and enter the costs for dialing through it (see "Setting Gateway Call Routing Properties" on page 145).
3. Select registered end points and access their MXM ISDN Call Routing Properties. Select the preference of using Least Cost Routing rules or Bandwidth rules for routing calls (see "Setting Preference of Using Least Cost Routing or Bandwidth Rules" on page 145).
4. Before initiating a gateway call from a registered end point, test the Least Cost Routing rules to select the least expensive gateway and service available ("Testing for the Optimal Gateway Service" on page 147).

10.1 Setting ISDN Call Routing Properties

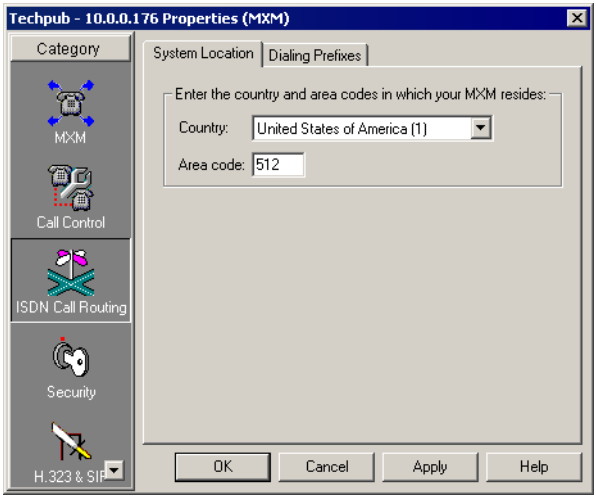
One of the factors that determine the costs of ISDN calls is the location of the end points on the network. You must enter this information in the MXM's System Properties in order to test and implement least cost routing.

In addition, you must enter the prefixes required by the local telephone company or ISDN provider for dialing international and long distance destinations.

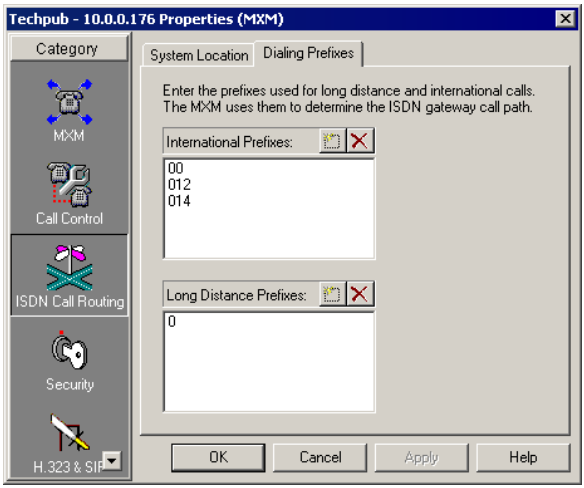
➤ To set the location and define the prefixes

1. Right-click the local MXM object, point to **Property** and then **ISDN Call Routing**, and click **System Location**. The **System Location** tab appears.
2. Enter the country and area code in which the local MXM is located and click **Apply**.
3. Click the **Dialing Prefixes** tab.

4. Click the New Prefix button.
5. Type the prefix and press <Enter>.
6. To enter more prefixes, repeat steps 1 and 2 as many times as required.
7. Click **OK** to implement the settings and close the dialog box.



Local MXM Location



Gateway Dialing Prefixes for Local MXM Network

10.2 Setting Gateway Call Routing Properties

In the registered gateways' **Call Routing** Properties, enter the physical location of the gateway and define the cost rates for using the gateway's services.

When you run a Least Cost Routing test to find available gateway services and costs for a gateway call to a certain location, the resulting cost estimates will be based on the cost rates defined here (see "Testing for the Optimal Gateway Service" on page 147).

For the complete Call Routing procedure, see "Call Routing" on page 136.

10.3 Setting Preference of Using Least Cost Routing or Bandwidth Rules

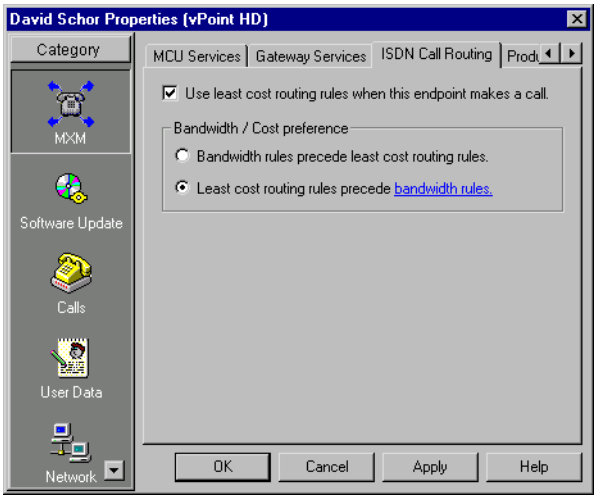
The MXM provides various rules for deciding how to route calls through gateways:

- Least Cost Routing Rules
- Bandwidth Rules (nodes' Properties **Services** tab - see "Gateway Services" on page 99)

When gateway calls are initiated, the MXM applies the rules in accordance to the ISDN Call Routing properties of the initiating end point. These settings are located in nodes' MXM Properties.

➤ To select the preferred set of rules

1. Select the nodes that will be affected by the rule preference.
2. Right-click, point to **Properties** and then **MXM**, and click **ISDN Call Routing**. The **ISDN Call Routing** tab appears.



H.323 End Point - ISDN Call Routing Properties

3. Select **Use least cost routing rules when this end point makes a call**. This selection allows the MXM to apply least cost routing to the end points' gateway calls.
4. Select a preference for applying rules:

Bandwidth rules precede least cost routing rules	When initiating a gateway call, the MXM first searches for gateway services that meet the criteria defined in the initiating end point's Service properties.
Least cost routing rules precede bandwidth rules	When initiating a gateway call, the MXM chooses the most efficient gateway service based on the application of the least cost routing rules.

5. To implement the changes and close the dialog box, click **OK**.

10.4 Testing for the Optimal Gateway Service

The ISDN Dialing Simulator enables you to find the most cost-efficient gateway services available for registered end points. The results are based on gateway services that meet the criteria defined in:

- The end points' ISDN Call Routing Properties (see page 100)
- The end points' Gateway Services Properties (see page 99)
- The gateways' Call Routing Properties (see page 136).

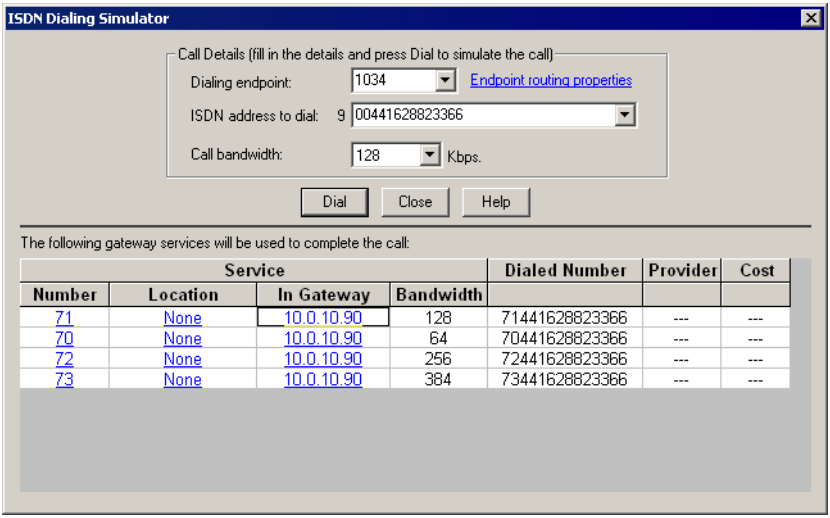
For example, suppose that you allocate a maximum bandwidth of 256K for calls from Hong Kong to Canada. The initiating end point is allowed to use bandwidths equal or lower than the requested one. In addition, least cost rules were enabled for the end point. After you enter the required information in the Simulator, it will display a table of gateway services available to the end point and their costs, sorted by cost. The MXM initiates dialing through the cheapest route first, trying all routes, if necessary, until the call connects successfully.

➤ To test the least-cost-routing rules

1. Right-click the node that will initiate the call and then click **Test Least Cost Routing Rules**. The ISDN Dialing Simulator appears.
2. Based on the information that you enter, the simulator will provide possible gateway services and their costs for calling your destination. Enter the following details:

Dialing End Point	The initiator of the call. Click **End Point Routing Properties** to view or change the end point's ISDN routing properties before testing.
Dialed ISDN Address	The phone number of the destination node.
Call Bandwidth	The maximum bandwidth required for the call.

3 Click **Dial**. The available registered gateway services appear in the table. The most cost-efficient service appears first in the table, followed by lesser efficient ones until the most expensive service, which appears at the bottom of the table.



ISDN Dialing Simulator

11 Registering an MCU

The Emblaze-VCON MXM supports the use of Multipoint Control Units (MCU) for connecting registered end points with a number of other end points in a multipoint videoconference.

For Accord MGC users

The operation of Accord MGC in conjunction with the MXM requires a special configuration. For more information, see Chapter 13, "Using Polycom® MGC™ with the MXM".

11.1 Logging in a New MCU

If the MXM is in Open Mode for MCUs, any MCU that attempts to register is automatically logged in.

If the system is in Closed Mode for MCUs, an MCU must be granted login permission by an administrator with Super User privileges. During this process, the administrator must define or confirm the MCU's MXM properties.

➤ To register an MCU to the MXM

1. In the MCU's configuration application, enter the IP address of the MXM and complete the appropriate commands to register.

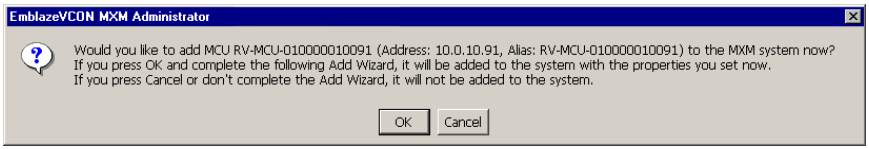
   If the MXM is in Closed Mode for MCUs, a Login Request notification will appear on the Administrator tree after several seconds.

2. Expand the Login Request item.

Login Request Notification for MCU

3. Right-click the MCU name and then click **Grant Login Permission**.

   A message appears, asking if you want to register the MCU now.



MCU Registration Request

4. Click **OK** if you want to manually set the MCU's properties, such as exchange function capabilities (Product Info). The New MCU Wizard appears. The original property values are the default values defined in the H.323 MCU template (see "Setting Up Templates" on page 47).

   If you click **Cancel**, the MCU does not log in, but remains under the Login Requests object until you delete it (and the MCU stops trying to log in). See "Deleting a Login Request" on page 30.

5. Change properties according to your system specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see "Setting MCU Properties" on page 151.

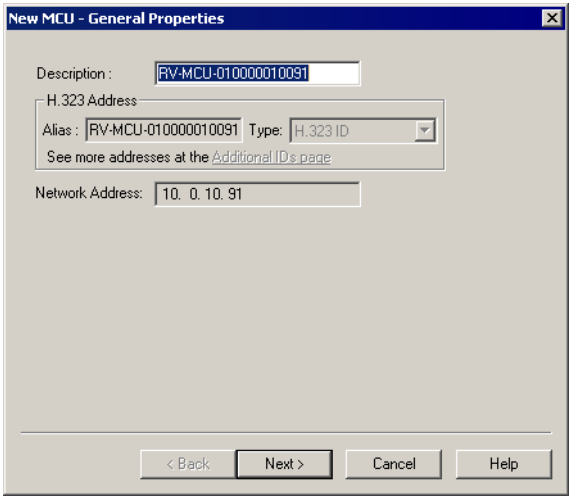
6. When you finish the last page, click **Finish**.

11.2 Setting MCU Properties

In step 5 of "Logging in a New MCU" on page 150, the Add Wizard provided the chance to change various MCU properties. This section describes these properties.

General

The **General** page contains identity information of the new MCU.



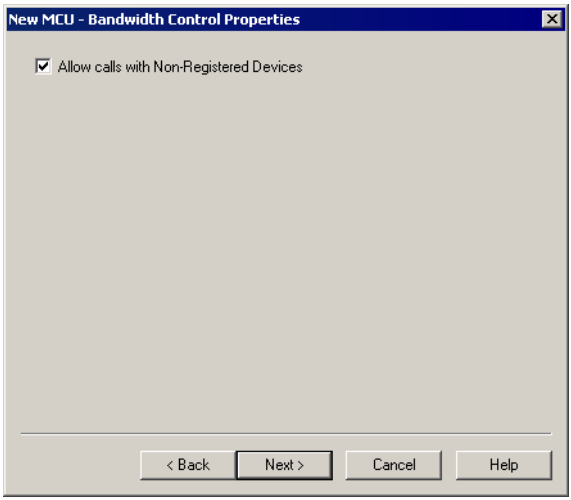
New MCU - General Properties

In the **General** Properties tab, the following properties appear:

Description	Identity of the MCU. This name will appear in the Main View after the login process is finished.
Alias	The MCU's alias name.
Type	The type of address used by the MCU for registering with the MXM.
Network Address	IP address of the MCU. Changing the MCU's IP address must be done through its configuration utility. The address cannot be changed from the MXM.

Bandwidth Control

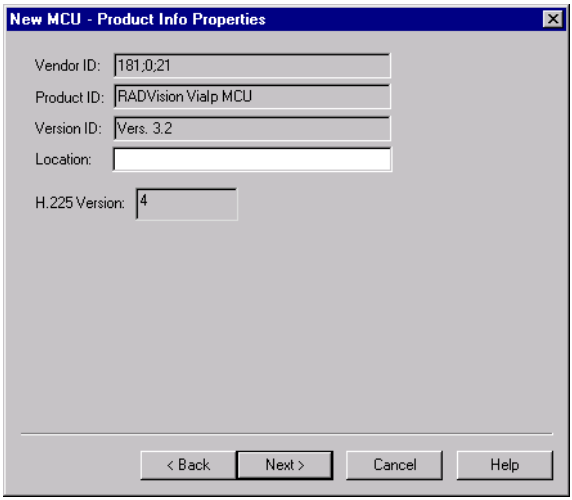
In the **Bandwidth Control** page, select **Allow calls with Non-registered Devices** to allow non-registered devices to participate in any multipoint videoconferences managed by this MCU.



New MCU - Bandwidth Control Properties

Product Info

The **Product Info** page provides information about the MCU's manufacturer and model.

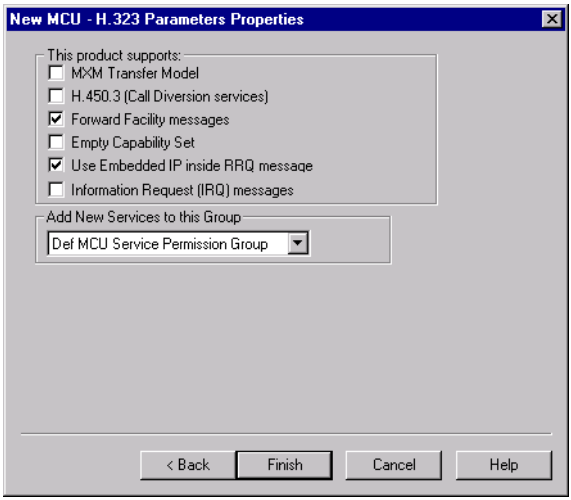


New MCU - Product Info Properties

Vendor ID	Identity of the manufacturer.
Product ID	Manufacturer's identity of the MCU product.
Version ID	Manufacturer's version identification of the MCU product.
Location	Physical location of the MCU.
H.225 Version	Protocol for control signaling in an H.323 conferencing environment.

H.323 Parameters

In the **H.323 Parameters** page, you can enable or disable the exchange functionalities supported for multipoint videoconferences through the MCU.



New MCU - H.323 Parameters Properties

MXM Transfer Model — If selected, videoconferences through this MCU may be transferred to another end point.

H.450.3 (Call Diversion services) — If selected, calls through this MCU may be forwarded according to the capabilities of H.450.3. It provides additional information about forwarded calls than Forward Facility does, such as the original destination of the call.

Forward Facility messages — If selected, calls through this MCU may be forwarded according to Forward Facility capabilities. A forwarded call does not provide information about the redirection.

If the selected MCU supports both H.450.3 and Forward Facility, we recommend enabling H.450.3.

Empty Capability Set — If selected, video and audio stream channels in a call are temporarily closed while a call transfer takes place. This option helps increase the speed of Call Transfer and Ad-hoc Videoconferences.

Use Embedded IP Inside RRQ Messages	In response to registration requests (RRQ) from this MCU, the MXM will send response to the IP address specified in the RRQ.
Information Request Messages (IRQ)	An IRQ is a request for status information from gatekeeper to terminal. If selected, the MXM can send IRQ messages checking if the MCU is online.
Add New Services to this Group	If a new MCU service is added to this MCU's configuration, it will automatically be included in the permission group selected here.

11.3 MCU Services

MCU Services define the MCU resources used during a multipoint videoconference.

A registered MCU's services are automatically listed in the MXM Administrator after the particular MCU is granted login permission to the MXM. One directory number is created for each service type. At any time, you can edit service entries from the Main View.

For Accord MGC users

In the Accord MGC, MCU services are provided through Meeting Rooms. For information about defining Meeting Room properties, see "Setting Meeting Room Properties" on page 212.

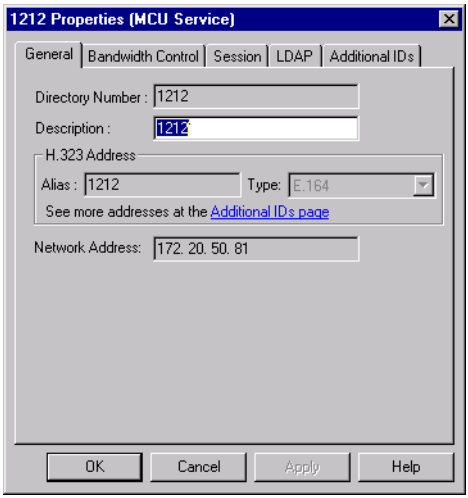
➤ To view or edit MCU Services

1. Double-click an MCU Service node. The specific service's Properties dialog box appears.
2. Define the MCU Service properties according to your system and MCU specifications, or keep the default settings.
3. To implement the changes and proceed to another tab in the dialog box, click the appropriate tab.
4. To implement all the changes and close the dialog box, click **OK**.

The following subsections describe the MCU Service properties.

General

The **General** tab contains identity information of the new MCU Service.



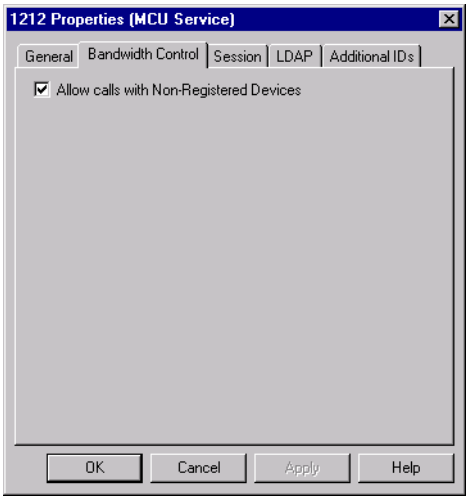
MCU Service - General Properties

In the **General** tab, the following properties appear:

Directory Number	Number to be dialed for using this service.
Description	Name of the service. This name will appear in the Main View after the login process is finished.
Alias	The MCU's alias as it is defined by its operating system.
Type	The type of address used by the MCU for registering with the MXM.
Additional IDs page	Click this link to view any additional IDs that have been configured for this MCU.
Network Address	IP address of the MCU. Changing the MCU's IP address must be done through the its configuration utility. The address cannot be changed from the MXM.

Bandwidth Control

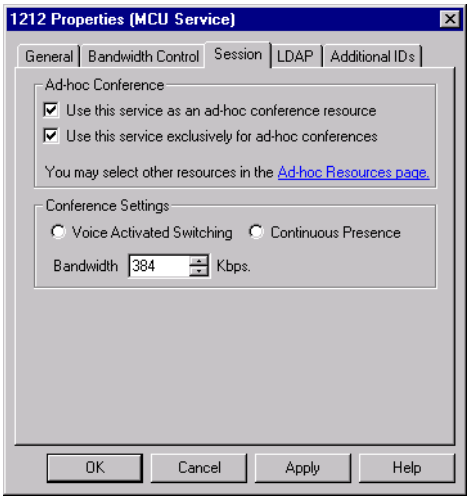
In the **Bandwidth Control** tab, select **Allow calls with Non-registered Devices** to allow non-registered devices to participate in any multipoint videoconferences using this MCU service.



MCU Service - Bandwidth Control Properties

Session

The **Session** tab contains settings which control the broadcast and display of an multipoint session.



MCU Service - Session Properties

Ad-hoc Conference

A point-to-point conference becomes an ad-hoc conference when additional end points are "invited" by one of the parties and they join the session. You can make this MCU Service available for use in ad-hoc conferences. This availability may be in addition to basic multipoint videoconferencing or exclusive for ad-hoc conferences.

Use this service as an ad-hoc conference resource

Select to make this service available for use when expanding to an ad-hoc videoconference.

If this service will be a Dedicated Service for a specific end point (see "MCU Services" on page 98), this option must be selected. The specific end point must either be one of the original two end points of the conference or the invited end point.

Use this service exclusively for ad-hoc conferences	Select to make this service available only for inviting additional users into ad-hoc videoconferences, but not available for initiating multipoint sessions.
Ad-hoc Resources page	Click this link to open the MXM's Ad-hoc Resources Properties, in which you can also select which MCU Services may be used for ad-hoc videoconferences (see "Ad-hoc Resources" on page 74).

Conference Settings

Voice Activated Switching	The participants see the video of the participant whose audio signal is strongest. For example, the non-speaking participants see the person speaking.
Continuous Presence	Several participants in a multipoint conference are viewed and heard simultaneously.
Bandwidth	The bandwidth available for each participant.

LDAP

The **LDAP** tab provides information about the MCU service's registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes' LDAP Properties, see "LDAP" on page 104.

Additional ID

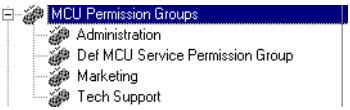
In addition to its directory (E.164) number, an MCU service may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** page, you may enter these, if applicable. For more information about adding Additional IDs, see "Additional IDs" on page 106.

11.4 MCU Service Permission Groups

An MCU Service Permission group is a set of MCU services that may be used by specific nodes. Its purpose is to control the use of MCU resources among an organization's end points.

An MCU Service Permission group may consist of one service, multiple services, or all available services. It may also include combinations of services from more than one registered MCU. In addition, you can define the automatic addition of new MCU services to a specific permission group (see "H.323 Parameters" on page 154).

By default, every registered end point is assigned to the default permission group. This may be changed when manually adding a new end point, or by editing the end point's properties (see "Gateway Services" on page 99). An end point is only permitted to use those services listed in its assigned permission group. If it attempts to dial a service not listed in its group, the MXM rejects the call.



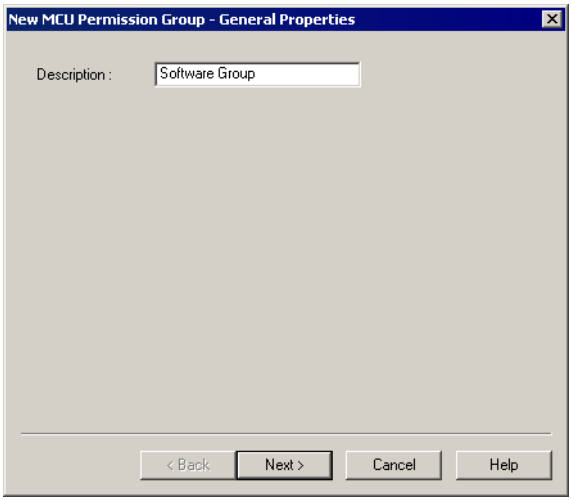
MCU Service Permission Groups in the Administrator Window

➤ To create an MCU Service Permission Group

1. Click the New MCU Permission Group button. The New MCU Permission Group dialog box appears.
2. Change properties according to your permission group requirements. To move to the next properties page, click **Next**. For explanations about the various properties, see pages 161 to 162.
3. Click **Finish**. In the Main View, the new group appears under the MCU Service Permission Group object.

General

In the **Description** box, type a name for the MCU Service Permission Group. This name will appear on the system tree and in nodes properties **MCU Services** tabs.



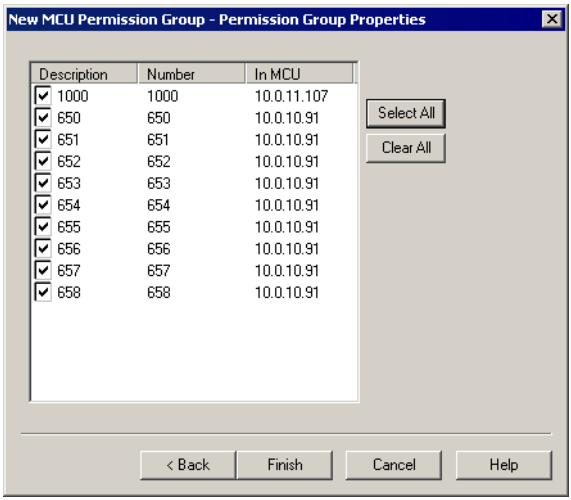
New MCU Permission Group - General Properties

Permission Group

The **Permission Group** Properties page includes all registered services from all registered MCUs.

Select any number of services from the list to be in the permission group. The group may also include combinations of services from more than one registered MCU.

- To place all services in the permission group, click **Select All**.
- To clear all the selections, click **Clear All**.



New MCU Permission Group Properties

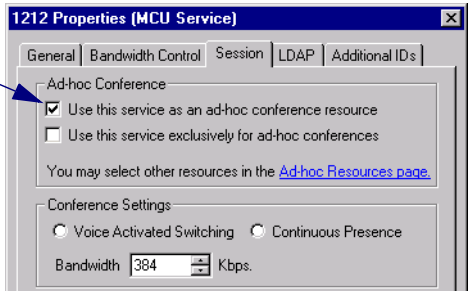
11.5 Dedicated MCU Services

A dedicated MCU service is set up only for expansion to an ad-hoc conference that includes a specific end point. That is, the service is "dedicated" to that end point. That specific end point must be either one of the original two end points of a point-to-point conference or the invited end point.

➤ To dedicate a service to a specific end point

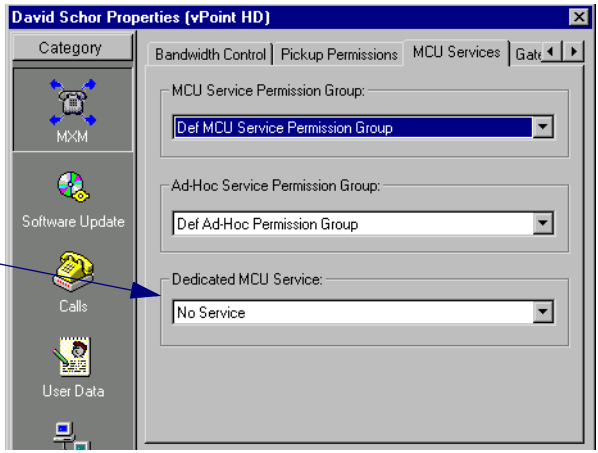
1. Right-click the MCU Service, point to **Property**, and then click **Session**. The **Session** tab appears.

2. Select **Use this service as an ad-hoc conference resource** and then click **OK** (in addition, you may also set the service to be exclusive for ad-hoc conferences only).



3. Right-click the end point, point to **Property**, **MXM**, and then click **MCU Services**. The **MCU Services** tab appears.

4. In the **Dedicated MCU Service** list, select the service.



11.6 Ad-hoc Permission Groups

An Ad-hoc Permission group is a set of MCU and VCB services that are defined for use in ad-hoc conferences. Its purpose is to control the use of resources for expanding to ad-hoc conferences.

An Ad-hoc Permission group may consist of one service or multiple services. It may also include combinations of services from more than one registered VCB and/or MCU. The order in which services are requested is important and controllable by Super User-level administrators.

During expansion to an ad-hoc conference, the MXM only uses those services listed in its assigned permission group. After an end point invites another end point, the MXM first tries to use the first service defined in the permission group. If the first service is not available, it tries to use the second defined service, and so on. If all enabled services are unavailable, the MXM does not complete the "invitation" to the additional end point.

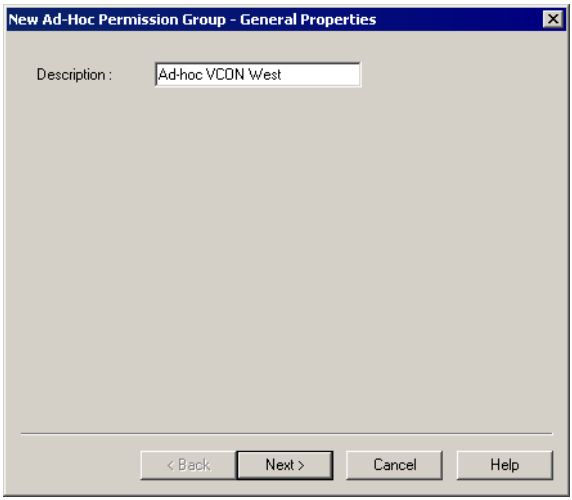
By default, every registered end point is assigned to the default Ad-hoc Permission Group. This may be changed when manually adding a new end point, or by editing the end point's properties.

➤ To add an Ad-hoc Permission Group

1. In the toolbar, click the New Ad-hoc Permission Group button . The New Ad-hoc Permission Group dialog box appears.
2. Change properties according to your permission group requirements. To move to the next properties page, click **Next**. For explanations about the various properties, see pages 161 to 162.
3. Click **Finish**. In the Main View, the new group appears under the Ad-hoc Permission Group object.

General

In the **Description** box, type a name for the Ad-hoc Permission Group. This name will appear on the system tree and in node Properties dialog boxes' MCU Services tab.



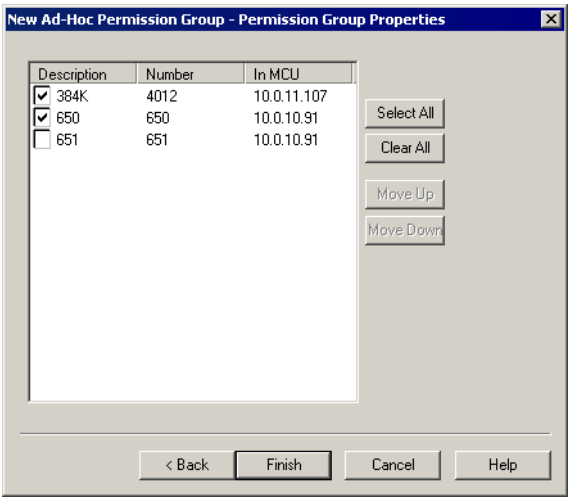
New Ad-hoc Permission Group - General Properties

Permission Group

The **Permission Group** Properties page includes all registered services that are defined for use as an ad-hoc resource (see "Session" on page 158).

Select any number of MCU or VCB services from the list to be in the Ad-hoc Permission Group. The group may also include combinations of services from more than one registered VCB and/or MCU.

- To place all services in the permission group, click **Select All**.
- To clear all the selections, click **Clear All**.



New Ad-hoc Permission Group - Permission Group Properties

Setting the Usage Order

The services' locations in the list determines the order in which the MXM tries to use them. After an end point invites another end point, the MXM first tries to use the first service in the permission group. If the first service is not available, it tries to use the second defined service, and so on. If all enabled services are unavailable, the MXM does not complete the "invitation" to the additional end point.

In the Permission Group page, you can move the services to different places in the usage order.

➤ To set the usage order of the selected services

❑ Click the name (*not* the checkbox) of a selected service. To move the service up and down the list to its designated place, click **Move Up** or **Move Down** as many times as necessary.

Repeat this step for as many services as necessary.

12 Setting Up Multipoint Conferences Managed by a VCB

The VCB5 is available only for licensed users of the Emblaze-VCON VCB Option. If you want to add this product to your videoconferencing network, please contact your local Emblaze-VCON distributor.

12.1 Overview of the Emblaze-VCON VCB

The Emblaze-VCON VCB is an MCU that enables:

- Initiation and management of multipoint conferences, including both scheduled and ad-hoc conferences, which are multipoint sessions that were expanded from point-to-point calls.
- Wide range of rich, dynamic layouts for the simultaneous viewing of several participants. Up to 16 users may be displayed at the same time.
- Web-based management/configuration and videoconference scheduling/ moderating applications.
- Simultaneous multicast streaming of active conferences and multimedia to multiple passive participants.

The VCB includes advanced features, such as audio transcoding, speed matching and bandwidth management, as well as basic features such as continuous presence, voice-activated switching, and multiple audio and video algorithms.

The VCB supports the Conference Moderator (VCB 2500 unit includes it as a standard feature), which provides administrators and users with the ability to schedule conferences in advance and to manage them remotely. At the appointed time, the system connects all of the conference end points, without the intervention of individual users. Conference hosts can also control when participants join or exit sessions, and transmit video and data streams to the participants. For more details, see the *Conference Moderator Help*.

The VCB's robust Chair Control provides several options for displaying conference participants. A rich selection of predefined layouts expands on the tradtional methods of Continuous Presence and Voice-activated Switching. Additionally, conference organizers can choose among the following view switching modes for each session:

Dominant Speaker	Showing the most recent speakers in the conference or from within predefined groups.
Fixed Image	Showing specific views throughout the conference's duration, selected by the conference's initiator.
Timer Image	Showing a rotation of Continuous Presence views, changing at timed intervals.

The VCB supports the following features:

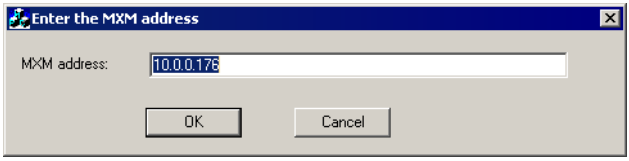
- ❑ G.722.1, G.723.1, G.728 and AAC audio algorithms with audio transcoding, allowing users to participate in a multipoint conference using different audio standards.
- ❑ Up to 4 Mbps data rate per participant in Voice-activated Switching and in Continuous Presence (H.263 and H.264 only - for H.261, up to 1 Mbps).
- ❑ H.261/H.263/H.263+/H.263++/H.264 video codec support in Voice-activated Switching
  H.261/H.263/H.264 video codec support in Continuous Presence.
- ❑ Dial-in conference initiation.
- ❑ Handles calls connecting up to 48 concurrent users.
- ❑ Support for sessions including H.323 end points/devices and SIP User Agents (through the MXM's embedded SIP proxy server).
- ❑ Multi-point sessions can be joined (cascaded) onto other sessions, contingent on similar data rates, display types, and audio/video algorithm.
  VCB to VCB
  VCB to other IP MCU

- Dynamic resource allocation pool – unallocated ports may be used as overflow for configured sessions.
- Applies H.239 support with HD DualStream™, in which both video and data application-sharing may be transmitted to conference participants (whose end points support dual streams). End points that don't support dual streams will receive either the data or video stream, depending on the active VCB Service's configuration.
- The streams may be sent in CIF, QCIF, 4CIF, VGA, SVGA, or XGA.
- Speed matching, allowing participants in Continous Presence to connect using two different data rates (for example, 128 Kbps and 384 Kbps)
- Mode switching, allowing participants to choose the type of viewing mode (Dominant Speaker, Fixed Image or Timer Mode) during a conference.
- Symmetric bandwidth usage during Continuous Presence calls.
- Protection of calls using H.235 (AES) encryption.
- Optional deployment of Emblaze-VCON vPoint HD videoconferencing clients.

12.2 Logging in a New VCB

➤ To register a VCB to the MXM

1. In the VCB computer's Windows desktop, click **Start**, point to **Programs**, **VCON** and **VCB**, and then click **Update MXM Address**.
2. Enter the IP address of the MXM and click **OK**.



Entering the MXM's IP Address

If the MXM is in Open Mode, the VCB automatically logs in, and appears under the Emblaze-VCON VCBs object. Services appear under the specific VCB. To edit VCB properties, see "Setting VCB Properties" on page 173. To edit Services properties, see "Setting VCB Services Properties" on page 179.

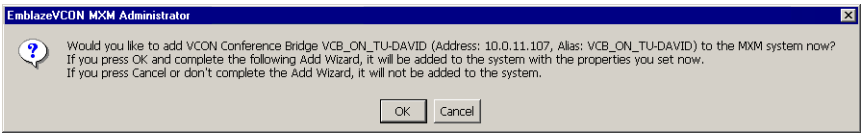
If the MXM is in Closed Mode for MCUs, a Login Request notification will appear on the Administrator tree after several seconds. To complete the Setup process, proceed to step 3.

3. Expand the Login Request item.

Login Request Notification for VCB

4. Right-click the VCB name and then click **Grant Login Permission**.

   A message appears, asking if you want to register the VCB now.



VCB Registration Request

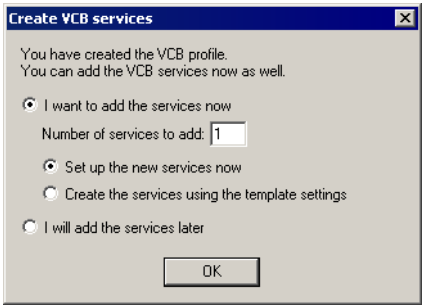
5 Click **OK** if you want to manually set the VCB's properties, such as Firewall ports. The New VCB Wizard appears. The original property values are the default values defined in the Emblaze-VCON VCB template (see "Setting Up Templates" on page 47).

If you click **Cancel**, the VCB does not log in, but remains under the Login Requests object until you delete it (and the VCB stops trying to log in). See "Deleting a Login Request" on page 30.

6 Change properties according to your system specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see "Setting VCB Properties" on page 173.

7 When you finish the last page, click **Finish**.

8 In the Create VCB Services dialog box, you can choose to add VCB Services now or to add them later.



Decision to Add VCB Services Now or Later

I want to add the services now
Set up the VCB Services during this registration process.

In the **Number of Services to Add** box, type the number of VCB Services that you want to set up.

Set up the new services now
Select to set up the configurations for the services now.

The New VCB Service wizard appears. Set properties as required. For more information about the VCB Service properties, see "Setting VCB Services Properties" on page 179.

Create the Services Using the Template Settings
Select to set up the configurations for the new services based on the VCB Service template.

The new services will appear automatically in the Main View under the Emblaze-VCON VCB object.

I Will Add the Services Later Select to add the VCB to the Main View without services at this time. You may add services later.

Click **OK**.

In the Main View, the VCB appears under the Emblaze-VCON VCB object. If you added services in Step 8, they appear under the VCB.

VCB Entry in Main View

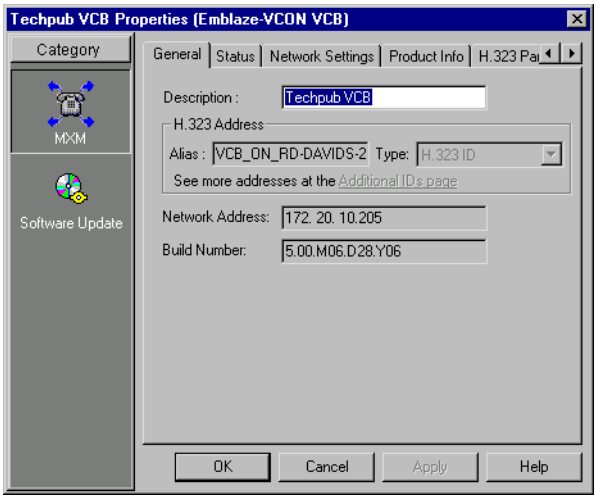
12.3 Setting VCB Properties

In step 6 of "Logging in a New VCB" on page 171, the Add Wizard provided the chance to change various VCB properties. VCB Properties define network and location information for the VCB. This section describes these properties.

If an open conference is using the VCB when you make configuration changes, some of these changes may take effect immediately. Otherwise, changes will take effect in the next session.

General

The **General** tab contains identity information of the VCB.



VCB - General Properties

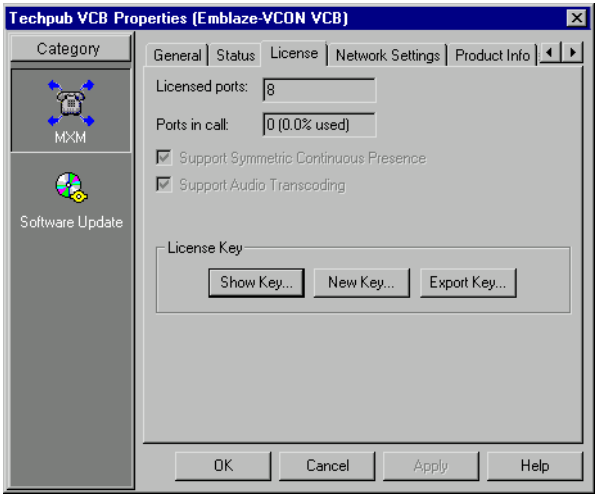
In the **General** Properties tab, the following properties appear:

Description	Identity of the VCB. This name will appear in the Main View after the login process is finished.
Alias	The VCB's alias name.
Type	The type of address used by the VCB for registering with the MXM.
Network Address	IP address of the VCB.
Build Number	Version information for the VCB.

License

The **License** tab appears only for VCB 2500 units whose licenses were obtained separately from this MXM.

The **License** tab shows the details of your VCB 2500 license key. If you need to change this number, contact your local Emblaze-VCON distributor.



VCB 2500 - License Properties

Licensed Ports — Maximum number of concurrent participants that may be serviced by this VCB.

Ports in Call — Number of participants that are engaged in active videoconferences managed by this VCB.

Support Symmetric Continuous Presence — To send the video of a Continuous Presence conference, the VCB uses the alloted bandwidth (per channel) multiplied by 4. If any connected nodes' (end point, gateway, etc.) bandwidth limits are lower than the bandwidth used by the VCB, the VCB routes the call through the node at lower bandwidth, according to the Low Bandwidth during CP setting of the VCB Service's Advanced Properties (see "Advanced" on page 190).

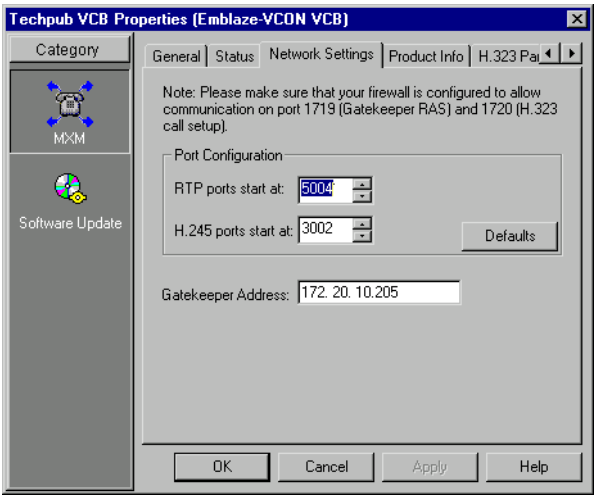
Support Audio Transcoding — Converts audio from one standard to another, such as G.722 to G.728. This allows end points supporting different audio standards to retain and play the audio stream of a call.

License Key

Show Key	Click to view the key code for the current VCB installation.
Export Key	To change the licensed number of ports, click this button to create a license file for the VCB on the host computer. Contact your local Emblaze-VCON sales representative to send the file. You will then receive an updated license key.
New Key	After receiving a new license file from your Emblaze-VCON distributor, click this button, browse to select the file and click **Open**. When prompted to apply the license code, click **OK**. To implement the license change and close the dialog box, click **OK** again.

Network Settings

In the **Network Settings** tab, enter the allocation of ports for communication through your organization's firewall.



VCB - Network Settings Properties

RTP & RTCP Port Range

The MXM allocates a range of ports for video and audio during videoconferences. The value indicates the lowest port number allowed.

This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

H.245 Port Range

The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences. The value indicates the lowest port number allowed.

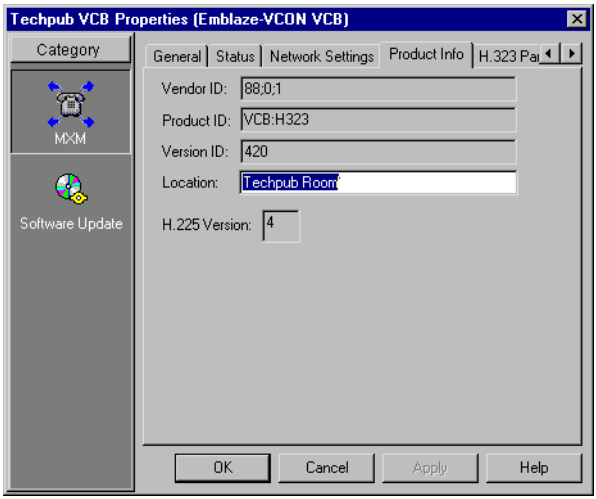
This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

Defaults

Click this button to return to the default settings.

Product Info

The **Product Info** tab provides information about the VCB's manufacturer and model.



VCB - Product Info Properties

Vendor ID Identity of the manufacturer.

Product ID Manufacturer's identity of the product.

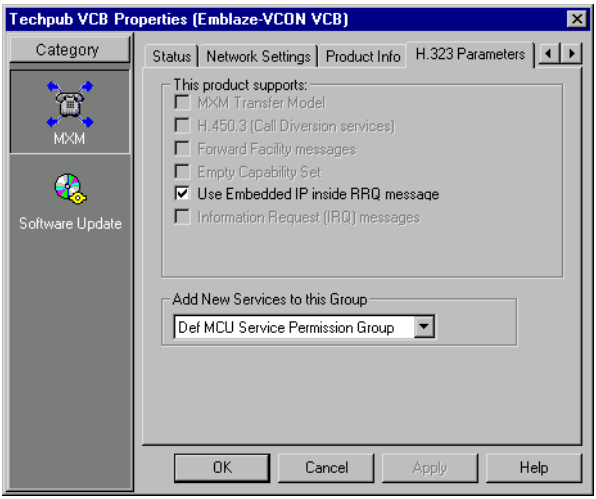
Version ID Manufacturer's version identification of the product.

Location Physical location of the VCB.

H.225 Version Protocol for control signaling in an H.323 conferencing environment.

H.323 Parameters

In the **H.323 Parameters** page, you can enable or disable the exchange functionalities supported for multipoint videoconferences through the VCB.



VCB - H.323 Parameters Properties

Use Embedded IP Inside RRQ Messages — In response to registration requests (RRQ) from this VCB, the MXM will send response to the IP address specified in the RRQ.

Add New Services to this Group — If a new MCU service is added to this VCB's configuration, it will automatically be included in the permission group selected here.

12.4 Setting VCB Services Properties

VCB Services define the usage of resources used during a multipoint videoconference managed by the VCB.

After the VCB's installation and restart of the VCB's computer, you can add or edit service entries under the Video Conference Bridge object. One directory (E.164) number is created for each service type.

To handle situations in which additional participants require additional resources, set up several VCB Services with incremental increases in bandwidth, number of ports, or multicast capabilities.

Services with Incremental Increases in Available Resources

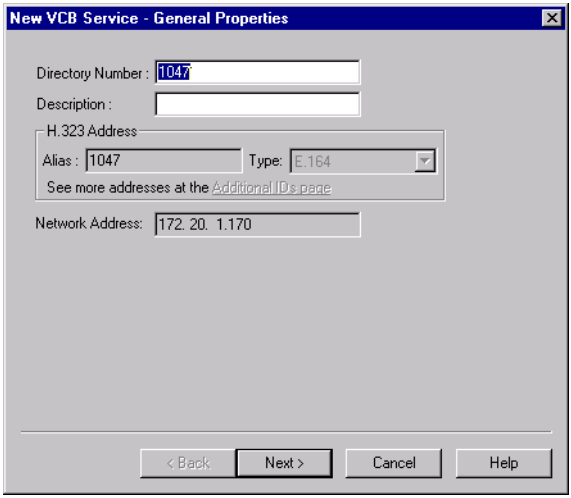
➤ To add VCB Services

1. Right-click the VCB and then click **New Service**. The New VCB Service wizard appears.
2. Change properties according to your ad-hoc videoconferencing specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see the following subsections.
3. When you finish the last page, click **Finish**.

The following subsections describe the VCB Service properties.

General

In the **General** page, enter identity information of the new VCB Service.



VCB Service - General Properties

In the **General** Properties tab, the following properties appear:

Directory Number — Number to be dialed for using this service.

Description — Name of the service. This name will appear in the Main View after the login process is finished.

H.323 Address

Alias — The service's alias.

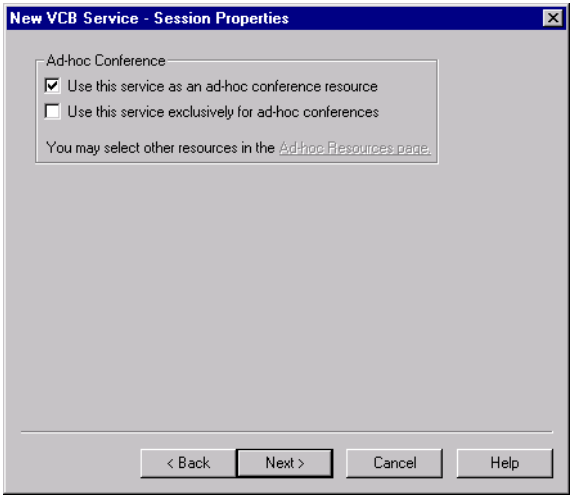
Type — The type of address used by the VCB for registering the service with the MXM.

Additional IDs page — Click this link to view any additional IDs that have been configured for this service.

Network Address — IP address of the VCB.

Session

A point-to-point conference becomes an ad-hoc conference when additional end points are "invited" by one of the parties and they join the session. In the **Session** page, define if the selected VCB Service can be used for expanding to ad-hoc conferences.



VCB Service - Session Properties

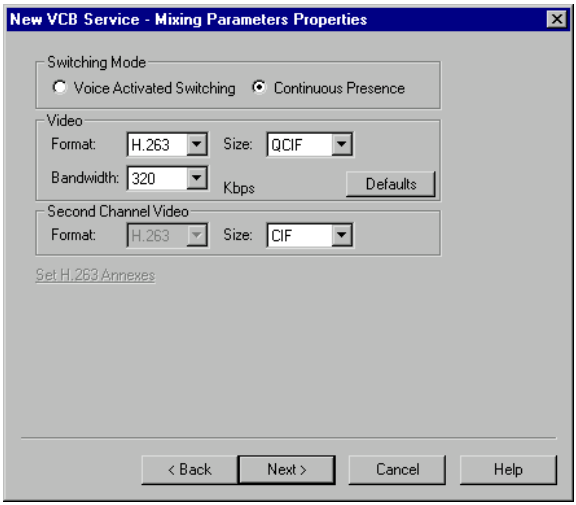
Use this service as an ad-hoc conference resource — This service is available for use when expanding to an ad-hoc videoconference.

Use this service exclusively for ad-hoc conferences — This service is only available for inviting additional users into ad-hoc videoconferences, but not available for initiating multipoint sessions.

Ad-hoc Resources page — Click this link to open the MXM's Ad-hoc Resources Properties, in which you can also select other VCB Services that may be used for ad-hoc videoconferences (see "Ad-hoc Resources" on page 74).

Mixing Parameters

In the **Mixing Parameters** tab, define the video display configuration for sessions initiated with this service.



VCB Service - Parameters Properties

Switching Mode

Voice Activated Switching — The participants see the video of one participant at a single time.

Continuous Presence — Several participants in a multipoint conference are viewed simultaneously.

Video

Format — The video codec (**H.261**, **H.263**, **H.264**) used in the multipoint conference.

H.264 is not supported in Continuous Presence.

Size The format and resolution of the transmitted video images.

In Continuous Presense, the local side transmits QCIF video and receives CIF video.

In Voice-Activated Switching, the available formats are:

- **CIF** (Common Interchange Format), or normal size - 352x288
- **QCIF** (Quarter Size Common Interchange Format), or quarter size - 176x144
- **4CIF** (4 x CIF) - 704x576
- **VGA** (Video Graphics Array) - PC standard - 640x480
- **SVGA** (Super VGA) - 800X600
- **XGA** (Extended Graphics Array) - 1024x768

Bandwidth The bandwidth available for each participant.

Default Click to restore the default video configuration.

Second Channel Video

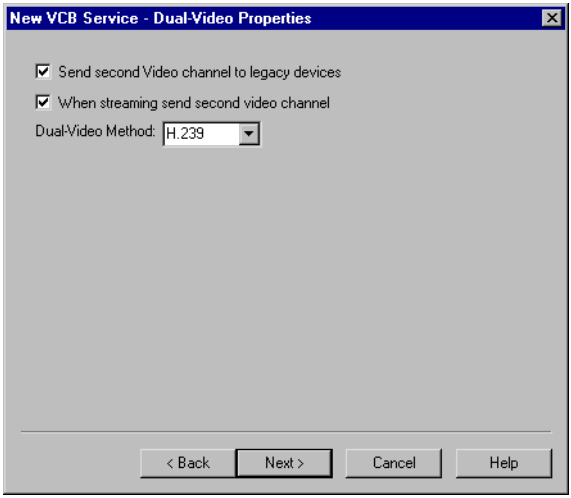
Video Format/ Size The format and resolution of any second-channel stream, such as data, which is sent to all participants in a multipoint conference:

CIF, **QCIF**, **4CIF**, **VGA**, **SVGA**, **XGA**

Set H.323 Annexes Click the link to go to the **H.263 Annexes** tab of this VCB Service's properties.

Dual Video

End points that support Emblaze-VCON's HD DualStream™ (vPoint HD, HD5000, HD4000, HD3000 and HD2000) or other dual-video capability can send video and data streams simultaneously to a multipoint conference through the VCB. During a conference, end points supporting HD DualStream can view documents, graphics, and presentations as the main image, while the video appears as a PIP inset on the screen.



VCB Service - Dual Video Properties

Send second video channel to legacy devices — If a receiving end point does not support dual streams, it receives only the stream carrying the shared data application. However, the data appears in video format.

When streaming send second video channel — If data sharing takes place during a multicast conference, the multicast session's Participants receive the data stream only.

Dual-Video Method

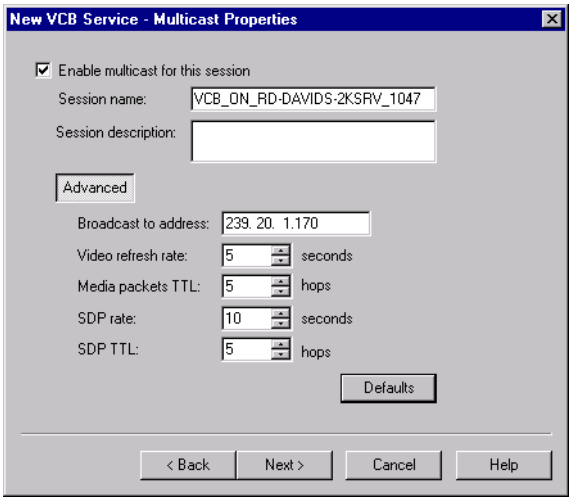
Define the permitted method for transmitting dual video streams during a conference managed through this service.

The H.239 standard enables end points to convert data into a separate media stream and transmit it parallel to the video stream. Video systems supporting H.239 display shared data and live video in separate windows. Systems not supporting H.239 display only the shared data in a single window.

- ❑ Choose **None** to block all dual video transmission.
- ❑ Choose **H.239** to allow H.239 dual video transmission.

Multicast

In the **Multicast** page, enable this service to support Emblaze-VCON's Interactive Multicast conferencing (simultaneous video and audio streaming to multiple users).



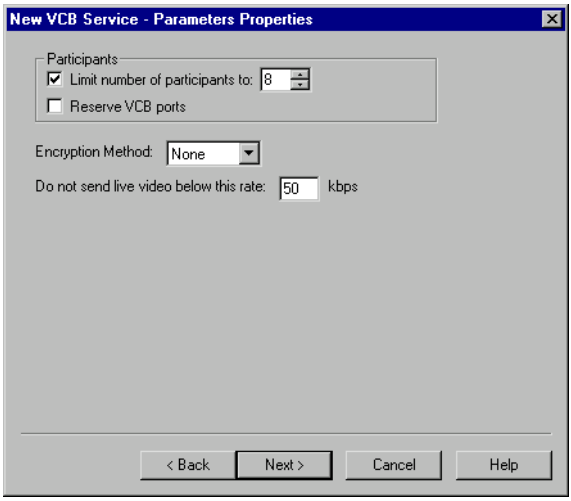
VCB Service - Multicast Properties

Enable Multicast for this Session	Select to enable this service to be used for multicast sessions.
Session Name	Type a name to identify this service's multicast session.
Session Description	Type a name or description of the multicast session.
Advanced	Click this button to display additional properties (described below).
Broadcast to Address	The destination IP address for the multicast session. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of **224.0.0.0** to **239.255.255.255**.
Video Refresh Rate	Define the interval at which the end point broadcasting the multicast synchronizes the video display at the receiving ends.
Media Packets TTL	The maximum number of routers (hops) that the multicast session's packets may pass through.

SDP Rate	Session Description Protocol Rate - The interval at which announcements and descriptions of the multicast session are sent out on the Internet Multicast backbone (Mbone), for Participants and passive third-party viewers.
SDP TTL	The maximum number of routers (hops) that the SDP announcement for this session may pass through.
Defaults	Click this button to return to the Multicast default settings.

Parameters

In the **Parameters** page, define the configuration for multipoint sessions initiated with this service.



VCB Service - Parameters Properties

Participants

Limit Number of Participants to

The maximum number of concurrent calls allowed in this session, according to your VCB's license terms. Selecting this option also enables you to reserve ports for the defined number of users.

If this option is not selected, the number of users that can participate in this session is limited to the number of free ports. However, no ports are reserved specifically for this session.

Reserve VCB Ports

Only available if the **Limit Number of Participants** option is selected.

The VCB reserves an equal number of ports as the number of maximum users in this session, in accordance with your VCB license terms. For example, if the session is limited to a maximum of 8 participants, the VCB will reserve 8 ports. None of those ports will be available for other sessions.

Encryption Method

Choose the mode of encryption for conferences using this service.

- Choose **None** to allow unsecured calls.
- **Auto** enables the transmitting end point to encrypt a call if the remote sides have also enabled encryption. If they have not enabled encryption, an outgoing call will be unsecured.
- **AES** (Advanced Encryption Standard) is a standard encoding method for encrypting data transmissions in commercial and government sectors of the USA and its use is growing worldwide.

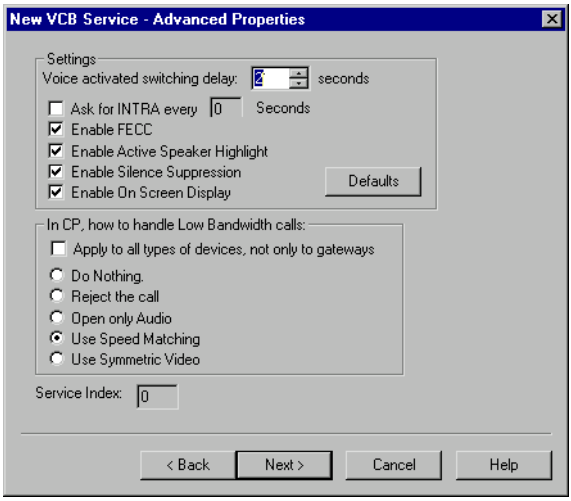
  Select this option to encrypt all calls using this VCB Service. If the remote sides have not also enabled encryption, the call attempt will be unsuccessful.

Do Not Send Live Video Below This Rate

The minimum bandwidth required for sending video during a conference using this service.

Advanced

In the **Advanced** page, define additional parameters required by the VCB for managing multipoint conferences.



VCB Service - Advanced Properties

Voice-activated Switching Delay — Delay period before changing the displayed video during a voice-activated switching multipoint conference. The displayed video changes only after the source of the new sound or voice is steady for the defined period. A delay period is necessary to prevent quick incoherent display changes that may be caused by sudden noises (such as a sneeze) rather than a steady speaker.

Ask for Intra Every ___ Seconds — Select to enable displayed end points to send periodic intras in order to synchronize the video display at the receiving end. This setting affects conferences managed with this VCB service.

In this box, define the interval between the transmission of intras.

Enable FECC — Select to enable Far End Camera Control (FECC) to all participants in a conference using this service. Applicable only to Voice-activated Switching mode.

Enable Active Speaker Highlight — Select to display a frame surrounding the active speaker in Continuous Presence.

Enable Silence Suppression Select to enable the VCB to lower bandwidth and CPU usage during periods of low audio and silence.

Enable On Screen Display Select to display the names of the displayed users in Continuous Presence.

In CP, how to handle low bandwidth calls If a Continuous Presence call tries to connect using a lower bandwidth than defined by this service, the VCB will handle the call's bandwidth according to the selected setting.

- To apply low bandwidth adjustment to all end points in a conference, select **Apply to all types of devices, not only to gateways**. Deselect this option to apply low bandwidth calling only through gateway connections.
- **Do nothing** - This setting is not applied to calls.
- **Reject the call** - The VCB does not allow the call to continue.
- **Open only audio** - The VCB allows the audio stream to continue.
- **Use Speed Matching** - The call continues at [4x the VCB Service's defined bandwidth + 64 Kbps audio]. However, all end points **not** supporting this bandwidth receive the call at the lowest bandwidth used among all participants.

  The table below shows the bandwidth used when a Continuous Presence call of [320 x4 Kbps + 64 Kbps audio] connects, resulting in the transfer of the full 1.5 Mbps bandwidth to those end points supporting it, but all end points supporting less (than 1.5 Mbps) bandwidth only receive 128 kbps.

Endpoint no.	Configured Bandwidth	Bandwidth During Call
1	1.5 Mbps	1.5 Mbps
2	1.5 Mbps	1.5 Mbps
3	768 Kbps	128 Kbps
4	384 Kbps	128 Kbps
5	128 Kbps	128 Kbps

In CP, how to handle low bandwidth calls (cont.)

- **Use Symmetric Video** - The call continues at [4x the VCB Service's defined bandwidth + 64 Kbps audio]. However, all end points that do not support the call's bandwidth receive the call at the bandwidth defined in their configuration.

  The table below shows the bandwidth used when a Continuous Presence call of [320 x4 Kbps + 64 Kbps audio] connects, resulting in the transfer of the full 1.5 Mbps bandwidth to those end points supporting it, but all end points supporting less (than 1.5 Mbps) bandwidth only receive their configured bandwidth.

Endpoint no.	Configured Bandwidth	Bandwidth During Call
1	1.5 Mbps	1.5 Mbps
2	1.5 Mbps	1.5 Mbps
3	768 Kbps	768 Kbps
4	384 Kbps	384 Kbps
5	128 Kbps	128 Kbps

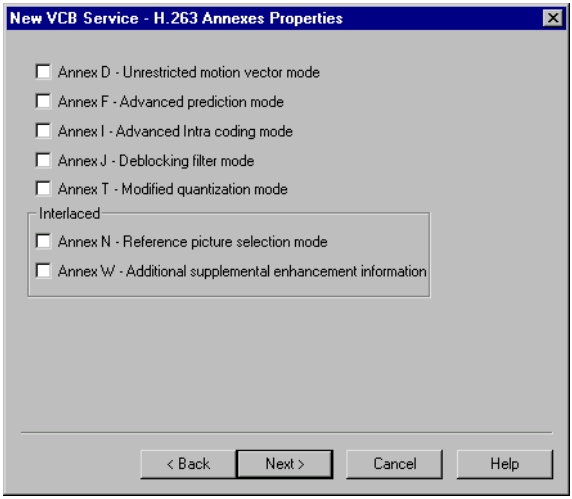
Service Index Identifier number of this service for technical support purposes. If requested, send this number to Emblaze-VCON Technical Support.

Defaults Click this button to restore the default settings for this page.

H.263 Annexes

In addition to Baseline H.263, enable supplemental H.263+ and H.263++ features which this VCB Service applies to conferences.

Make sure that all end points participating in this service's sessions support the enabled annexes. Any end point that does not support H.263+ or H.263++ may not be able to display the video.



VCB Service - H.263 Annexes Properties

Enable H.263 options as follows:

Annex D — **Unrestricted motion vector mode**
This option enables the use of unrestricted motion vector capability. Motion vectors can have larger values than in Baseline H.263, resulting in improved video quality when there is camera or background movement.

Annex F — **Advanced prediction mode**
This option enables the use of advanced prediction capability. This mode improves interframe prediction and improves picture quality for the same bitrate by reducing the blocking artifacts.

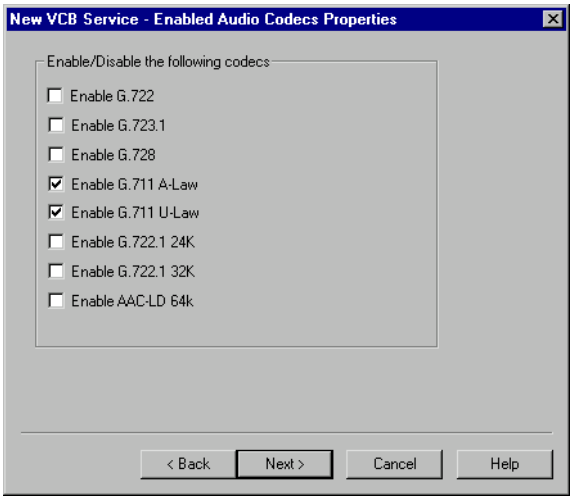
Annex I — **Advanced Intra Coding mode**
This option improves the compression efficiency for Intra macroblock encoding. This mode reduces the size of the encoded bitstream.

Annex J	**Deblocking filter mode** This option provides better prediction reduces the amount of block artifacts in the final image. It applies an adaptive filter across block boundaries.
Annex T	**Modified quantization mode** This mode includes three features. First, it allows rate control methods to change the quantizer at the macroblock level. Second, it enhances the chrominance quality by specifying a finer quantization step size. Third, it improves the picture quality by extending the range of DCT (Discrete Cosine Transform) coefficients.
Annex N	**Reference picture selection mode** In H.263, a picture is predicted from the previous picture. If parts of pictures suffer quality loss, the quality of the rest of the stream may suffer too. To reduce error propagation, this mode enables selection of reference frames for prediction. This improves picture reproduction quality in error-prone environments.
Annex W	**Additional supplemental enhancement information** This mode specifies interlaced field indications, repeated picture headers, and the indication of the use of a specific fixed-point inverse DCT.

Enabled Audio Codecs

Only audio codecs that are specified in your VCB's license may be used during its calls. In the **Enabled Audio Codecs** page, select which of these codecs are available for conferences using this specific VCB service.

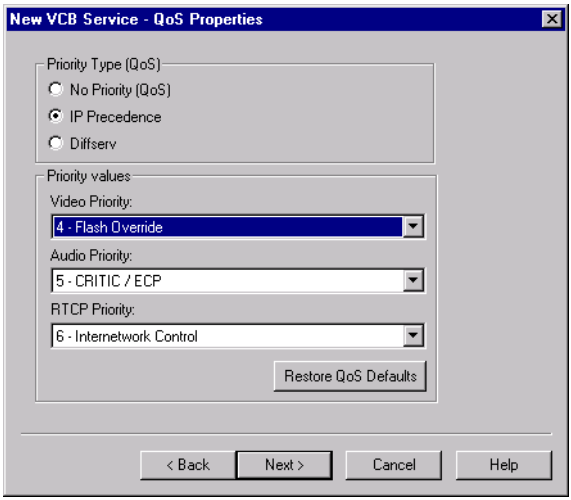
To reach the maximum active participants per session/server, enable no more than one (two for VCB 2500) codec per session.



VCB Service - Enabled Audio Codecs Properties

QoS

The **QoS** page contains properties for controlling the type of Quality of Service that will be used for transmitting packets during a multipoint conference that's initiated using this VCB service.



VCB Service - QoS Properties

Set QoS properties as follows:

Priority Type (QoS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

No Priority	Network transfers packets using normal Best-effort (or Routine) packet transmission.
IP Precedence	Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.
Diffserv	Network transfers packets according to specific needs of the sending application.

Priority Values

Video, Audio and RTCP Priority

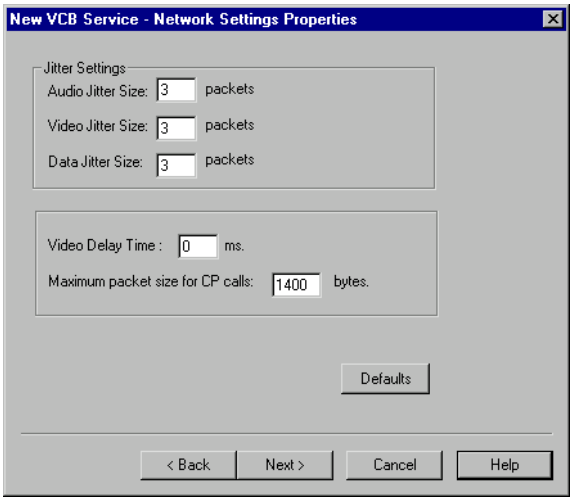
For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see Appendix F, "QoS Priority Values."

To reset the Priority default values, click **Restore QoS Defaults**.

Network Settings

The Network Settings enables the transmitted media to take problematic network conditions into consideration, in order to achieve high quality playback at the receiving end.



VCB Service - Network Settings Properties

Jitter Settings

Jitter prevents packet reordering, which sometimes occurs during the transmission of media through a network. Reordering is usually caused by network congestion, queuing errors, or configuration errors.

Audio/Video/ Data Jitter Size	Smooth playback of transmitted media continues even if the packets arrive out of order at the receiving end, up to the number of packets defined here for each packet type.
Video Delay Time	Delay between transmission of video packets. This parameter is intended for preventing video burst during transmission through various routers or servers.
Maximum Packet Size for CP Calls	To allow Continuous Presence calls to proceed, set this parameter either equal to or lower than your network's MTU.
Defaults	Click this button to restore the default settings for this page.

LDAP

The **LDAP** page provides information about the VCB service's registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes' LDAP Properties, see "LDAP" on page 104.

Additional ID

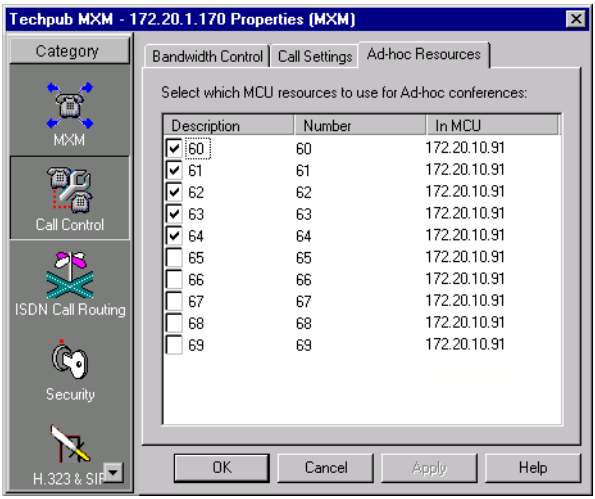
In addition to its directory (E.164) number, a VCB service may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** page, you may enter these, if applicable. For more information about adding Additional IDs, see "Additional IDs" on page 106.

12.5 Setting the Ad-hoc Resources Table

The Ad-hoc Resources table contains a list of VCB and MCU services registered with the MXM, together with the VCB or MCU with which they are associated. Select the services that the MXM may use to initiate ad-hoc conferences.

➤ To select ad-hoc resources

1. In the Administrator window, right-click the MXM node at the top, point to **Property**, **Call Control**, and click **Ad-hoc Resources**.
2. Select the services that the MXM may use to initiate ad-hoc conferences.
3. Click **OK**.



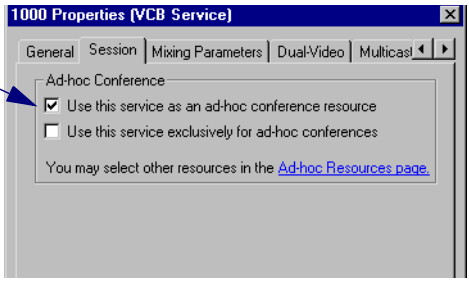
Available Ad-hoc Resources

12.6 Dedicated VCB Service for End Points

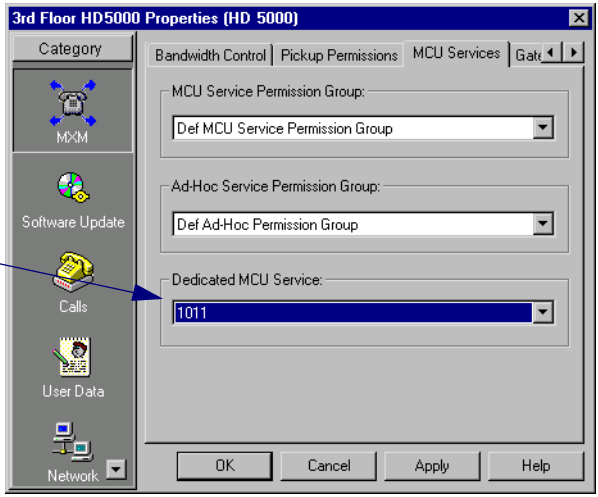
A dedicated VCB service is set up only for expansion to an ad-hoc conference that includes a specific end point. That is, the service is "dedicated" to that end point. That specific end point must be either one of the original two end points of a point-to-point conference or the invited end point.

➤ To dedicate a service to a specific end point

1. Double-click the VCB Service and then click the **Session** tab.
2. Select **Use this service as an ad-hoc conference resource** and then click **OK** (in addition, you may also set the service to be exclusive for ad-hoc conferences only).



3. Double-click the end point, click **MXM**, and then click the **MCU Services** tab.
4. In the **Dedicated MCU Service** list, select the service. Click **OK**.

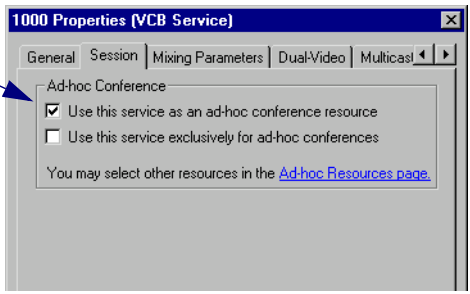


12.7 Dedicated VCB Service for a Zone

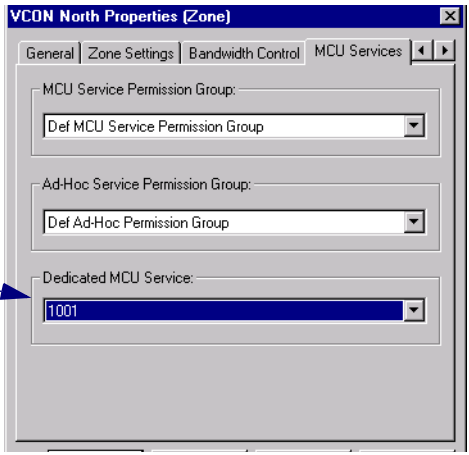
A dedicated VCB service for a neighboring zone may be used only if any of that zone's end points are in the resulting ad-hoc conference (either one of the original two end points of the conference or the invited end point).

➤ To dedicate a service for a neighboring zone

1. Double-click the VCB Service and then click the **Session** tab.
2. Select **Use this service as an ad-hoc conference resource** and then click **OK** (in addition, you may also set the service to be exclusive for ad-hoc conferences only).



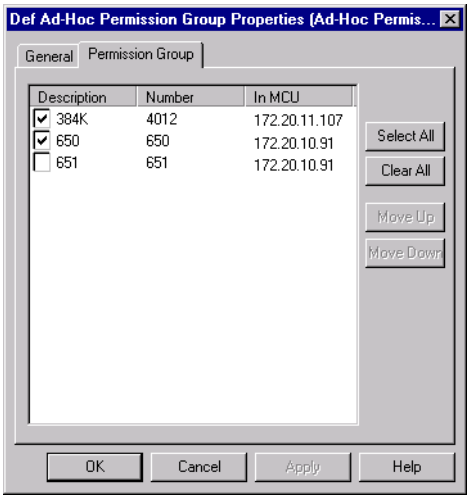
3. Double-click the neighboring zone, click **MXM**, and then click the **MCU Services** tab.
4. In the **Dedicated MCU Service** list, select the service. Click **OK**.



12.8 Adding VCB Services to an Ad-hoc Permission Group

An Ad-hoc Permission group is a set of MCU and VCB services that are defined for use in ad-hoc conferences. It helps you control the use of resources for expanding to ad-hoc conferences. Registered end points may be associated with an Ad-hoc Permission Group (see "MCU Services" on page 98). During expansion to an ad-hoc conference, the MXM only uses those services listed in the inviting end point's assigned permission group.

For a detailed procedure of adding VCB Services to an Ad-hoc Permission Group, see "Ad-hoc Permission Groups" on page 164.



VCB and MCU Services in an Ad-hoc Permission Group

12.9 Expanding to an Ad-hoc Videoconference

To expand from a point-to-point videoconference to an ad-hoc videoconference, one of the parties must invite the additional parties. This procedure depends on the party's videoconferencing application:

vPoint/vPoint HD

1. Enter an additional contact's user number (E.164) or address into the Manual Dialer's address box.
2. Click **Invite**.

-or-

1. Open the Dialer and locate the contact that you want to invite.
2. Right-click the contact and then click **Invite**.

HD3000/2000

1. Press any of the number keys on the remote control. The Manual Dial dialog box and SoftKey menu open.
2. Press the red **MXM CALL CONTROL** Softkey.
3. In the MXM Call Control box, enter the directory number of the party that you want to invite. To browse entries from the Phone Book, press the right and left arrow keys on the remote control.
4. Press the green **INVITE** SoftKey.

HD5000/4000

1. Click the Telephony Services button to open the Telephony Services menu.

2. Click ***Invite User***.
3. In the Dial Plan Number box, enter an additional party's user number.

-or-

Click the Online Directory button and choose a name from the Online Directory Dialer.

4. Click the Dial button.

Falcon

1. Press any of the number keys on the remote control. The Call Control dialog box and SoftKey menu open.
2. Enter the directory number of the party that you want to invite. To browse entries from the Phone Book, press the right and left arrow keys on the remote control.
3. Press the green **INVITE** SoftKey.

MeetingPoint 4.6

1. In MeetingPoint's Conference Panel, click the **Services** arrow and then click **Invite**. The Invite dialog box appears.
2. In the **Destination** box, enter the directory number of the user that will receive the call by one of the following methods:
   - Type the number or click it in the list.

     -or-
   - Click **Browse** at the end of the row. In the Select an Entry dialog box, select the user and click **OK**.
3. Click **OK**.

Other applications

Enter the defined Ad-hoc Conference code (default is *77) followed by the directory number of the additional party. For example, to invite end point 2345, enter ***772345**.

13 USING POLYCOM® MGC™ WITH THE MXM

The Polycom® MGC™ operates under a different configuration model than most other MCUs being used in the videoconferencing sector. This appendix provides instructions for setting up the MGC's configuration for operation in conjunction with the MXM. In addition, this appendix includes instructions for setting up an Accord Meeting Room for ad-hoc videoconferences and an Accord Gateway for routing IP-ISDN calls through the MGC.

This appendix only provides information directly related to the integrated operation of the Polycom MGC with the MXM. For additional information about using the MGC, see the MGC's accompanying user documentation.

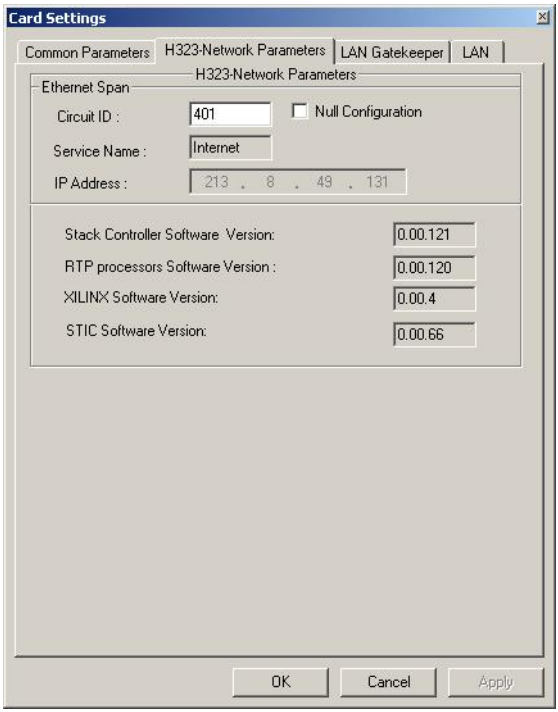
13.1 MGC Configuration

Network Services Configuration

Create a new Network Service, or if you're editing an existing configuration, choose the one that you want to change.

➤ **To set up Network Service properties**

1. Run the Polycom MGC management application.
2. In the left pane, browse through the tree to **MCU Configuration**, **Network Services**, and **Network Services-H.323**.

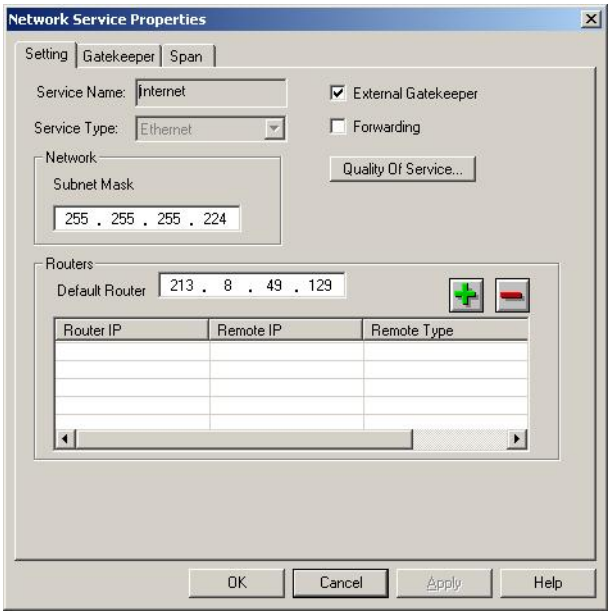


Browsing to Network Services-H.323

3 Create a new Network Service or choose the existing one allocated for use with your MXM.

4 In the **Setting** tab, enter the following information:

Subnet Mask	IP subnet mask used by the connected network.
Default Router	IP address of the default router used by the connected network.
External Gatekeeper	Select this option. The MXM is an external gatekeeper in relation to the MGC.



Network Services - Setting Configuration for MXM

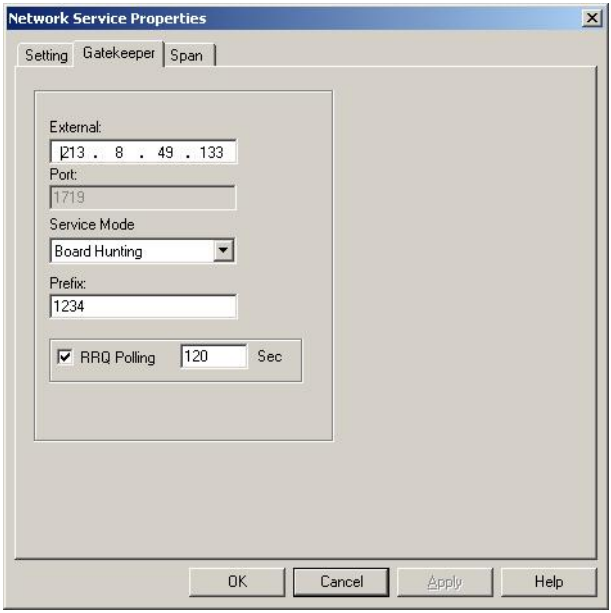
5 In the **Gatekeeper** tab, enter the following information:

External IP address of the MXM.

Port **1719** should be the defined port.

Prefix Prefix that must be dialed in addition to all of the MGC's Meeting Rooms' directory numbers (or "node number"). This number must be within the permitted directory number range (see "Dial Plan" on page 67) and be the same number of digits.

For example, if the prefix is "1234" and the Meeting Room's directory number is 1095, then a user must dial "12341095" to enter the videoconference.



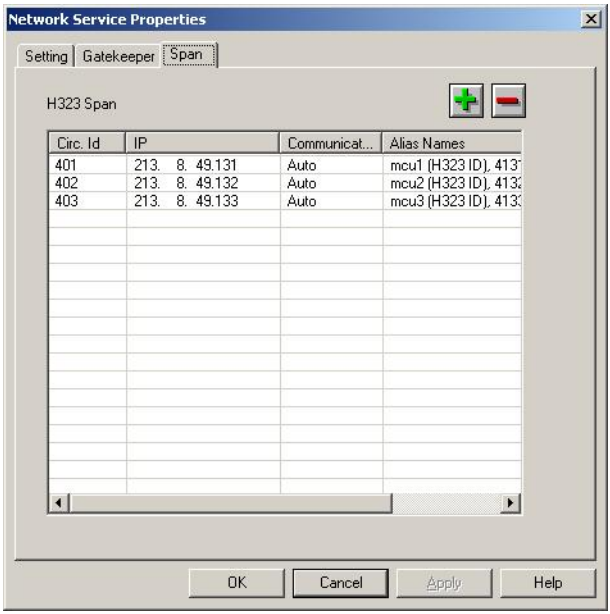
Network Services - Gatekeeper Configuration for MXM

6 The **Span** tab displays a list of H.323 cards in the MGC. You must enter a Circuit ID and unique alias for each H.323 card. Click the plus (+) button to add a new card configuration.

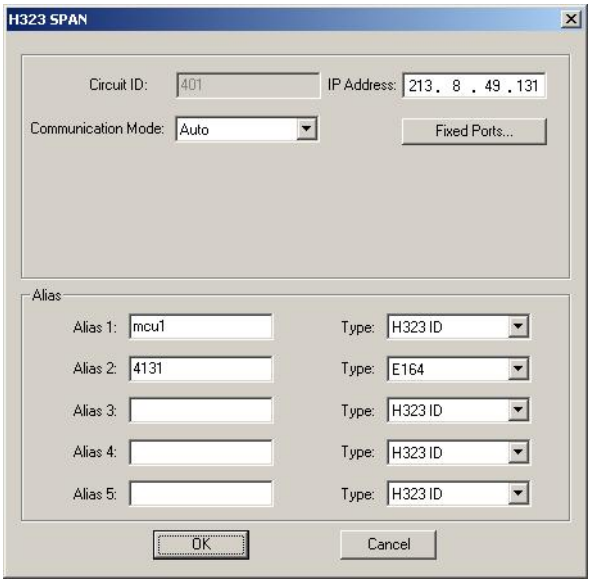
7 Enter the following information:

Circuit ID	Unique number for the H.323 card in the MGC.
IP Address	IP address for the H.323 card.
Alias	Enter one H.323 ID alias for this card (must be unique in the MXM).

8 Click **OK**.



Network Services - Gatekeeper Configuration for MXM



Adding a New H.323 Card Configuration

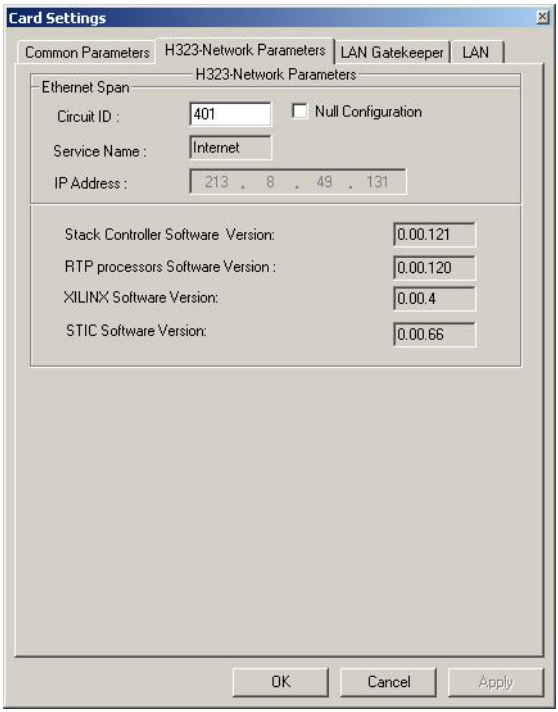
H.323 Card Configuration

After setting up the Network Services configuration, assign the appropriate Circuit IDs to the H.323 cards in the MGC.

➤ To assign a Circuit ID to an H.323 card

1. In the left pane, open the Cards object. Select the slot of the H.323 card.
2. Right-click the card, and then click Properties. The Card Settings dialog box appears.
3. In the **H.323 Network Parameters** tab, enter the Circuit ID for this card.
4. Click **OK**.

Following Network Services and H.323 card configuration, make sure that the Circuit IDs, IP addresses, and Service Type correspond in both configurations.



H.323 Card Network Parameters

13.2 Adding an Accord Meeting Room

A Meeting Room is a hunting group of MCU services provided by the Polycom MGC or other Accord hunting groups. A multipoint videoconference managed by the MGC must be associated with a Meeting Room.

If you will use the MGC to manage ad-hoc videoconferences, you must define this ability in a Meeting Room configuration.

To set up Meeting Rooms in the MGC, see the Polycom MGC user documentation.

➤ To add an Accord Meeting Room to the Main View

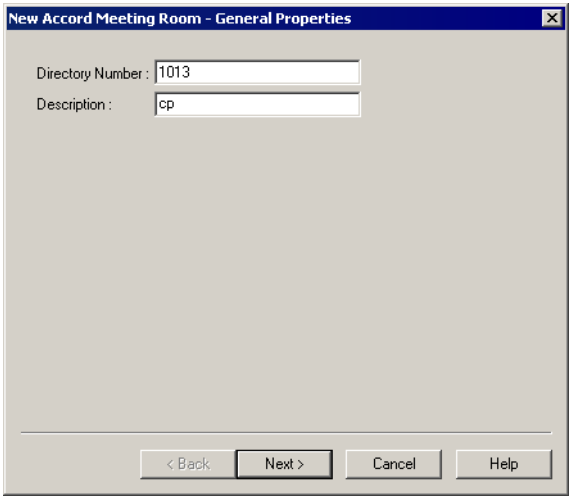
1. Right-click the MXM object, point to **Add Node**, and click **New Accord Meeting Room**. The New Accord Meeting Room wizard appears.
2. Change properties according to your multipoint videoconferencing specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see the following section.
3. When you finish the last page, click **Finish**.

13.3 Setting Meeting Room Properties

In step 2 of "To add an Accord Meeting Room to the Main View" in the previous section , the wizard provided the chance to change various Meeting Room properties. This section describes these properties.

General

The **General** page contains identity information of the new Meeting Room.



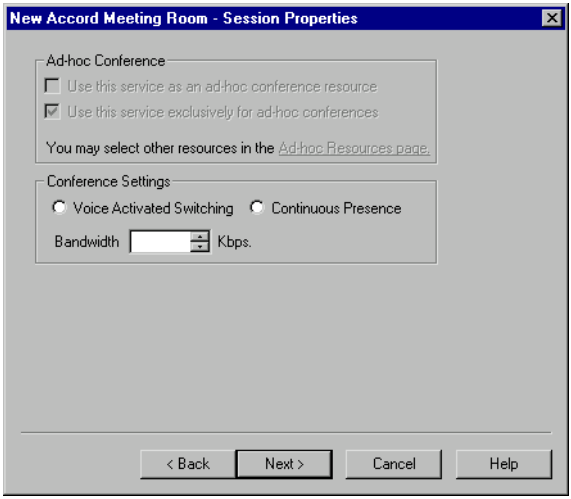
Accord Meeting Room - General Properties

In the **General** page, enter the following information:

Directory Number	Assign a directory number for the Meeting Room.
Description	Type an identity for the Meeting Room. This description does not affect the operation of the system.

Session

A point-to-point conference becomes an ad-hoc conference when additional end points are "invited" by one of the parties and they join the session. In the **Session** page, you can make this Meeting Room available for use in ad-hoc conferences. This availability may be in addition to basic multipoint videoconferencing or exclusive for ad-hoc conferences.



Accord Meeting Room - Session Properties

Enable ad-hoc videoconferencing using this Meeting Room as follows:

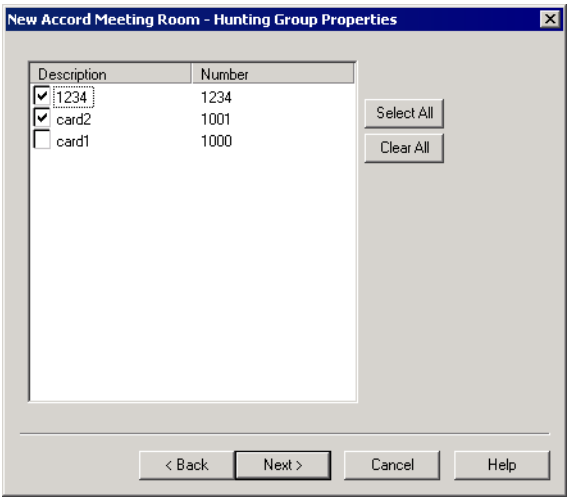
Use this service as an ad-hoc conference resource	Select to make this Meeting Room available for use when expanding to an ad-hoc videoconference.
Use this service exclusively for ad-hoc conferences	Select to make this Meeting Room available only for use in ad-hoc videoconferences, and unavailable for point-to-point sessions.
Ad-hoc Resources page	Click this link to open the MXM's Ad-hoc Resources Properties, in which you can also select which Meeting Rooms may be used for ad-hoc videoconferences (see "Ad-hoc Resources" on page 74).

Conference Settings

Voice Activated Switching	The participants see the video of the participant whose audio signal is strongest. For example, the non-speaking participants see the person speaking.
Continuous Presence	Several participants in a multipoint conference are viewed and heard simultaneously.
Bandwidth	The bandwidth available for each participant.

Hunting Group

In the Hunting Group Properties page, you can place specific H.323 cards (installed in the MGC) and/or other Accord hunting groups in the hunting group. Only selected cards may manage multipoint videoconferences that require this Meeting Room's services. The cards may be identified either by their prefixes or by their aliases.



Accord Meeting Room - Hunting Group Properties

Select any number of cards from the list to be in the hunting group.

- To place all cards in the hunting group, click **Select All**.
- To clear all the selections, click **Clear All**.

LDAP

The **LDAP** page provides information about the Meeting Room's registration, if applicable, in an LDAP (Lightweight Directory Access Protocol) server. For information about nodes' LDAP Properties, see "LDAP" on page 104.

A Meeting Room that's defined exclusively for ad-hoc videoconferences does not appear in the online directory.

Additional ID

In addition to its directory (E.164) number, a Meeting Room may have other addresses that may be used to dial it, such as additional E.164 addresses and/or H.323 Alias. In the **Additional ID** page, you may enter these, if applicable. For more information about adding Additional IDs, see "Additional IDs" on page 106.

13.4 Adding an Accord Gateway

If your organization is employing an Accord gateway for IP-to-ISDN and ISDN-to-IP videoconferences, prepare it for registration in the MXM by defining an appropriate Network H.323 Service configuration in the Polycom MGC. This configuration must include the MXM's IP address (in the Gatekeeper IP parameter), a prefix, and a span of cards that will be registered to the MXM.

Unlike the Accord IP cards, the gateway does not initiate a registration request with the MXM. You have to add the Accord Gateway node and its services to the MXM Administrator's Main View manually.

The setup of the Accord Gateway configuration for use in the MXM's network requires the following tasks:

- ❑ Set up the Network Services configurations for the gateway in the MGC (see "Network Services Configuration"on pages 216 to 226).
- ❑ Adding the Accord Gateway to the MXM Administrator's Main View (see "Adding the Accord Gateway to the Main View" on page 227).
- ❑ Adding gateway services to the Accord Gateway (see "Adding Accord Gateway Services" on page 232.

Network Services Configuration

First, you must set up the gateway's configuration for operation with your MXM. This process requires familiarity with the Polycom MGC. The tasks required to prepare the gateway's configuration in the MGC are:

- ❑ Creating ISDN Network Services
- ❑ Defining the Gateway's Network Parameters
- ❑ Defining the Gateway's H.320 and H.323 Session Profiles
- ❑ Associating ISDN Numbers with Specific H.323 End Points (optional)

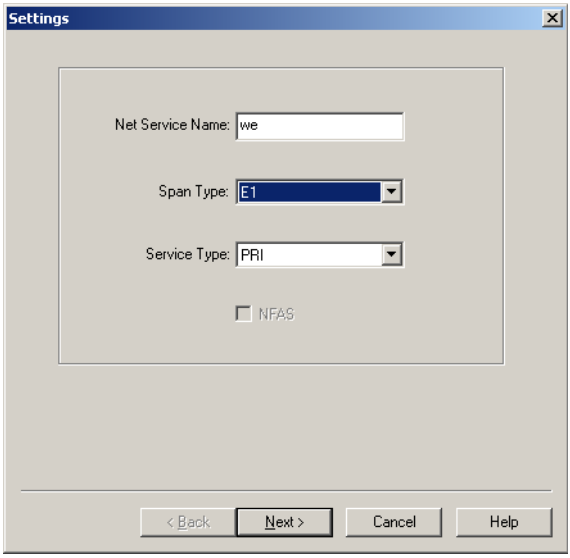
Creating ISDN Network Services

In the MGC, create new ISDN Network Services, or if you're editing an existing configuration, choose the one that you want to change.

➤ To create ISDN Network Services

1. In the left pane of the MGC Manager, browse to **Network Services**, right-click **ISDN** and select **New Network Service**.
2. In the Settings dialog box, enter the following information and click **Next**:

Net Service Name	Type a name for the ISDN service.
Span Type	Choose **E1** or **T1**, according to your region's communications infrastructure.
Service Type	Choose **PRI**.
NFAS	Do not select this option.

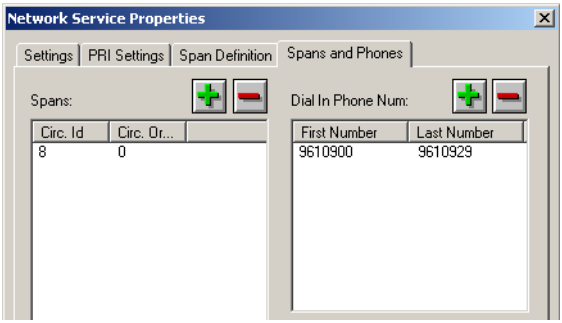


Creating a New ISDN Network Service

3 Keep the default PRI Settings and click **Next**.

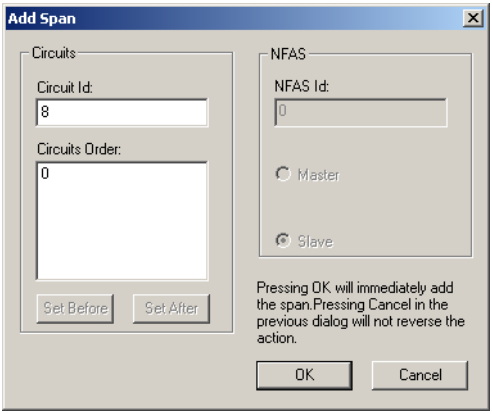
4 Keep the default Span Definition Settings and click **Next**.

5 In the Spans and Phones page, click the Spans + button.



Span and Phone Numbers Dialog Box

6 In the Add Span dialog box, type a **Circuit ID** number to identify this service. Click **OK**.

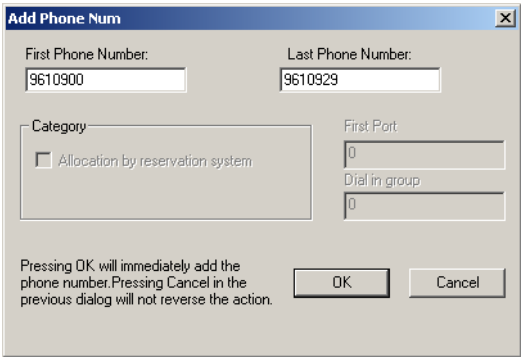


Assigning a Circuit ID

7 Click the Dial In Phone Number + button. 

In the Add Phone Num dialog box, define the range of ISDN numbers available for your organization's end points. Click **OK**.

Later, you may associate end points with their own ISDN numbers within this range, making those end points accessible by ISDN calls.

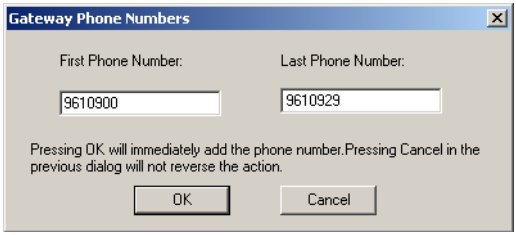


Assigning a Range of ISDN Numbers

8 Click the Gateway Range + button. 

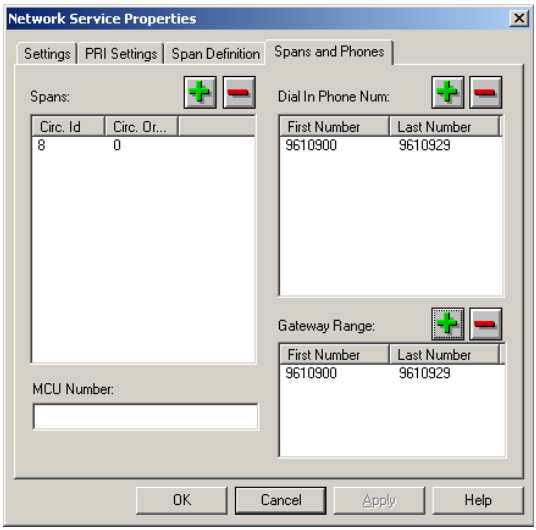
In the Gateway Phone Numbers dialog box, type the range of ISDN phone numbers available for associating with the gateway you create. Click **OK**.

When your organization's end points will call over ISDN, they have to dial this number to route the call through the gateway.



Assigning a Range of Available Gateway Numbers

9 Check that the Network Service Properties dialog box shows the correct span and phone number configurations (done in steps 5 to 8). If yes, click **OK**. If no, correct the erroneous item and then click **OK**.



Completed Span and Phone Numbers Configuration

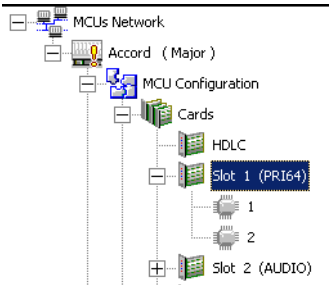
10 If you have additional BRIs, repeat this procedure to create additional services.

Defining the Gateway's Network Parameters

The next task of the gateway configuration is associating services with the gateway.

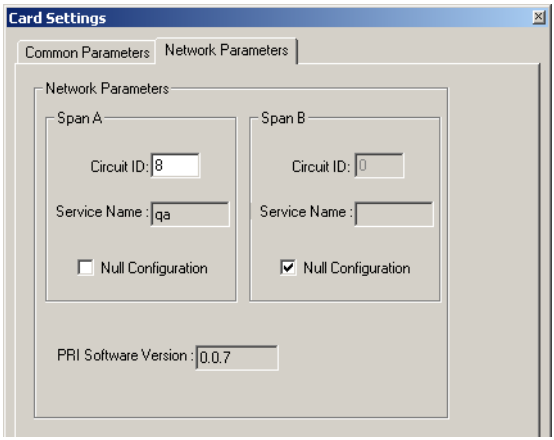
➤ To set the gateway network parameters

1 In the left pane of the MGC Manager, double-click the ISDN card's slot.



Selecting ISDN Card in MGC Manager

2 In the **Network Parameters** tab, deselect **Null Configuration**. Then, type the **Circuit ID** of the Service that you defined in the previous procedure (Step 6). Click **OK**.



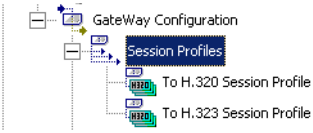
Defining the Gateway Card's Network Parameters

Defining the Gateway's H.320 and H.323 Session Profiles

A session profile includes parameters for routing a session through the gateway. It includes a service ID (which identifies the service in the MXM Administrator), available bandwidth for a call, and an associated gateway service (created previously - see "Creating ISDN Network Services" on page 216). You may define H.320 and/or H.323 session profiles, in accordance with your network requirements and infrastructure.

➤ To define session profiles

1. In the left pane of the MGC Manager, browse to Gateway Configuration>Session Profiles, right-click **To H.320 Session Profile** and click **New Session Profile**.

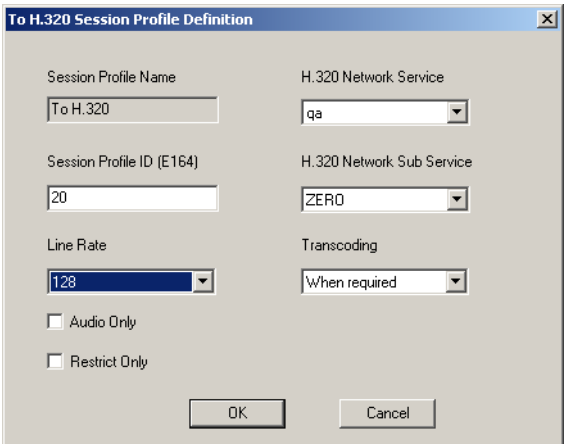


Selecting a New H.320 Session Profile

2. Define the following for the Session Profile:

Session Profile Name	Enter a name for this profile.
Session Profile ID	Specify an ID number. Write this number down - you will need to identify this service with this number when you add it later to the MXM Administrator.
Line Rate	Available bandwidth for this service.
H.320 Network Service	Name of the gateway service that you previously created.

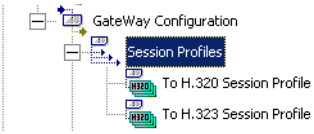
3. Leave the default settings for the remaining parameters.
4. Click **OK**.



Setting Up an H.320 Session Profile

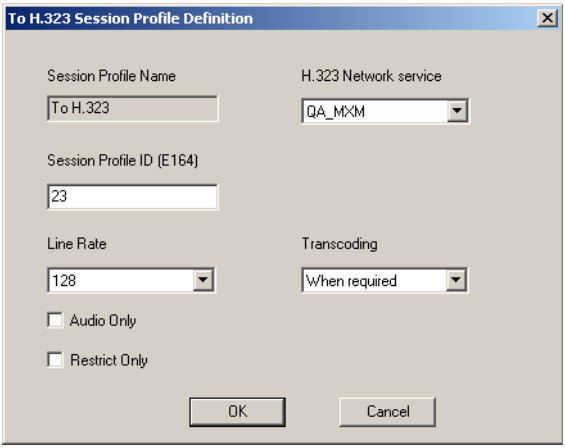
5 Repeat Steps 1 to 4 to define additional profiles.

6 In the left pane of the MGC Manager, right-click **To H.323 Session Profile** and click **New Session Profile**.



Selecting a New H.323 Session Profile

7 As in Step 2 above, specify a **Name**, **Profile ID**, **Line Rate** for the H.323 Session Prolfile. In addition, choose a previously created **H.323 Network Service**. Click **OK**.



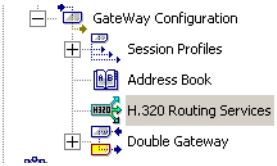
Setting Up an H.323 Session Profile

8 Repeat Steps 6 to 7 to define additional profiles.

Associating ISDN Numbers with Specific H.323 End Points

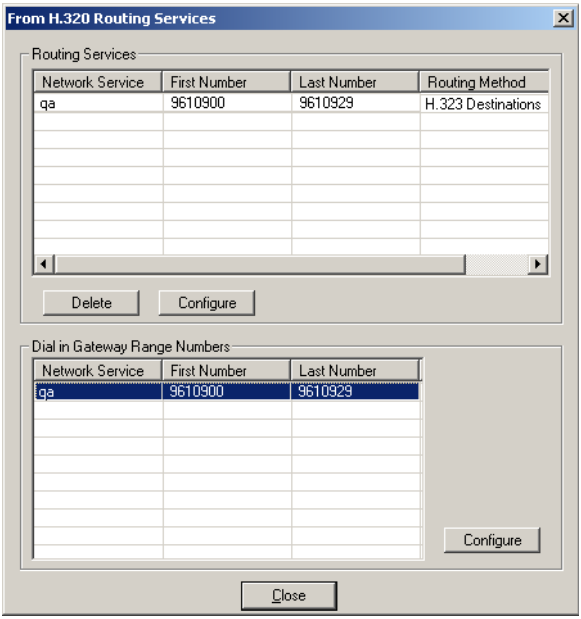
Optionally, you may associate end points with their own ISDN numbers within the range previously defined, making those end points accessible by ISDN calls.

1 Under Gateway Configuration, right-click **H.320 Routing Services** and click **Properties**.



Selecting H.320 Routing Services

2 In the Dial in Gateway Range Numbers table, select the previously created **Network Service** and its range of ISDN numbers. Click **Configure**.

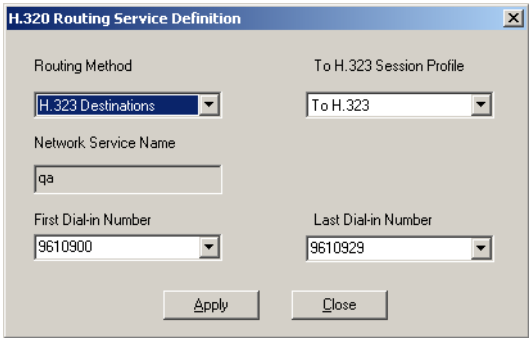


H.320 Routing Service Configuration

3 Define Routing Service parameters as follows:

Routing Method — Choose **H.323 Destinations**.

First/Last Dial-in Number — Choose a range that's within the range of available ISDN numbers that you specified for this gateway.



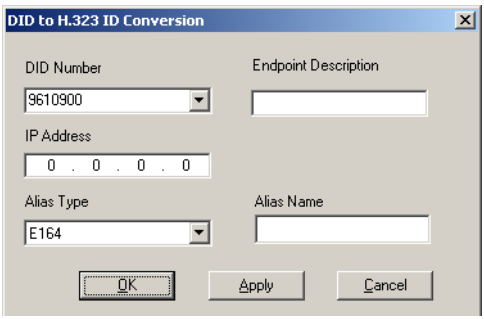
Defining H.320 Routing Service

Click **Apply**.

After a Successful Configuration message appears, click **OK**.

4 In the Routing Services table, select the ISDN **Network Service** with its range of ISDN numbers. Click **Configure**.

5 Associate specific ISDN numbers to specific end points. In the H.320 Routing Service Definition dialog box, click the + button.

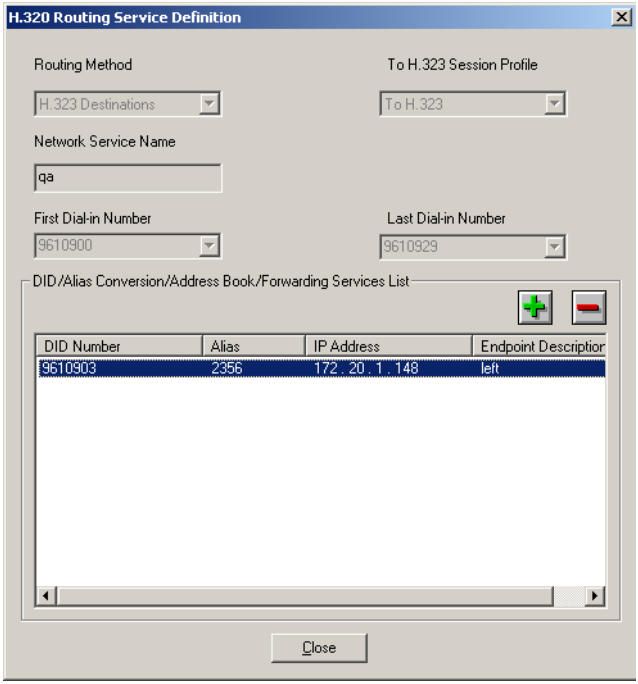


Associating ISDN Number with H.323 End Point

6 In the **DID Number** list, choose an ISDN number.

7 Enter the details for the H.323 end point (**Alias Type**, **Alias Name**, and **Endpoint Description**).

8 Click **Apply** and repeat steps 6 and 7 to associate additional ISDN numbers to end points. When you finish, click **OK**.



List of ISDN Numbers to H.323 Routing

13.5 Adding the Accord Gateway to the Main View

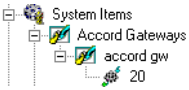
After the gateway configuration is set up in the Polycom MGC, the gateway does not initiate a registration request with the MXM. You have to add the Accord Gateway node and its services to the Main View manually.

➤ To add an Accord Gateway to the Main View

1 In the Main View's toolbar, click the New Accord Gateway button . The New Accord Gateway Wizard appears.

2 Change properties according to your videoconferencing specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see the following section, "Setting Accord Gateway Properties".

3 When you finish the last page, click **Finish**.



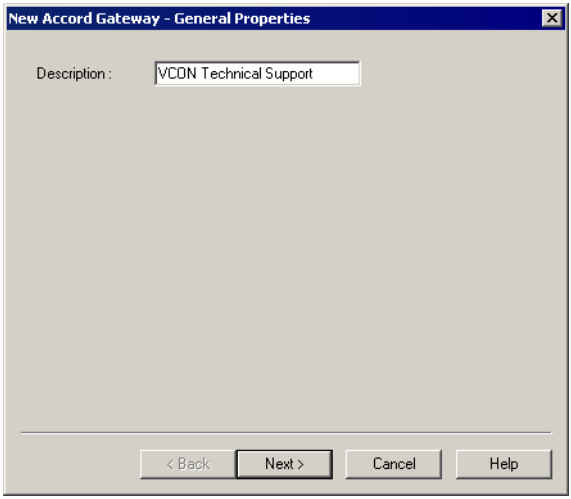
Accord Gateway in Main View

13.6 Setting Accord Gateway Properties

In step 2 of "Adding an Accord Gateway" on page 227, the New Accord Gateway wizard provided the chance to change various gateway properties. This section describes these properties.

General

The **General** page contains a **Description**, such as a name, of the Accord gateway.

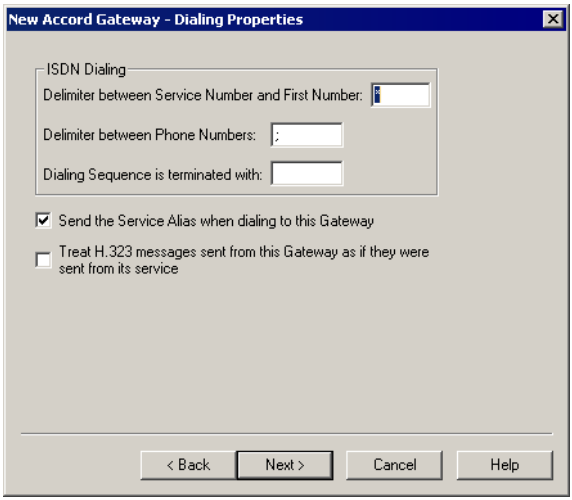


New Accord Gateway - General Properties

Dialing

Dialing conventions vary among gateways, according to the manufacturer's design and configuration. Refer to your gateway's documentation for the specific delimiters or other characters that are required to access the gateway's services.

The values entered in this page must be identical to the dialing configuration of the gateway.



New Accord Gateway - Dialing Properties

Delimiter between Service Number and First Number — Type the character, if applicable, that the MXM adds before the first ISDN number. For Accord gateways, the default delimiter should be an asterisk (*).

Delimiter between Phone Numbers — Type the character, if applicable, that the MXM adds between each ISDN number to be dialed. For Accord gateways, the default delimiter should be a semi-colon (;).

Dialing sequence is terminated with	Type the character, if applicable, that the MXM must enter at the end of the dialing string. For Accord gateways, by default, this box should be blank.
	All of the above values must be identical to the dialing configuration of the Gateway
Send the Service Alias when dialing to this Gateway	Video gateways support multiple services. If the gateway's dialing syntax requires the inclusion of the service number, select this option.
Treat H.323 messages sent from this Gateway as if they were sent from its service	Select this option if the gateway does not define services. The MXM will handle messages sent through the gateway as H.323 64K Voice messages. For Accord Gateways, we recommend leaving this option unselected (default).

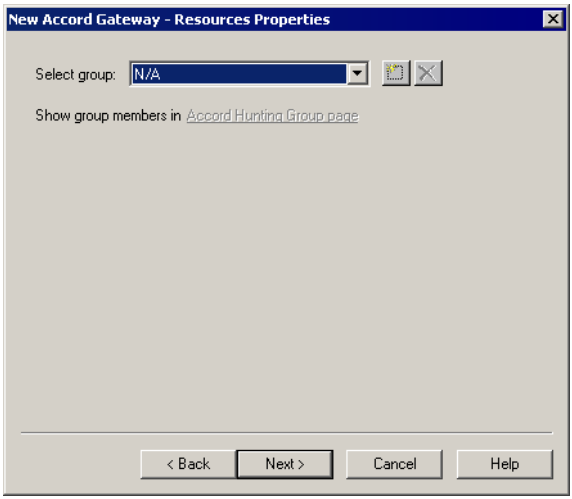
Resources

To provide access to the Accord gateway services, you then have to place Accord cards (which includes the span of cards configured in the Polycom MGC) in one or more Accord hunting groups. MXM nodes must dial the hunting group prefix in order to receive these services.

If the span includes more than one card, an Accord hunting group is automatically created in the MXM Administrator's Main View. If the span includes ONLY one card, you have to manually create an Accord Hunting Group which includes this single card.

To provide access to the Accord Gateway services, you then have to assign the Accord Hunting Group to each registered Accord gateway.

In the **Resources** page, select the hunting group for this gateway from the **Select Group** list. If you need to add a new hunting group, perform the following procedure.



New Accord Gateway - Resources Properties

➤ To add a new hunting group

1 Click the Add New Hunting Group button . The New Accord Hunting Group Wizard appears.

2 Enter a **Directory Number** (E.164) and a **Description**.

The E.164 number must be identical to the Network H.323 Service prefix as defined in the cards' configuration in the Polycom MGC.

To go to the next page, click **Next**.

3 In the Hunting Group Properties page, select the Accord services (cards) that will belong to this hunting group.

4 Click **Finish**. The new hunting group now appears in the Accord gateway's Resources Properties.

To delete a hunting group, select it in the list and click the Remove Accord Hunting Group button.

Call Routing

In the **Call Routing** page, enter the physical location of the gateway and define the cost rates for using the gateway's services.

When you run a Least Cost Routing test to find available gateway services and costs for a gateway call to a certain location, the resulting cost estimates will be based on the cost rates defined here (see "Testing for the Optimal Gateway Service" on page 147).

For a description of the Call Routing page, see "Call Routing" on page 136.

13.7 Adding Accord Gateway Services

The Accord Gateway does not initiate registration of itself and its services with the MXM. Therefore, you have to manually add the Accord Gateway's services under the Accord Gateway node in the Main View.

Make sure to choose only services that are defined as ISDN services in the Polycom MGC.

➤ To add an Accord Gateway Service

1. In the Main View's toolbar, click the New Gateway Service button . The New Gateway Service Wizard appears (for descriptions of the properties, see "Setting Gateway Service Properties" on page 139).
2. Define **Directory Number** and **Bandwidth** of the service *exactly* as they are defined in the Polycom MGC configuration (Directory Number = H.320 Session Profile ID - see page 221). When you finish each page of the wizard, click **Next**.
3. When you finish the last page, click **Finish**.

14 NEIGHBORING ZONES

14.1 The MXM's Relationship with Neighboring Zones

In addition to its own registered nodes, the MXM provides an organization with the ability to carry on videoconferences with nodes outside its administrative area. These nodes may be managed by other MXMs or third-party Gatekeepers, or unregistered with any management device.

The collections of nodes that MXMs and Gatekeepers register and manage are called *zones*. Multiple zones may be listed in the Administrator's system tree, where you may manage the communication between them and the local MXM.

Neighboring zones may be added automatically if calls are made between it and the local MXM's zone, or added manually by you. Additional zones must be configured, according to the inter-zone management policy that you implement. After zones are added to the tree, you may manually add entries for end points, MCUs and Gateways that are registered in those zones.

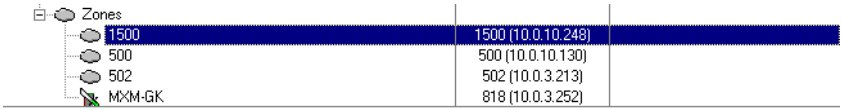
After zones are set up in the Administrator Main View, you can perform the following inter-zone management tasks (see "Inter-Zone Videoconferencing Management" on page 251):

- ❑ Start a point-to-point videoconference between two end points
- ❑ Setting up a dialing plan, which defines how to dial users in other zones
- ❑ Restrict the bandwidth allotment for inter-zone videoconferences
- ❑ Generate Call Details Records (CDR) records for inter-zone videoconference calls
- ❑ Share gateway services and MCU services with neighboring zones
- ❑ Restrict the use of exchange features such as Call Transfer and Call Forwarding.

14.2 Logging in New Zones

Inter-zone functions are available between the local MXM and zones known to it. Neighboring MXMs or Gatekeepers may be listed in the MXM automatically or manually.

Registered MXMs and Gatekeepers appear on the system tree under the Zones object. You can manually add any *neighbor node* (end point, MCU, or gateway) from a specific zone under that same zone in the Administrator. You can then initiate calls involving these nodes and manage their MXM configuration (see "Setting End Point MXM Properties" on page 91) in the same way as nodes registered with the local MXM (*MXM node*).



Listing of Neighboring MXMs and Gatekeepers

Adding Zones Automatically

The MXM System Properties include an option for adding zones in Open Mode. If this option is selected, the MXM will automatically add other MXMs' and Gatekeepers' zones only after one of the following occurs:

- ❑ The local MXM tries to dial using the Multicast search method.
- ❑ An incoming call from another zone arrives.

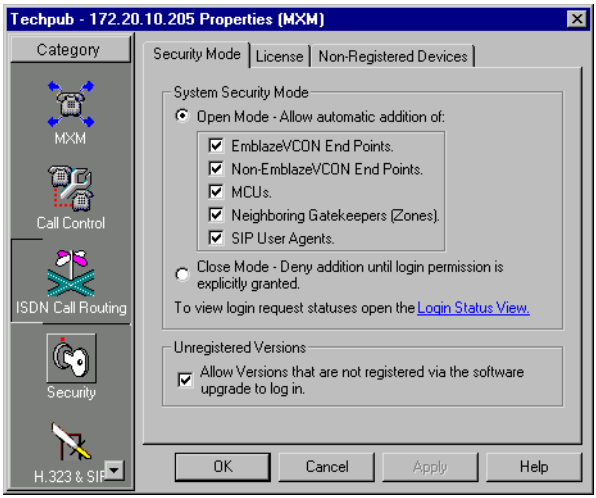
Discovered zones are listed in the Administrator (see the illustration above).

➤ To add zones automatically

1. Right-click the MXM node, point to **Property** and then **Security**, and click **Security Mode**. The **Security Mode** tab opens.
2. Select the **Open Mode** and **Neighboring Gatekeepers (Zones)** options. The other MXMs and/or gatekeepers must also be in Open Mode.
3. Click the **H.323 & SIP** icon on the left side of the dialog box. By default, the **Zone Settings** tab is open.

4 We recommend the Multicast search technique for searches of zones and neighboring nodes. Select **First Multicast Location Requests, then in Defined Zones** (default selection) or **Send Multicast Location Requests** (see "Zone Settings" on page 84).

5 Click **OK**.



Setting Open Mode for Neighboring MXMs and Gatekeepers

Adding Zones Manually

If the MXM is in Closed Mode for zones, neighboring MXMs and Gatekeepers may only be added to the Administrator manually. In this process, you must define or confirm each node's properties.

➤ To add a zone manually

1 Click the New Zone button. The New Zone Wizard appears. The original property values are the default values defined in the Zone template (see "Setting Up Templates" on page 47)

2 Change properties according to your network specifications, or keep the default settings. When you finish each page of the wizard, click **Next**. For explanations about the various properties, see "Setting Zone Properties" on page 236.

3 When you finish the last page, click **Finish**.

14.3 Setting Zone Properties

The main objective of defining zone properties is the definition of policies and the allocation of bandwidth for inter-zone videoconferences. This section describes these properties.

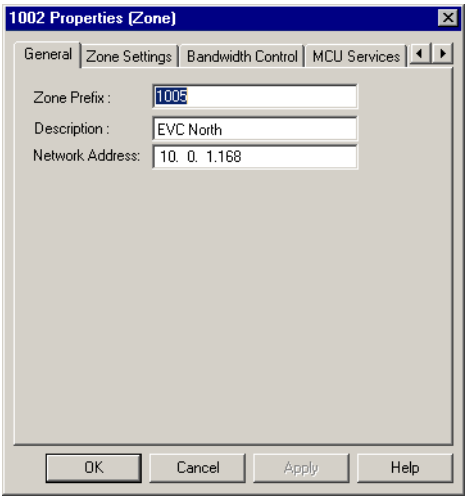
➤ To define zone properties

1. Double-click a neighboring zone. The zone's Properties dialog box appears.
2. Define the zone properties according to your network's videoconferencing needs and specifications, or keep the default settings.
3. To implement the changes and proceed to another tab in the dialog box, click **Apply** and then the appropriate tab.
4. To implement all the changes and close the dialog box, click **OK**.

The following sections describe the zone properties.

General

The **General** tab contains identity information of the new MXM or Gatekeeper.



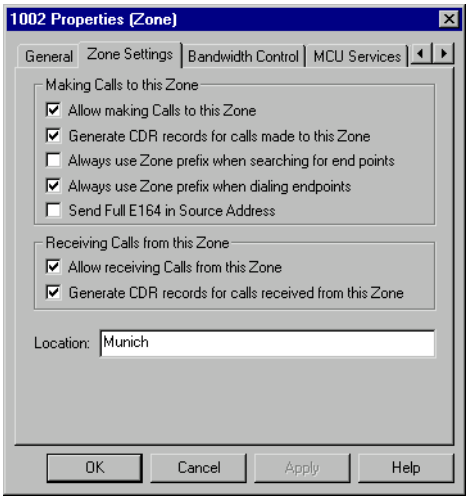
Zone - General Properties

In the **General** Properties tab, the following properties appear:

Zone Prefix	Directory number (E.164 number) assigned to the MXM or Gatekeeper. The zone prefix functions as an "area code," which may be used by the MXM to dial nodes in the selected zone (to enable zone prefix dialing, see the next section, "Zone Settings").
Description	Identifying name of the zone. This name will appear in the Main View.
Network Address	IP address of the zone's MXM or Gatekeeper.

Zone Settings

In the **Zone Settings** tab, define the local MXM's intercommunication relationship with the neighboring zone. This relationship includes permission to make and receive calls, generation of CDR reports, and the use of prefixes when dialing.



Zone - Zone Settings Properties

In the **Zone Settings** Properties tab, the following properties appear:

Making Calls to this Zone

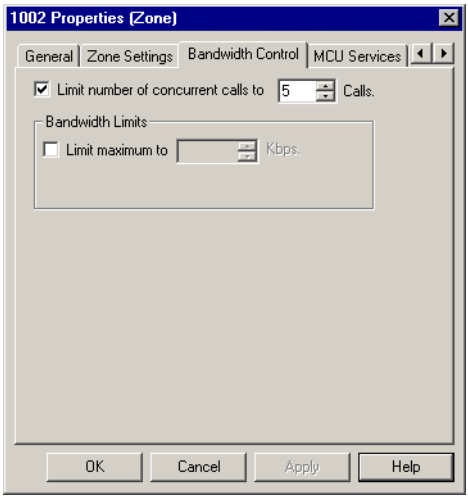
Allow Making Calls to this Zone	If selected, all local MXM nodes may start videoconferences with neighbor nodes registered in this zone.
Generate CDR records for calls made to this Zone	If selected, all calls to neighbor nodes in this zone will be listed in a Call Details Record (CDR). For more details about CDRs, see **Getting Started>Monitoring System Status>Call Accounting** in the MXM's online help.
Always use Zone prefix when searching for end points	Select this option to enable searching for end points in gatekeepers that require a full zone prefix in the setup message (for example, when using a Radvision ECS gatekeeper in non-stripping mode).
Always use Zone prefix when dialing end points	Select this option to enable dialing to gatekeepers that require their zone prefix in the dialing syntax (non-Emblaze-VCON gatekeepers). To dial nodes managed by these gatekeepers, users must receive the appropriate prefixes from the system administrator or from the remote party.
Send Full E.164 in Source Address	If selected, the local MXM will add the local area code and directory number (E.164) to the ID information of any outgoing call from the local MXM to this zone.

Receiving Calls from this Zone

Allow receiving calls from this zone	If selected, local MXM nodes may receive videoconference calls from neighboring nodes registered in this zone.
Generate CDR records for calls received from this Zone	If selected, all calls from neighbor nodes in this zone will be listed in a Call Details Record (CDR). For more details about CDRs, see **Working with the MXM>Reporting Option>Call Accounting** in the MXM's online help.
Location	Enter a general physical location of the zone's MXM or Gatekeeper and its end points

Bandwidth Control

In the **Bandwidth Control** tab, you can define the available amount of bandwidth for all concurrent videoconferencing calls between the local zone and the neighboring zone.



Zone - Bandwidth Control Properties

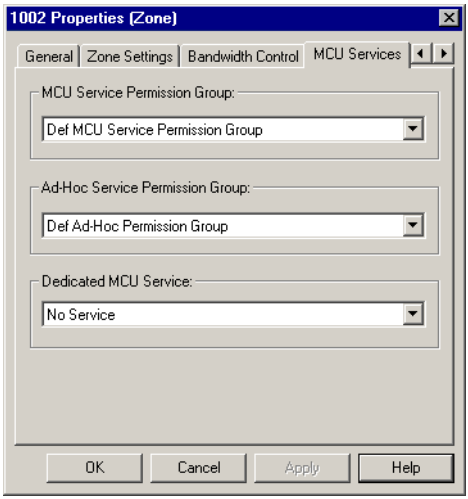
Set bandwidth control properties as follows:

Limit Number of Concurrent Calls to — Select the maximum number of calls between the two zones at the same time. The default setting is **5**.

Limit Maximum to — Select this option to define the total available bandwidth that the local MXM allocates to all calls to the neighboring zone. In the list, select the bandwidth.

MCU Services

In the **MCU Services** tab, define how the local MXM allocates MCU resources for incoming videoconferencing calls from the neighboring zone.



Zone - MCU Services Properties

MCU Service Permission Group

If you want to limit the usage of MCU services during incoming videoconferences from the neighboring zone, select an MCU Service Permission Group. The available options are all MCU Service Permission Groups that are listed in the current Administrator Main View. For more information about MCU Service Permission Groups, see "MCU Service Permission Groups" on page 160.

To disable the selection of MCU services, select No Group. As a result, nodes in the neighboring zone will not be able to participate in MCU-managed videoconferences that include nodes from the local MXM's zone.

Ad-hoc Service Permission Group

Select the name of the Ad-hoc Service Permission Group from which the neighboring zone's end points can choose a service for initiating an ad-hoc conference to the local zone. For more information about Ad-hoc Service Permission Groups, see "Ad-hoc Permission Groups" on page 164.

Dedicated Service

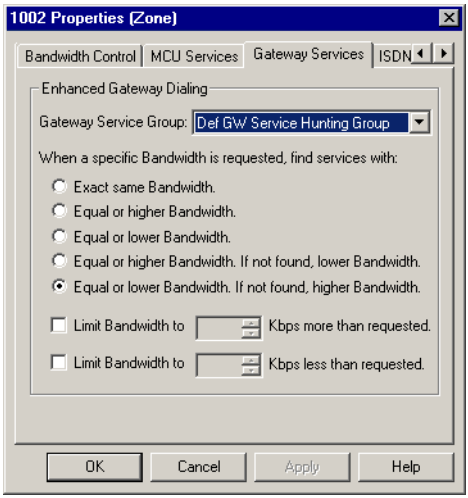
A dedicated service is an ad-hoc service resource that may be used only if any of the neighboring zone's end points are in the resulting ad-hoc conference (either one of the original two end points of the conference or the invited end point).

If you want to dedicate a specific MCU or VCB service for this neighboring zone's end points, select the service from the list.

To be a dedicated service, the service must be set up as an ad-hoc resource. See "Session" on page 158.

Gateway Services

In the **Gateway Services** tab, define how the local MXM allocates gateway resources for incoming videoconferencing calls from the neighboring zone.



Zone - Gateway Service Properties

Gateway Service Group

Select the Gateway Service hunting group that defines the services that will be available for incoming videoconferences from the neighboring zone. If a neighbor node dials the defined gateway access number (default is "**9**"), it may use any of the included services within that particular Service group.

The available options are all Gateway Service hunting groups that are listed in the current Administrator Main View (see "Gateway Service Hunting Groups" on page 141).

Some calls from the neighboring zone through a gateway may specify a required bandwidth. The following options define how the MXM allocates bandwidth in this situation:

Exact same bandwidth

Provide a choice only among services that provide the exact bandwidth required.

Equal or higher bandwidth

Provide a choice only among services that provide the exact bandwidth required or more.

Equal or lower bandwidth

Provide a choice only among services that provide the exact bandwidth required or less.

Equal or higher bandwidth - if not found, lower bandwidth

Provide a choice among services that provide the exact bandwidth required or more. If none exist, then offer services allocating lower than required bandwidth.

Equal or lower bandwidth - if not found, higher bandwidth

Provide a choice among services that provide the exact bandwidth required or less. If none exist, then offer services allocating higher than required bandwidth.

Limit bandwidth to ___ Kbps more (or less) than requested

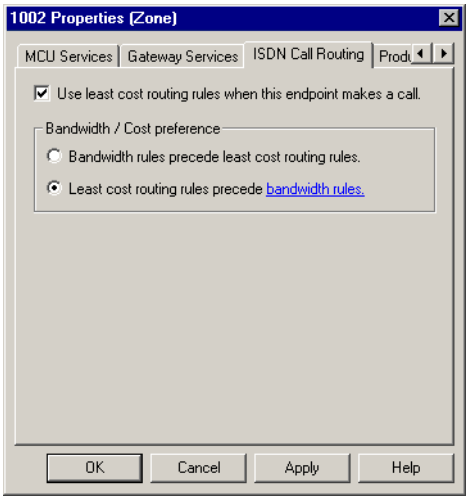
Select the appropriate option to enable only a specific amount of deviation (higher or lower) from the requested bandwidth. From the appropriate list, choose the amount of deviation (in Kbps) allowed.

For example, if you want to allow no more than an additional 128 Kbps, then choose **128** from the appropriate list.

ISDN Call Routing

In the **ISDN Call Routing** tab, define how the MXM decides how to route gateway calls from this zone. The MXM can prioritize between several sets of gateway routing rules:

- Least Cost Routing Rules (see "Testing for the Optimal Gateway Service" on page 147)
- Bandwidth Rules (nodes' Properties **Gateway Services** tab - see "Gateway Services" on page 99)



Zone - ISDN Call Routing Properties

Set ISDN Call Routing properties as follows:

Use least cost routing rules when this end point makes a call — Select to allow the MXM to apply least cost routing to gateway calls from this zone.

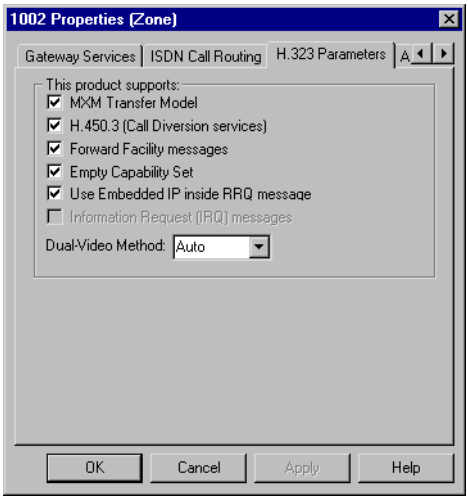
Bandwidth/Cost Preference

Select one of the following:

Bandwidth rules precede least cost routing rules	When initiating a gateway call, the MXM chooses a gateway service based on the rules defined in the initiating end point's Service properties.
Least cost routing rules precede bandwidth rules	When initiating a gateway call, the MXM chooses the most efficient gateway service based on the application of the least cost routing rules.

H.323 Parameters

In the **H.323 Parameters** tab, select the exchange functionalities that are supported by the neighboring zone's MXM or gatekeeper.



Zone - H.323 Parameters Properties

MXM Transfer Model — If selected, videoconferences between neighbor nodes and MXM nodes may be transferred to another end point

H.450.3 (Call Diversion services — If selected, calls between the neighboring zone and the local MXM's zone may be forwarded according to the capabilities of H.450.3. It provides additional information about forwarded calls than Forward Facility does, such as the original destination of the call.

Forward Facility messages — If selected, calls between the neighboring zone and the local MXM's zone may be forwarded according to Forward Facility capabilities. A forwarded call does not provide information about the redirection.

If the neighboring zone supports both H.450.3 and Forward Facility, we recommend enabling H.450.3.

Empty Capability Set — If selected, video and audio stream channels in a call are temporarily closed while a call transfer takes place between the neighboring zone and the local MXM's zone. This selection also enables the joining of neighbor nodes in ad-hoc videoconferences.

Use Embedded IP Inside RRQ Messages	In response to registration requests (RRQ) from the neighboring zone, the MXM will send response to the IP address specified in the RRQ.

Additional IDs

In addition to its zone prefix, a neighboring zone may have additional prefixes to which its nodes may be dialed, such as additional E.164 addresses and/or H.323 IDs (node name).

For more information about adding Additional IDs, see "Additional IDs" on page 106.

Redundancy

In addition to its main gatekeeper (as defined in this configuration), a neighboring zone may also have redundant gatekeeper IP addresses. The zone's administrator should activate one of the IP addresses at a time (not controllable from the local zone's MXM).

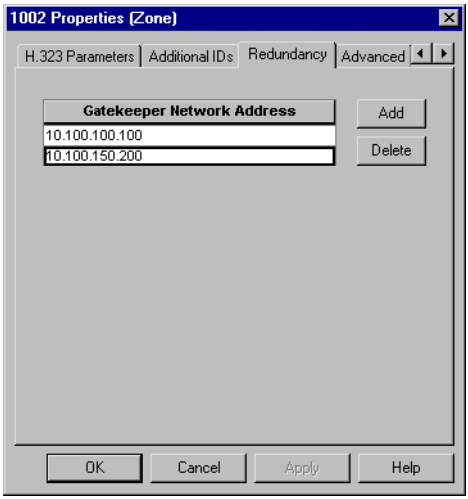
When a call is made from the local zone to this zone, the local MXM tries to route the call through the active gatekeeper. If more than one gatekeeper is active, the MXM routes the call through the first gatekeeper that responds to the MXM's Location Request (LRQ).

➤ To add a redundant gatekeeper

1. In the **Redundancy** tab, click **Add**. An entry line appears in the Gatekeeper Network Addresses table.
2. Type the IP address of the gatekeeper.
3. To add another gatekeeper , repeat steps 1 and 2.

➤ To delete a redundant gatekeeper

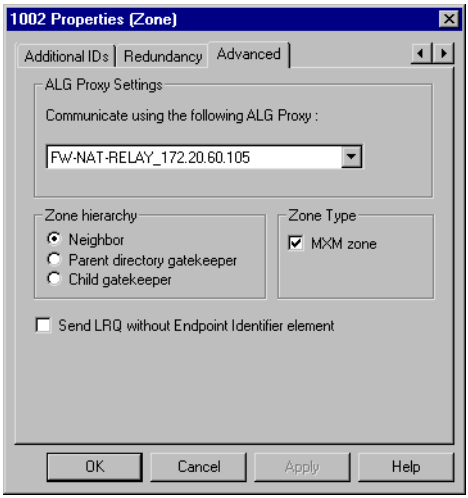
1. In the **Redundancy** tab, select the gatekeeper entry.
2. Click **Delete**.



Zone - Redundancy Properties

Advanced

In the **Advanced** tab, define the local MXM's intercommunication relationship with the neighboring zone.



Zone - Advanced Properties

Set Advanced Properties as follows

ALG Proxy Settings

Communicate using the following ALG Proxy — If at least one ALG Proxy is installed between the local MXM and this neighboring zone, select the ALG Proxy through which the MXM will automatically address calls to the neighboring zone.

Zone Hierarchy

Neighbor — The selected zone is a neighboring zone. Nodes registered in the local MXM zone may carry on videoconferences with nodes registered in the selected zone.

Parent Directory Gatekeeper	The selected zone contains records of gatekeepers and nodes within its domain, which is usually a LAN or WAN covering a local region. Within the network, Location Requests (LRQ) arrive here from other MXMs and gatekeepers. The directory gatekeeper switches the request and the call to the zone in which the destination node resides. For more information about directory gatekeepers, see "Directory Gatekeepers" on page 254.
Child Gatekeeper	The selected zone covers an area inside a parent gatekeeper's domain which is identified by a specific dialing prefix.

Zone Type

MXM Zone	Select this option if an MXM provides management and gatekeeper services to this neighboring zone. If the zone is managed by a non-Emblaze-VCON gatekeeper, deselect this option.
Send LRQ Without End Point Identifier Element	Select this option if the neighboring zone is managed by a Cisco MCM or another gatekeeper that does not accept end point identifier elements.

14.4 Permanent Non-Registered Devices

There may be situations where nodes will not register with any gatekeeper, but should still be available for videoconferencing with registered end points. In such a case, you can make the node known to the MXM by listing it as a *permanent non-registered device*.

Adding a Permanent Non-Registered Device

A non-registered node may be "discovered" if it is in a videoconference with an MXM node. In such a case, the non-registered node appears on the system tree under the Non-registered Devices object during the duration of this call. The administrator may then permanently add the node to the tree (depending on the system Non-registered Device Properties - see page 83).

Non-registered Device Appearing in Main View

➤ To add a non-registered node to the system tree

1. Right-click the node and then click **Make Permanent**. The New Permanent Non-registered Device Wizard appears.
2. Set the properties according to your system specifications. When you complete a page, click **Next** to advance to the next properties page). For explanations about the various properties, see "Setting End Point MXM Properties" on page 91.
3. Click **Finish** to exit the wizard.

14.5 Inter-Zone Videoconferencing Management

You can perform the following inter-zone management tasks:

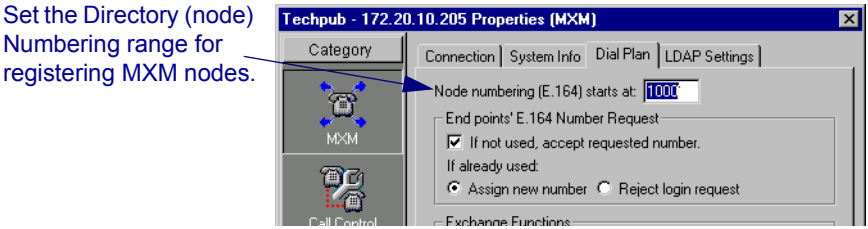
- ❑ Setting up a dialing plan, which defines how the MXM starts point-to-point videoconferences between MXM nodes and neighbor nodes, or with a non-registered node.
- ❑ Restrict the bandwidth allotment for inter-zone videoconferences
- ❑ Restrict the use of exchange features such as Call Transfer and Call Forward.
- ❑ Sharing gateway resources with other zones.

Setting Up Inter-Zone Dialing

If your organization contains more than one MXM or other gatekeepers, you likely want to provide the ability of end points to videoconference with nodes in the other zones, as well as to zones outside the organization. This section explains how to set up the relevant configurations to permit inter-zone videoconferencing.

To permit dialing between nodes in different zones, the MXMs and the relevant zones must have a specific configuration. Perform the following tasks:

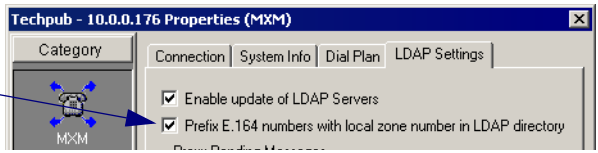
1 Within your own organization, we recommend that you assign different directory numbering ranges in all MXMs. If identical directory numbers exist in different zones, zone prefixes must be added to numbers when dialing, and must be added to the node configurations (for more details, see "Dial Plan" on page 67).



Setting a Directory Number Range for the MXM

2 If your organization is using an online directory (such as ILS or NDS), enable the zone prefix to be appended to each entry's configuration. If a node is moved to a different zone, the MXM also updates the prefix in the online directory (for more details, see "LDAP Settings" on page 70).

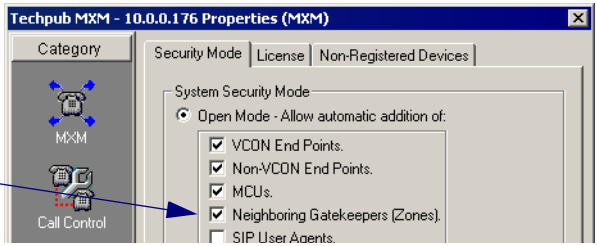
Enable the zone prefix to be appended to each entry's configuration in online directories.



LDAP Settings Properties

3 All of the respective zones must be known to each other. If the MXM is set to Open Mode registration, any neighboring zones managed by MXMs and H.323 gatekeepers may be listed automatically in the Main View. If the MXM is set to Closed Mode registration, you have to add the neighboring MXMs and gatekeepers to the Main View manually (to set the MXM to Open or Closed Mode, see "Security Mode" on page 79).

Set Open Mode for Neighboring Gatekeepers (Zones)

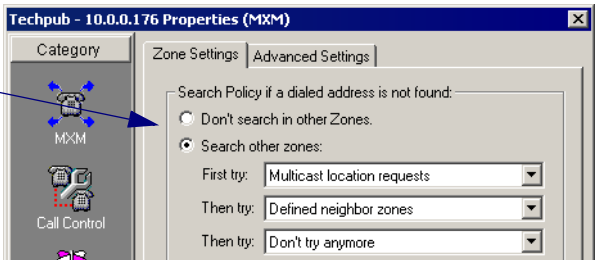


Open Mode for Adding Neighboring MXMs and Gatekeepers

Make sure that the zone prefixes (directory numbers) are listed identically in all known MXMs and gatekeepers.

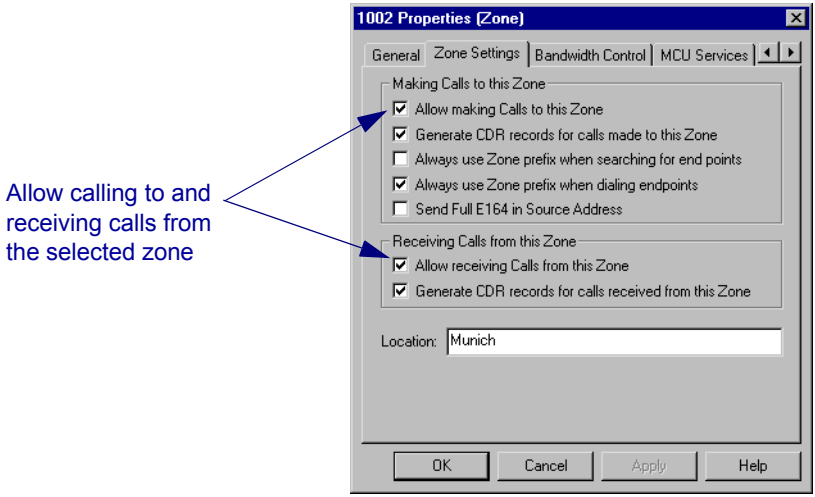
4 Inter-zone search for addresses must be enabled in the MXMs. You can set the MXMs to search using a combination of the Multicast Location Requests, Defined Neighbor Zones, and Directory Gatekeeper methods. See the figure on the next page (for more details, see the MXM's "Zone Settings" on page 84).

Select the method of searching for addresses in other zones



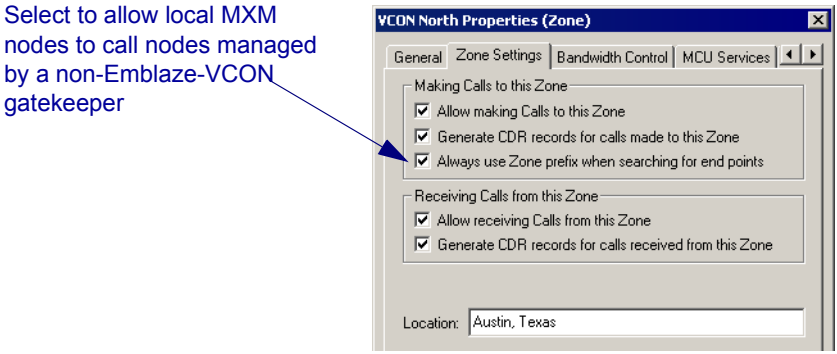
Selecting Address Search Method

5 The ability to receive and send calls must be enabled in the Zone Settings of each relevant zone's properties (for more details, see the zone's "Zone Settings" on page 237).



Allow Videoconferences Between this Zone and the Local Zone

6 To enable dialing to gatekeepers that require their prefix in the dialing syntax (non-Emblaze-VCON gatekeepers), select the **Always use Zone prefix when searching for end points** option in the Zone Settings of the zone. To dial nodes managed by these gatekeepers, users must receive the appropriate prefixes from the system administrator or from the remote party (for more details, see the zone's "Zone Settings" on page 237).



Allow Videoconferences Between a Zone Managed by a non-Emblaze-VCON Gatekeeper and the Local Zone

Directory Gatekeepers

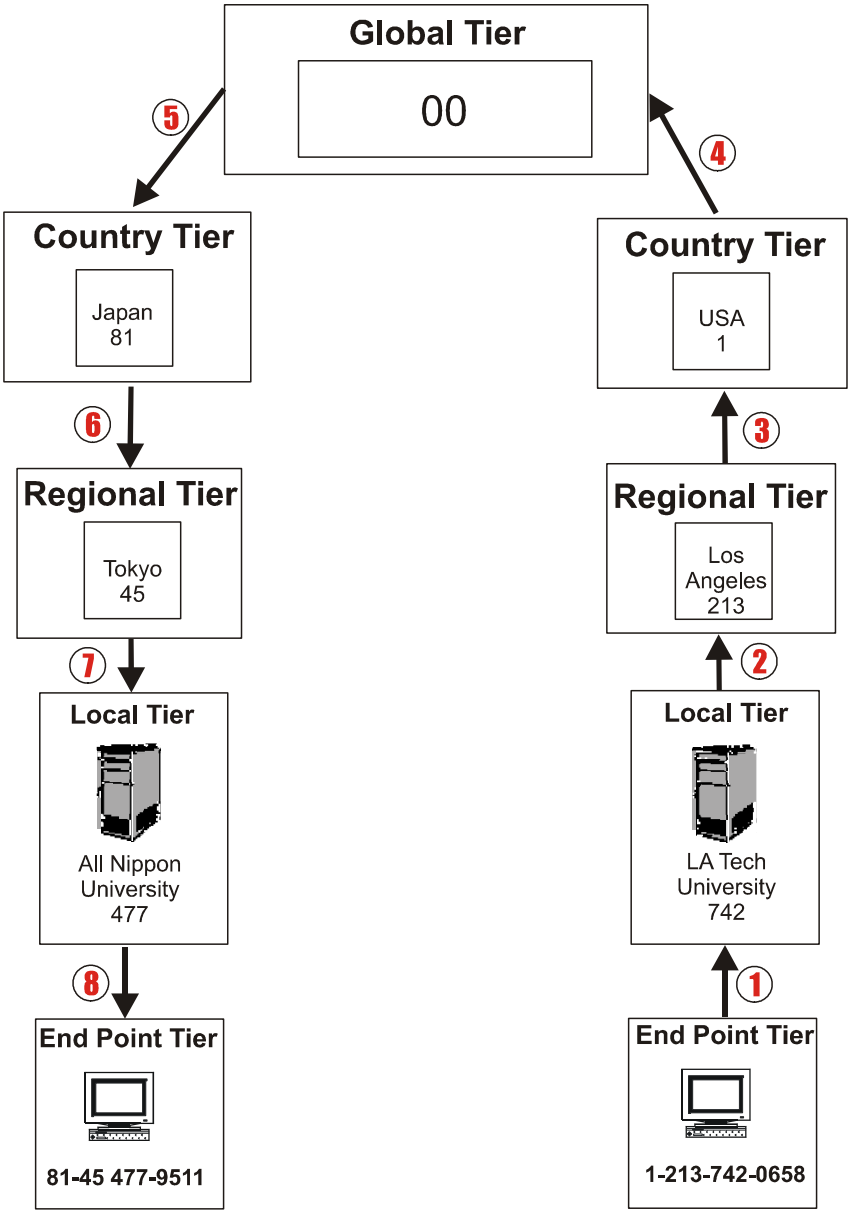
Directory gatekeepers are used for connecting neighbor gatekeepers and end points over WANs. They simplify the process of searching for dialed addresses in different zones over large areas.

The MXM can operate within a network that includes a hierarchy of directory gatekeepers (DGK). A typical hierarchy maintained by telephony and Internet service providers may include a global gatekeeper, country gatekeepers, regional and local gatekeepers. By concentrating address searches through such a hierarchy, an organization can significantly simplify the search and connection process.

A typical DGK hierarchy is based on parent-children-type relationships among the gatekeepers, including MXMs. The following is a sample hierarchy:

Tier	Parent/Child Relationship
Global gatekeeper	Children - Country gatekeepers
Country gatekeeper	Parent - Global gatekeeper Children - Local gatekeepers
Regional or Local gatekeeper	Parent - Country gatekeeper Children - End points
	 MXMs are usually located within the Regional/Local tier. Depending on the size and range of the network, there may be multiple layers of regional and/or local directory gatekeepers.
End point	Registered with Local MXM/gatekeeper

If the Search policy among your network is set to Directory Gatekeepers, the MXM routes calls to its parent directory gatekeeper, which searches its database to see if the prefix of the dialed number is known to it. If not, the parent gatekeeper routes the call to its parent gatekeeper, and so on, if necessary, until it reaches the global gatekeeper. The global gatekeeper then routes the call to a child gatekeeper matching the prefix. From this point, each gatekeeper continues switching the call to the appropriate child entity (according to area codes and local exchange codes).



Sample Call Through Directory Gatekeeper Hierarchy

Illustration Legend

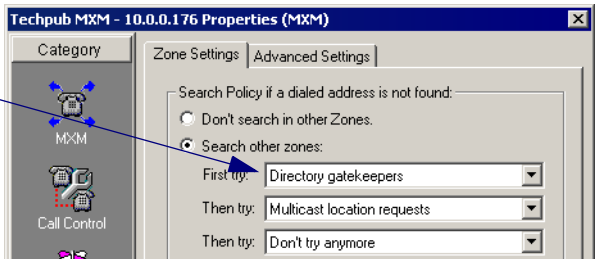
1	End point managed by LA Tech University MXM in Los Angeles dials end point in Japan.
2	LA Tech University MXM does not have the global code (00) listed in its registered nodes. It forwards call to its parent, the Los Angeles regional directory gatekeeper.
3	Los Angeles gatekeeper does not have the global code (00) listed in its database. It forwards call to its parent, the USA country gatekeeper.
4	USA gatekeeper forwards call to its parent, the global gatekeeper (00).
5	The global gatekeeper routes the call to Japan country gatekeeper (81).
6	Japan gatekeeper locates the 45 exchange and routes the call to Tokyo regional gatekeeper.
7	Tokyo gatekeeper locates the 477 exchange's zone controlled by the All Nippon University MXM.
8	All Nippon University MXM completes the call to the 9511 end point.

Setting Up an MXM-Directory Gatekeeper Configuration

To set up your MXM to work with a Directory Gatekeeper, perform the following tasks:

1 To configure the local MXM to send location requests (LRQs) to directory gatekeepers, set the Search policy in the MXM System Zone Settings (for more details, see "Zone Settings" on page 84).

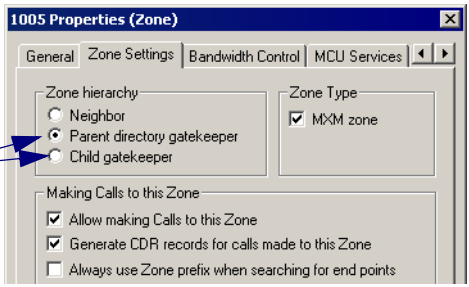
Select **Directory Gatekeeper** as the method of searching for addresses in other zones



Selecting Directory Gatekeeper as the Address Search Method

2 Define any directory gatekeeper listed in the MXM Administrator Main View as a Parent or Child directory gatekeeper in its Zone Settings (for more details, see "Zone Settings" on page 237).

Define the zone as a Parent or Child directory gatekeeper



Defining the Zone as a Directory Gatekeeper

3 Create additional IDs, such as aliases, for the directory gatekeeper (see "Additional IDs" on page 106).

Restricting Bandwidth Allotment

For each neighboring zone, you can restrict the amount of bandwidth that is available for all concurrent videoconferences between that zone and the local MXM. For individual nodes, you can also define a maximum bandwidth allotment.

➤ To set bandwidth allotment for inter-zone calls

1. Double-click the neighboring zone and click the **Bandwidth Control** tab.

   -or-

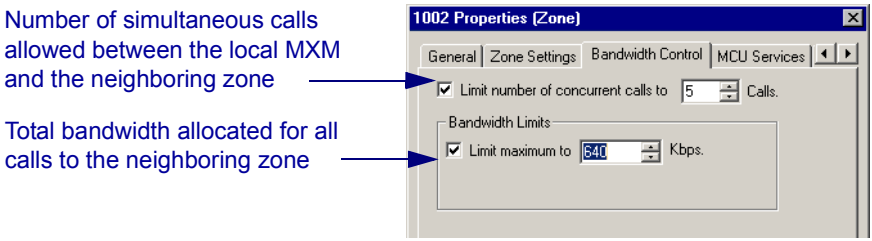
   Right-click the neighboring zone, point to **Property** and then click **Bandwidth Control**.

2. In the Bandwidth Control page, select **Limit Maximum to** to define the total bandwidth that the local MXM allocates for all calls to the neighboring zone. In the list, select the bandwidth in Kbps.

3. Select **Limit Number of Concurrent Calls** to restrict the number of simultaneous calls allowed between the local MXM and the neighboring zone. From the list, choose the number of calls.

4. To implement the changes and close the dialog box, click **OK**.

For example, if you allocated 384 Kbps for all calls and there are four concurrent calls, a possible distribution of the available bandwidth for all calls would be 128, 128, 64 and 64 Kbps.



Setting Bandwidth Allotment for Inter-zone Calls

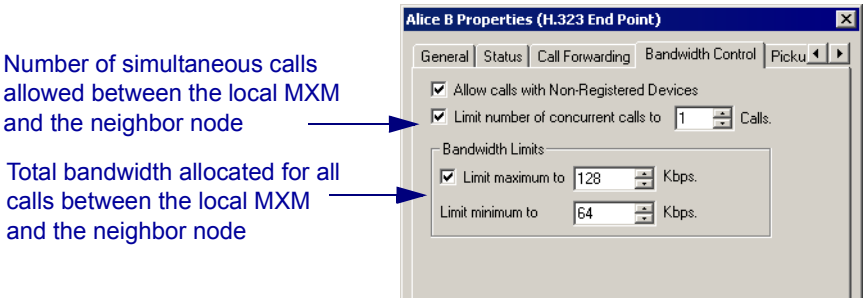
➤ To set bandwidth allotment for calls between the local MXM and a neighbor node

1. Double-click the neighbor node and click the **Bandwidth Control** tab.

   -or-

   Right-click the neighbor node, point to **Property** and then click **Bandwidth Control**.

2. In the Bandwidth Control page, select **Limit Maximum to** to define the total bandwidth that the local MXM allocates for all concurrent calls to the neighbor node. In the list, select the bandwidth in kbps.
3. Select **Limit Number of Concurrent Calls** to restrict the number of simultaneous calls allowed between the local MXM and the neighbor node. From the list, choose the number of calls.
4. To implement the changes and close the dialog box, click **OK**.



Setting Bandwidth Allotment for Inter-zone Calls to a Neighbor Node

Restricting H.450 Exchange Functions

You can allow or forbid H.450 Exchange functions, such as Call Forwarding and Call Transfer, between the local MXM and the neighboring zone or node.

➤ To allow H.450 Exchange functions to the neighboring zone

1. Double-click the neighboring zone and then click the **Product Info** tab.

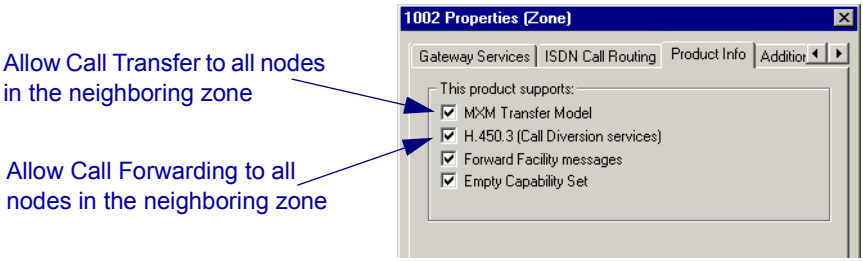
   -or-

   Right-click the neighboring zone, point to **Property** and then click **Product Info**.

2. In the Product Info page, select **MXM Transfer Model** to allow Call Transfer to all nodes in the neighboring zone.

3. Select **H.450.3 (Call Diversion services)** to allow Call Forwarding to all nodes in the neighboring zone.

4. To implement the changes and close the dialog box, click **OK**.



Enabling H.450 Exchange Functions to a Neighboring Zone

➤ To allow H.450 Exchange functions to a neighbor node

1. Double-click the neighbor node and then click the **Product Info** tab.

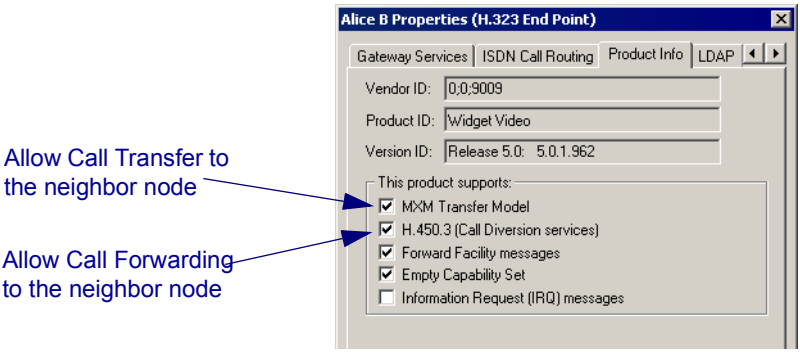
   -or-

   Right-click the neighbor node, point to **Property** and then click **Product Info**.

2. In the Product Info page, select **MXM Transfer Model** to allow Call Transfer to the neighbor node only.

3. Select **H.450.3 (Call Diversion services)** to allow Call Forwarding to to the neighbor node only.

4. To implement the changes and close the dialog box, click **OK**.



Enabling H.450 Exchange Functions to a Neighbor Node

Sharing Gateway and MCU Services with Other Zones

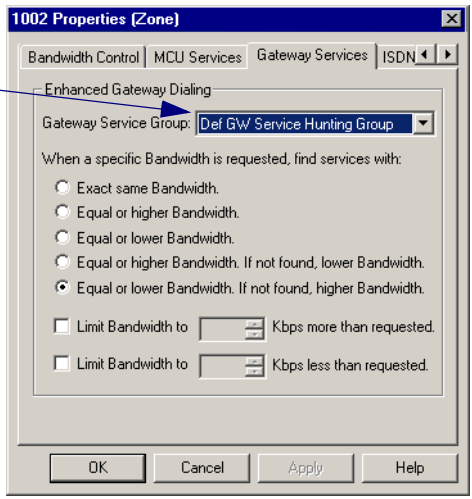
Gateway and MCU services from local and neighbor MXMs may be made available to nodes registered with the involved MXMs.

Direct Gateway Service Dialing

This method may be used for providing neighbor nodes with gateway services that are registered in the local MXM.

➤ To set up direct gateway service dialing

1. Right-click the neighbor zone, point to **Properties**, and then click **Gateway Services**. The **Gateway Services** tab appears.
2. Select a Gateway Service Hunting Group and bandwidth allocation policy (see page 242). To limit the gateway services available to neighbor nodes, you can even create a specific Gateway Service Hunting Group (see "Gateway Service Hunting Groups" on page 141).



3. Click **OK**.

Dialing a Gateway Service

To obtain a gateway service, the neighbor node must dial:

[Zone Prefix][Gateway Access Number][ISDN number of remote party]

For example, **40093334444**, where

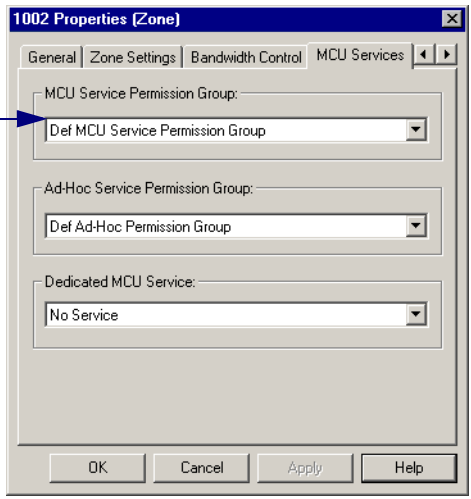
400 is the prefix, *9* is the access number, and *3334444* is the ISDN number.

Direct MCU Service Dialing

This method may be used for providing neighbor nodes with MCU services that are registered in the local MXM. It is easy to set up but requires users to obtain the local MXM's zone prefix and enter it while dialing.

➤ To set up direct MCU service dialing

1. Right-click the neighbor zone, point to **Properties**, and then click **MCU Services**. The **MCU Services** tab appears.
2. Select an MCU Service Permission Group. To limit the MCU services available to neighbor nodes, you can even create a specific Permission Group (see "MCU Service Permission Groups" on page 160).



3. Click **OK**.

Dialing an MCU Service

To obtain an MCU service, the neighbor node must dial:

[Zone Prefix][MCU's directory number]

For example, **4004444**, where

400 is the prefix and *4444* is the MCU's directory number.

Adding Neighbor Gateways and MCUs to other MXMs

This method may be used for providing MXM nodes with gateway and MCU services that are registered in a neighboring zone. Listing gateways, MCUs, and their services under their neighboring zone in the Main View offers the following advantages:

- ❑ Users do not need to obtain and add zone prefixes when they dial.
- ❑ The listed services may be placed in Gateway Service Hunting Groups or MCU Service Permission Groups in the local MXM.

The available operations for setting up this situation are:

- Drag-and-drop
- Copy and paste
- Manually adding a gateway or MCU

➤ To copy a gateway or MCU to a neighboring MXM

1. Log in to the MXM to which you want to make services available (see page 13).
2. Drag the gateway or MCU entry from your local MXM to the local MXM entry under the neighboring MXM's Zones object.

   -or-

   Copy the gateway or MCU entry from your local MXM and paste it on the neighboring MXM's Zones object.

Gateway and its Services Copied to another MXM

Dragging gateways and MCUs to your MXM's corresponding zone in the neighboring MXM makes all their services available to nodes in the neighboring zone. If you do not want all the services available in the neighboring zone, create a Gateway Service Hunting Group, MCU Service Permission Group or delete the unwanted services.

➤ To manually add a neighbor gateway or MCU to the local MXM

1. Right-click the neighboring zone, point to **Add Node to Zone**, and then click **Add Gateway** or **Add MCU**.
2. In the new node's wizard, edit the node's properties according to its configuration and your network specifications (for details, see "Setting Gateway Properties" on page 132 or "Setting MCU Properties" on page 151). Click **OK** to finish.
3. After adding the gateway or MCU, right-click it and then click **Add Service**. The New Service wizard appears.
4. Edit the service's properties according to its configuration and your network specifications (for details, see "Setting Gateway Service Properties" on page 139 or "MCU Services" on page 155). Click **OK** to finish.
5. To add additional services, repeat step 4 as many times as necessary.

The neighbor gateway or MCU and its services are now listed in the local MXM.

The gateway may be dialed by MXM nodes simply by entering the gateway access number and the remote party's ISDN number. The gateway's services are now available for inclusion in Gateway Service Hunting Groups (see "Gateway Service Hunting Groups" on page 141).

Neighbor Gateway and Service

The MCU may be dialed by MXM nodes simply by dialing the MCU's directory number. The MCU's services are now available for inclusion in MCU Service Permission Groups (see "MCU Service Permission Groups" on page 160).

Neighbor MCU and Service

15 Registering with LDAP Directories

15.1 Overview of LDAP

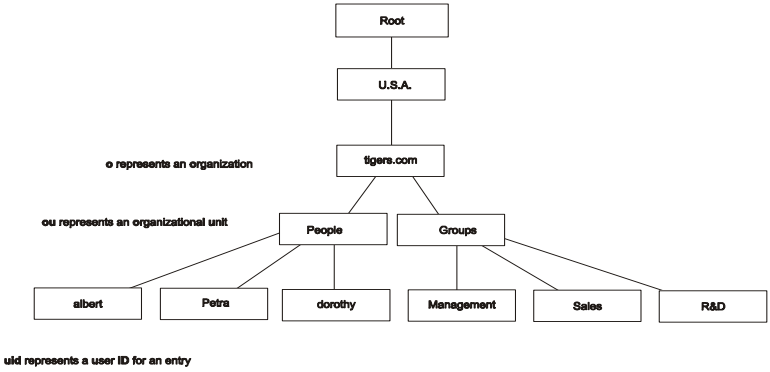
Online directories, such as Microsoft ILS Servers and Novell NDS, are lists of users or network resources which include descriptive and contact information about all entries. They may be used to look up someone's contact information or to retrieve a list of e-mail addresses. They are accessible through an Internet connection. The MXM supports access to online directories.

Using the Lightweight Directory Access Protocol (LDAP), MXM end points may locate any other user or node on a public X.500-based network (X.500 is a standard for directory services in a network). In such a network, directory information is consolidated in central servers located throughout the network. These servers coordinate their directory information so that each maintains an updated, current mail client directory.

An LDAP directory is usually organized in a "tree" hierarchy with levels of objects (similar to the System tree in the Main Administrator window). Each object in the hierarchy must have a unique name. An LDAP directory tree may consist of the following levels:

- The "root" directory (the starting place or the source of the tree)
- Countries
- Organizations (such as a company or government ministry)
- Organizational units (such as divisions and departments)
- Individuals (such as persons, files, and shared resources such as printers).

For example, a sample hierarchy may look like this:



Sample LDAP Directory Hierarchy

An LDAP directory can be distributed among many servers. All of the LDAP servers may contain identical versions of the total directory which are synchronized periodically. An LDAP server that receives a request from a user may pass it to other servers as necessary, but ensures a single coordinated response for the user.

The MXM supports the following directory servers:

- Microsoft Internet Location Server (ILS)
- Microsoft Exchange Server
- Microsoft Window 2000 Active Directory
- Novell Directory Services (NDS)
- Site Server ILS
- Netscape Directory Server.

You may register an MXM's end points and various other nodes in more than one LDAP server directory. There are several reasons why an organization would make such an arrangement. For example, a company may create a list of all employees and another list in which senior managers are removed. The company can provide the first list to its managers, and preserve its managers' online information by providing non-management employees with the latter list.

This chapter provides the configuration settings required for the MXM to register with the respective LDAP directories. For information and instructions for installing and working with these applications, see the specific application's user guides.

15.2 Registering the MXM with an ILS

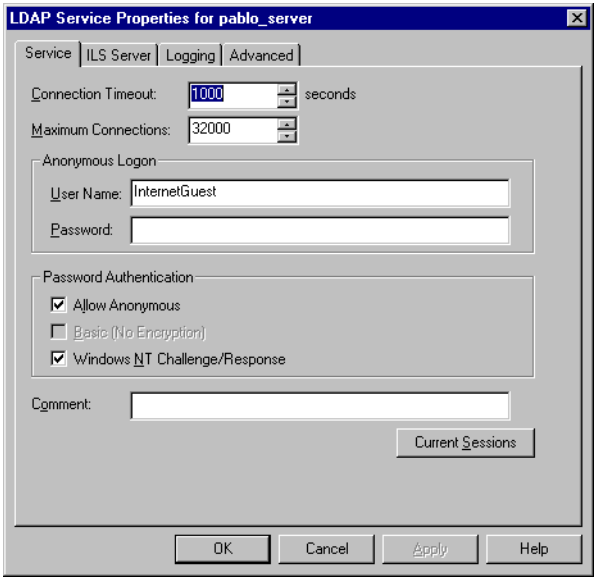
By supporting both Microsoft NetMeeting and Internet Location Server (ILS), the MXM can register with ILS servers, therefore providing its registered nodes with ILS services.

This section provides the required configuration information and values for registering the MXM and its users in the ILS.

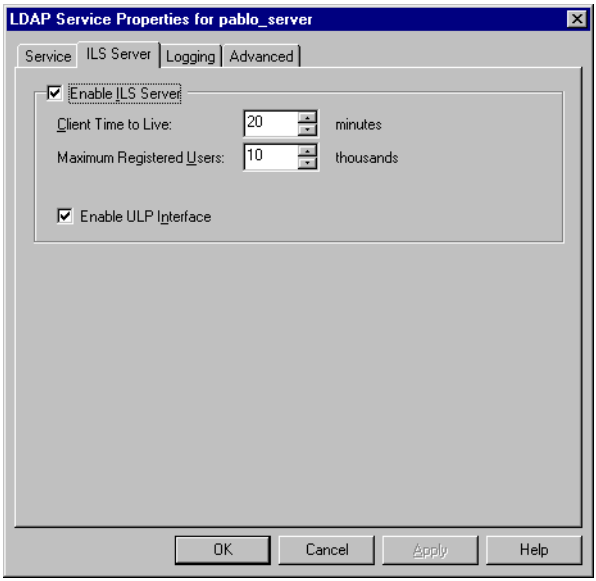
➤ To set up the MXM's configuration in the ILS

1. Run the Microsoft Internet Information Server (IIS) application and open the Microsoft Management Console (MMC).
2. In the **Console** menu, click **Add\Remove Snap-in**. In the Add\Remove Snap-in dialog box, click **Microsoft Information Server** and then click **Add**. Click **OK** to confirm.
3. In the MMC, right-click **LDAP** and click **Properties**. The LDAP Service Properties appears. The following illustrations show suggested settings.

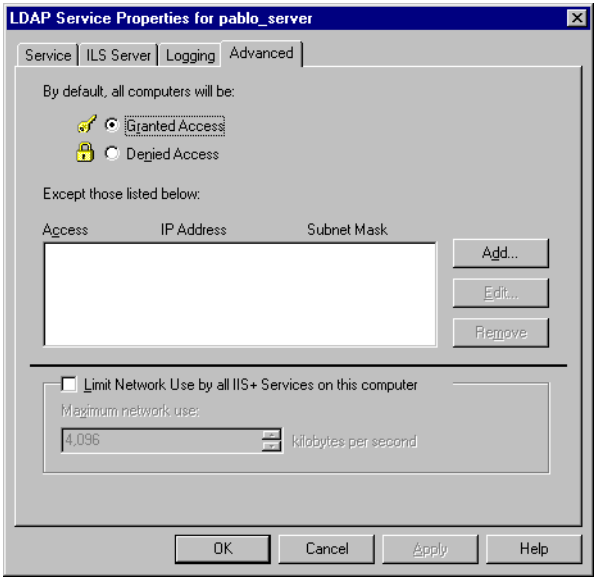
You may enter your own choices as the Anonymous Login User Name and Password (optional).



Recommended LDAP Service Settings



Recommended LDAP ILS Server Settings



Recommended LDAP Advanced Settings

4 To complete the configuration, you must perform the ILS Installation Verification.

In your web browser, enter the location **http://***IP address of local host*/**ils**. Click the **Installation Verification** link.

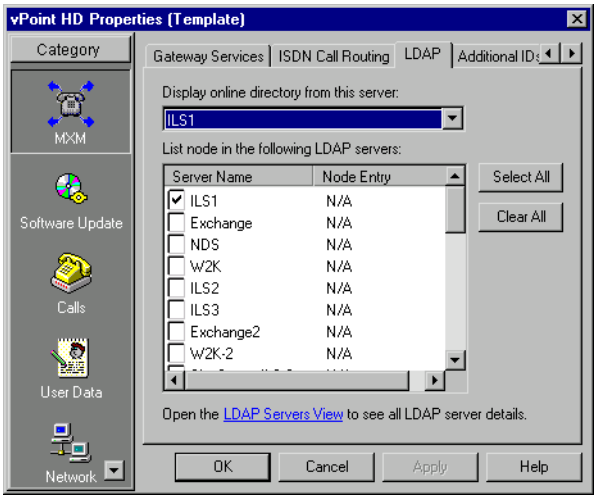
Follow the onscreen instructions to complete the verification process.

Setting Up the ILS Configuration in the MXM Administrator

Finally, you have to set up the ILS configuration for the MXM in the MXM Administrator.

➤ To set up the ILS configuration in the MXM

1 In the Main view, expand the **Templates** group. Right-click the node type to be registered in the LDAP Server, point to **Property**, then **MXM**, and then click **LDAP**. In the **Create an Entry in Server** list, choose **ILS** and then click **Apply**.



Template's LDAP Properties

2 Click **Show LDAP Servers**. The LDAP Servers View appears.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

3 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server).
- Default Directory - Folder as created in the ILS Server, reflecting the assigned organization ("o") and object class. For example, "**o=Microsoft, objectClass=RTPerson**".
- Domain, User, Password - keep these spaces blank.

To edit an entry, click in the relevant cell(s), then delete and type.

15.3 Registering the MXM with Microsoft Exchange Server

For systems using the Microsoft Exchange Server 5.5 for their messaging and collaboration, the MXM is compatible. The Exchange Server sets up directories in the form of a tree-like hierarchy (see the illustration on page 268). For example, your company may be the top of the tree, the next level may be an organization unit such as the MXM, Sales or Administration, and the next level may be individual Recipients, such as individual end points.

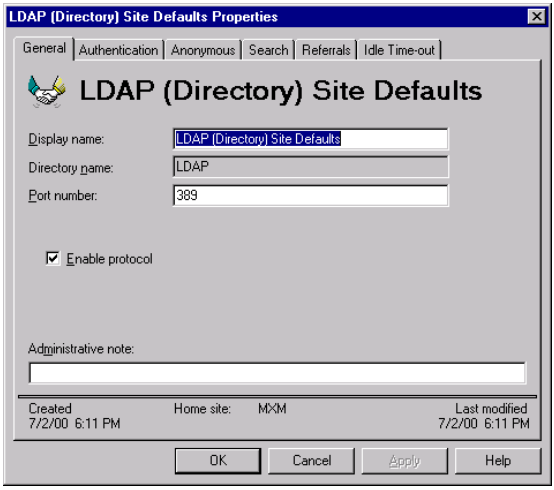
This section provides the required configuration information and values for registering the MXM and its users in a Microsoft Exchange Server.

To be listed, a Recipient must already have an open account in the Microsoft Exchange Server.

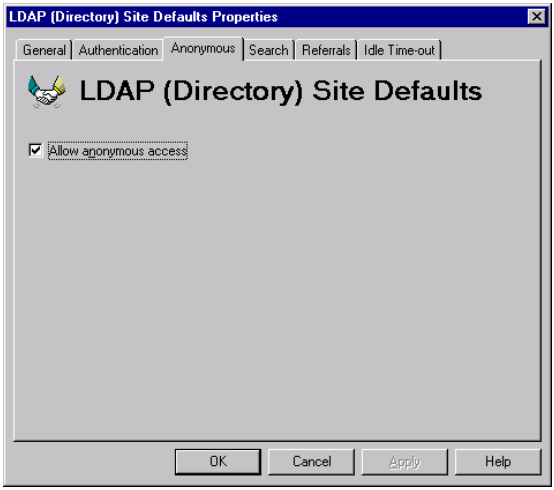
➤ To add MXM users to the Exchange Server

1. Run the Microsoft Exchange Administrator application and connect to a server.
2. In the Administrator tree, click the Organizational Unit (such as MXM) under which the users will be listed.
3. In the **File** menu, point to **New Other** and click **Recipients Container**. The Recipient's Properties dialog box appears.
4. In the **General** tab, enter a **Display Name** for the Recipient and the **Directory Name** under which the Recipient will appear on the tree.

   In the **Permissions** tab, the name of the MXM appears as the source of the Recipient's various conferencing privileges.
5. In the Administrator tree, expand the MXM's Configuration object. Click Protocol to display available protocol entries.
6. Double-click **LDAP (Directory) Site Defaults**. The following illustrations show suggested settings.

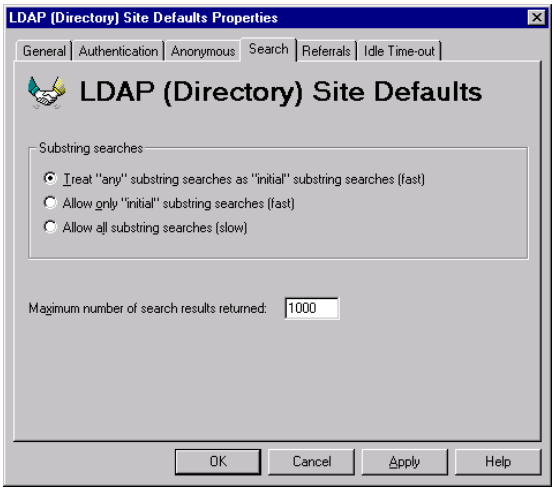


LDAP Site Defaults General Properties



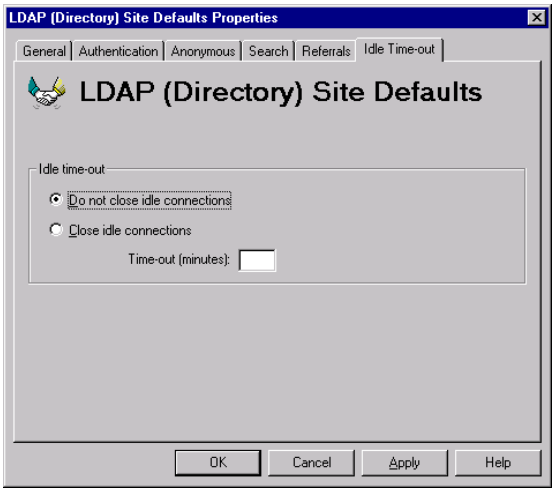
LDAP Site Defaults Anonymous Properties

Set your firewall to permit anonymous access to and from the directory.



LDAP Site Defaults Search Properties

For the **Maximum Number of Search Results**, enter a value equaling (*number of registered users* + 10).



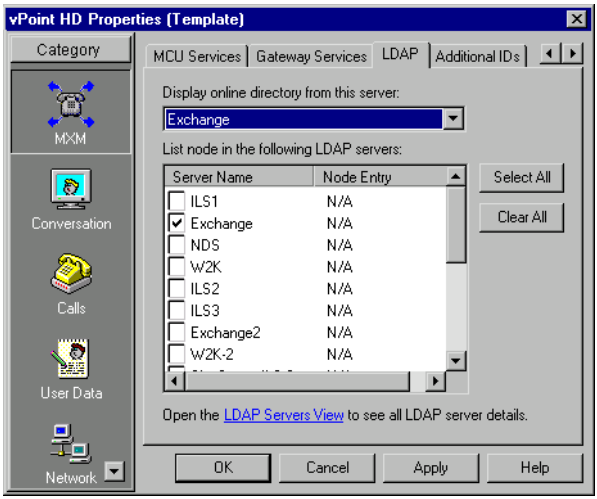
LDAP Site Defaults Idle Timeout Properties

Setting Up the Exchange Server Configuration in the MXM Administrator

Finally, you have to set up the Exchange Server configuration for the MXM in the MXM Administrator.

➤ To set up the Exchange Server configuration in the MXM

1. In the Main view, expand the **Templates** group. Right-click **Desktop** (or other node type to be registered iin the LDAP Server), point to **Property**, then **MXM**, and then click **LDAP**. In the **Create an Entry in Server** list, choose **Exchange** and then click **Apply**.



Template's LDAP Properties

2 Click **Show LDAP Servers**. The LDAP Servers View appears.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

3 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server). The recommended value is **30** (seconds).
- Default Directory - Folder as created in the Exchange Server, reflecting the assigned organization ("o"), organizational unit ("ou") and additional levels in the hierarchy ("cn", or common name). For example, "**cn=recipients, ou=Site_Name, o=Default_Organization_Name**".
- Domain - Domain of the Exchange Server.
- User - Valid user in the Exchange Server domain, with access rights to its MXM default directory
- Password - Password as defined in the Exchange Server.

To edit an entry, click in the relevant cell(s), then delete and type.

15.4 Registering the MXM with Windows 2000 Active Directory

The MXM supports Microsoft Windows 2000 Active Directory, which sets up directories in schemas. The schemas are made up of sublevels called classes. Each class is made up of uniquely named attributes.

In the Active Directory Console, you must expand its schema by creating a new class titled “MXMNode” and then create new attributes for the MXM with specific names.

This section provides the required configuration information, exact attribute names, and values for registering the MXM and its users in an Active Directory Server. To perform the tasks, you must open the Active Directory Console. Then, follow the series of procedures in this section.

Adding an Administrator with Full Configuration Rights

To extend the schema, you have to give full control (read and write permissions) to a user from the Schema Admin group. As a result, this user becomes an Administrator.

Then, add a new Active Directory schema snap-in.

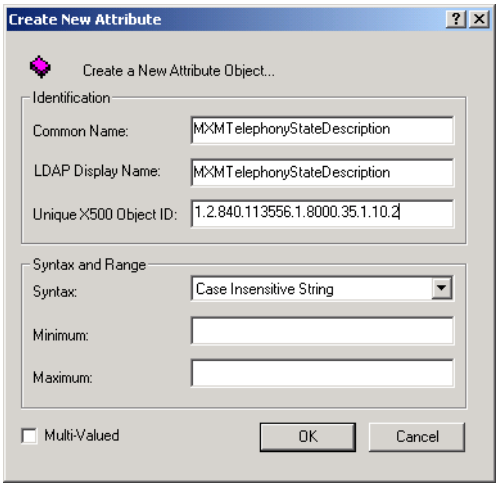
These tasks are basic Active Directory functions. If necessary, refer to the Active Directory documentation for instructions.

Adding the MXM Attributes

You have to add specific attributes, or characteristics, for MXM objects to the snap-in.

➤ To add MXM attributes to the snap-in

1. In the **Active Directory Schema** snap-in on the left side of the Active Directory Console, right-click the **Attributes** folder and then click **Create Attribute**.



Creating New MXM Attributes

2. In the Create New Attribute dialog box, type identical names in the **Common Name** and the **LDAP Display Name** boxes.

   In the **Unique X500 Object ID** box, type the OID of the attribute.

The table following this procedure contains the required attribute names and their respective OIDs. Enter them as they appear in the table.

3. In the **Syntax** list, select **Case Insensitive String**.
4. Click **OK**.

5 Repeat this procedure for all the attributes in the following table.

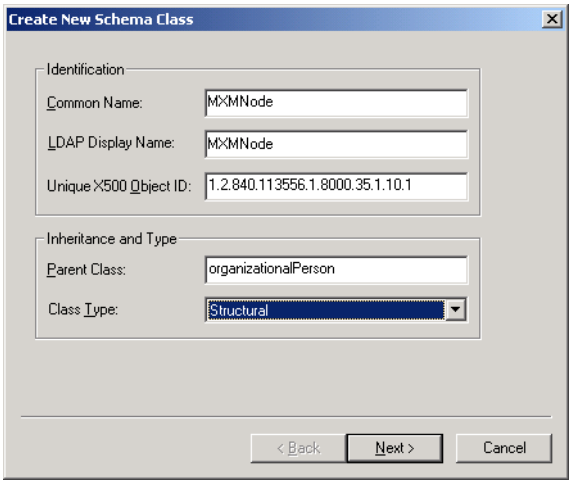
Attribute Name	OID
MXMTelephonyStateDescription	1.2.840.113556.1.8000.35.1.10.2
MXMUserType	1.2.840.113556.1.8000.35.1.10.3
MXMBChannelNum1	1.2.840.113556.1.8000.35.1.10.4
MXMBChannelNum2	1.2.840.113556.1.8000.35.1.10.5
MXMBChannelNum3	1.2.840.113556.1.8000.35.1.10.6
MXMBChannelNum4	1.2.840.113556.1.8000.35.1.10.7
MXMBChannelNum5	1.2.840.113556.1.8000.35.1.10.8
MXMBChannelNum6	1.2.840.113556.1.8000.35.1.10.9
MXMRestricted56k	1.2.840.113556.1.8000.35.1.10.10
MXMVideoSupport	1.2.840.113556.1.8000.35.1.10.11
MXMAudioSupport	1.2.840.113556.1.8000.35.1.10.12
MXMInCall	1.2.840.113556.1.8000.35.1.10.13
MXMH323Alias	1.2.840.113556.1.8000.35.1.10.14
MXMDeskTopUserDataNotes	1.2.840.113556.1.8000.35.1.10.15

Adding the MXMNode Class

You must now create an MXMNode class, to which you will later add the attributes you created in the previous section.

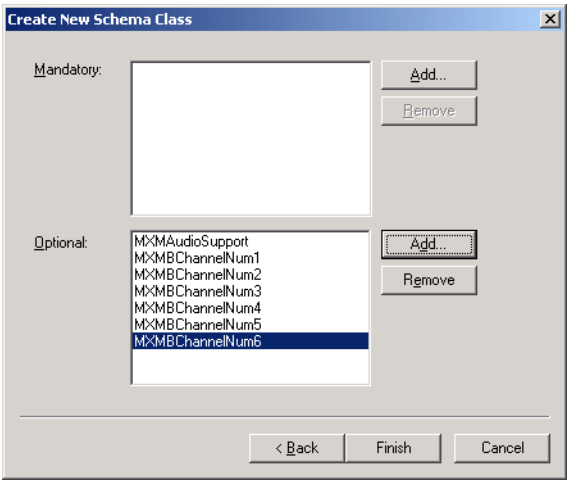
➤ To create the MXMNode class

1. In the **Active Directory Schema** snap-in on the left side of the Active Directory Console, right-click the **Classes** folder and then click **Create Class**.



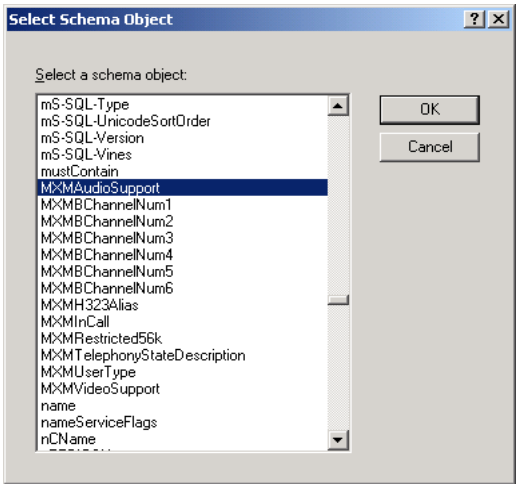
Creating the MXMNode Class

2. In the Create New Schema Class wizard, type **MXMNode** in the **Common Name** and the **LDAP Display Name** boxes.
3. In the **Unique X500 Object ID** box, type **1.2.840.113556.1.8000.35.1.10.1** as the OID of the attribute.
4. In the **Parent Class** box, enter **organizationalPerson**.
5. In the **Class Type** list, select **Structural**.
6. Click **Next**.



Adding MXM Attributes to MXMNode Class

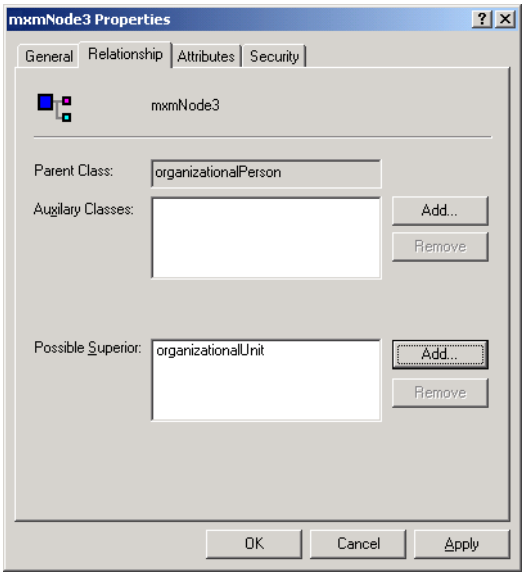
7 Next to the **Optional** list, click **Add**.



Selecting MXM Attributes for the MXMNode Class

8 In the Select Schema Object dialog box, select all the new MXM attributes and click **OK**.

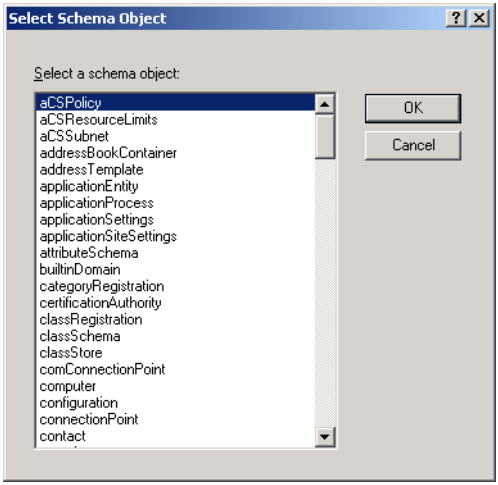
9 Right-click the **MXMNode** Class object on the left side of the Active Directory Console, and then click **Properties**. In the Properties dialog box, click the **Relationship** tab.



MXMNode Class Relationship

10 Opposite the **Possible Superior** box, click **Add**.

11 In the Select Schema Object dialog box, select an Organizational Unit and then click **OK**.



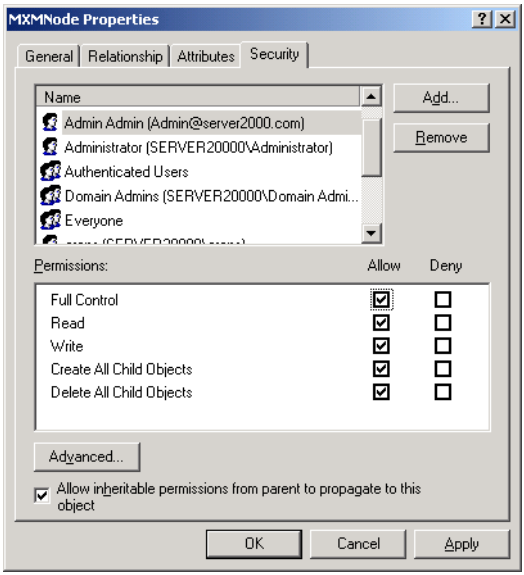
Selecting an Organizational Unit for the MXMNode Class

The MXMNode class is now contained inside the selected Organizational Unit.

Granting Full Control for the MXMNode Class to an Active Directory User

To work with the newly created MXMNode class, create an Active Directory User account with Administrator privileges.

1. Right-click the **MXMNode** Class object on the left side of the Active Directory Console, and then click **Properties**. In the Properties dialog box, click the **Security** tab.
2. In the Names list, select the user and then select **Full Control** in the **Allow** column. Click **OK**.



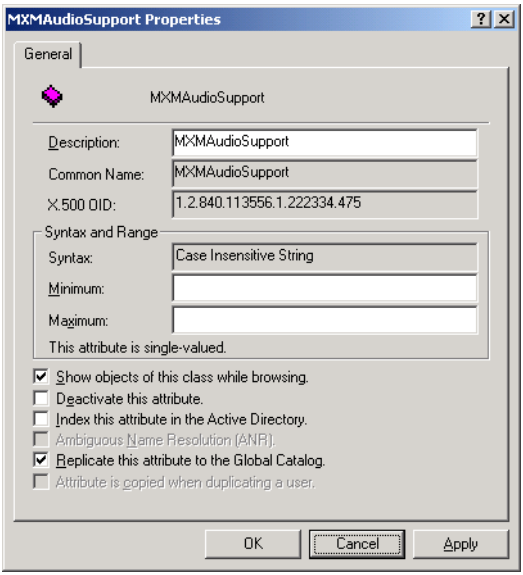
Granting Full Control Privileges to an Active Directory User

Setting the Properties of the MXM Attributes

In this procedure, you must assign specific properties to all the MXM attributes.

➤ To set the properties of the MXM attributes

1. In the **Attributes** folder, right-click an MXM attribute and then click **Properties**.



Setting MXM Attribute Properties

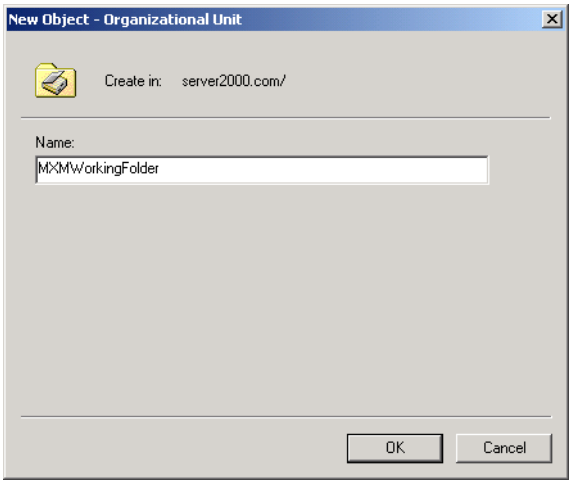
2. In the **Description** box, enter the identical name of the attribute.
3. Select the following options:
   - **Show objects of this class while browsing**
   - **Replicate this attribute to the Global Catalog**
4. Click **OK**.

Creating an Organizational Unit for Your MXM

At this time, create a new Organizational Unit which will be your MXM's working folder in the LDAP server.

➤ To create your MXM's Organizational Unit

1 Expand the **Active Directory Users and Computers** snap-in on the left side of the Active Directory Console. Right-click the **LDAP Server** object, point to **New** and then click **Organizational Unit**.



Creating the MXM Organizational Unit

2 In the **Name** box, type **MXMWorkingFolder**.

3 Click **OK**.

Setting Up the LDAP Configuration in the MXM Administrator

Finally, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connecti on	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table in the W2K row:

- Host address - Exact host name or IP address of the LDAP server.
- Port - **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server). The recommended value is **30** (seconds).
- Default Directory - Path as created in the Active Directory tree, reflecting the assigned organizational unit ("ou") and domain controls. For example, "**ou=MXMWorkingFolder,dc=servername,dc=com**".
- Domain - keep this space blank.
- User - Active Directory User with Administrator rights, as defined in "Granting Full Control for the MXMNode Class to an Active Directory User" on page 285. For example, "**su,cn=users,dc=server_name,dc=com**".
- Password - Password for this user as defined in the Active Directory application.

To edit an entry, click in the relevant cell(s), then delete and type.

15.5 Registering the MXM with Novell Directory Services (NDS)

The MXM is compatible with Novell NDS® scalable LDAP directory services. The NDS sets up directories in schemas and hierarchies.

NDS hierarchies are made up of sublevels called classes. Each class is made up of uniquely named objects.

We recommend that you register your MXM and its registered users either during NDS installation or while the MXM is shut down. You must expand its schema by creating a new class titled “MXMNode” and then create new attributes for the MXM with specific names.

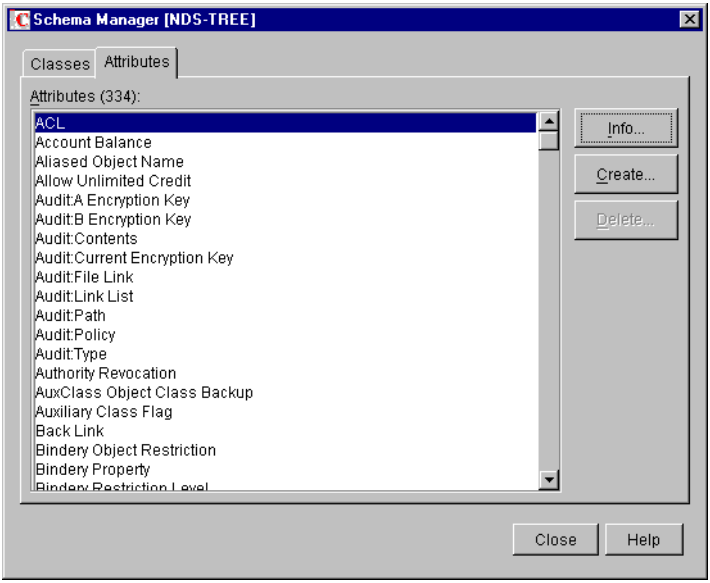
This section provides the required configuration information, exact attribute names, and values for registering the MXM and its users in an NDS LDAP Server. Follow the series of procedures.

Creating MXM Attributes

First, you have to add specific attributes, or characteristics, for MXM objects.

➤ To create MXM attributes

1. Run the NDS management application.
2. In the **Object** menu, click **Schema Manager**.
3. In the Schema Manager, click **Attributes**.



Schema Manager

4. To make a new attribute, click **Create**. The Create Attribute wizard appears.
5. In the **Attribute Name** box, type the exact name of the attribute and click **Next**.

Entering Attribute Name

6 In the **Syntax** List, select a value that describes the way that item may be written or requested in the directory service. For working with the MXM, select **Case Ignore String** and click **Next**.

Selecting a Syntax

7 As flags, select **Single valued** and **Public read**. Click **Next**.

Selecting Flags

8 Click **Next** until the last page of the wizard, keeping the default values for the new attribute. In the last page, click **Finish**.

9 Repeat steps 3 - 8, setting identical properties as specified, for the following attribute names.

MXMIPAddress	**MXMBChannelNum2**	**MXMRestricted56k**
MXMTelephonyStateDescription	**MXMBChannelNum3**	**MXMVideoSupport**
MXMUserType	**MXMBChannelNum4**	**MXMAudioSupport**
MXMNotes	**MXMBChannelNum5**	**MXMInCall**
MXMBChannelNum1	**MXMBChannelNum6**	

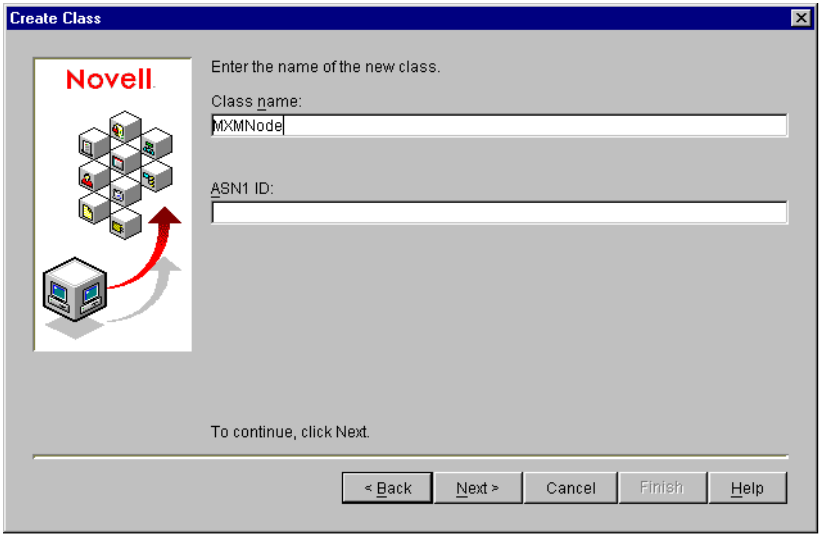
Creating the MXMNode Class

You must now create an MXMNode class based on the default super class named User. Attribute flags and rules will be inherited from the super class.

CAUTION Do not make changes to the NDS default schemas. Otherwise, the LDAP functions of the MXM may be affected.

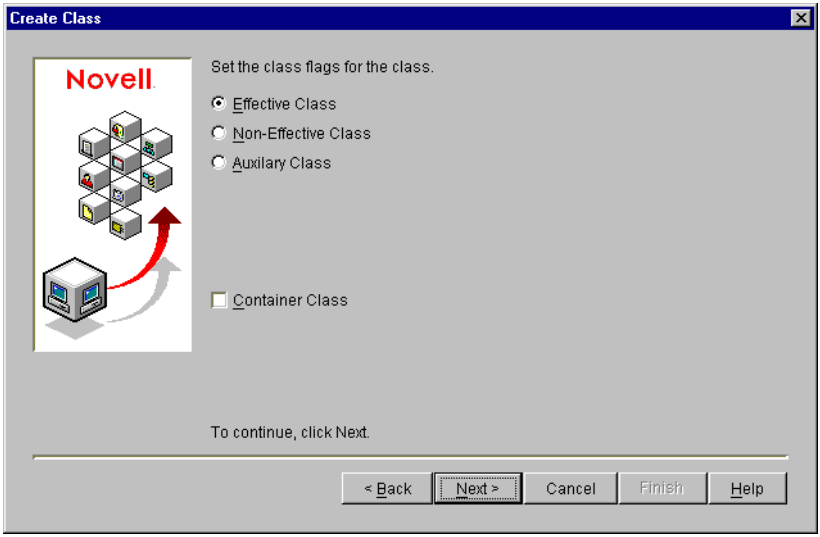
➤ To create the MXMNode class

1. In the **Object** menu, click **Schema Manager**. Click **Create** to open the Create Class wizard.
2. In the **Class Name** box, type **MXMNode** as the exact name of the class and click **Next**.



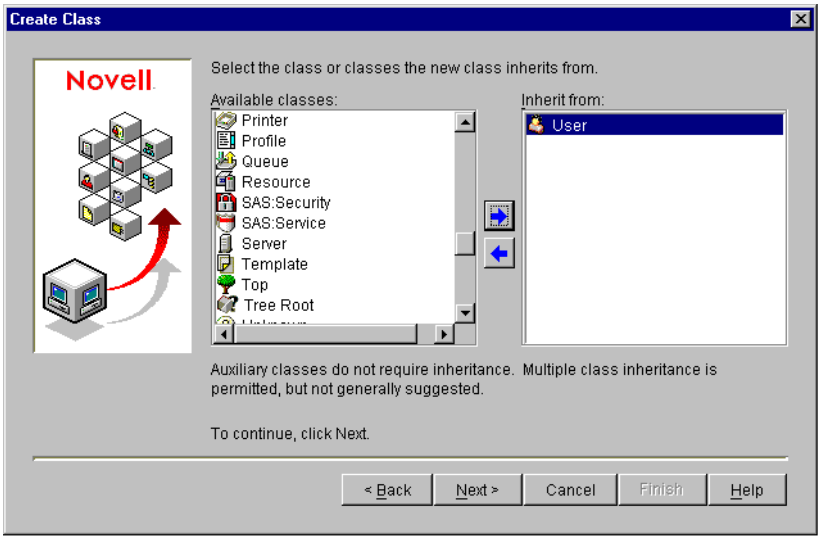
Entering Class Name

3. As the Class flag, select **Effective Class** (for creating instances from this class) and then click **Next**.



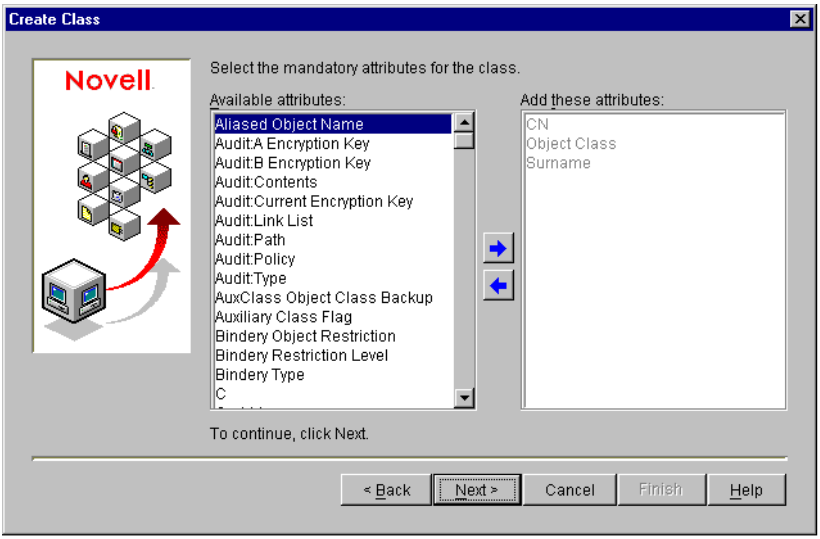
Selecting Class Flag

4 From the **Available Classes** list, choose **User** as the existing class from which the new class will inherit attributes. Click **Next**.



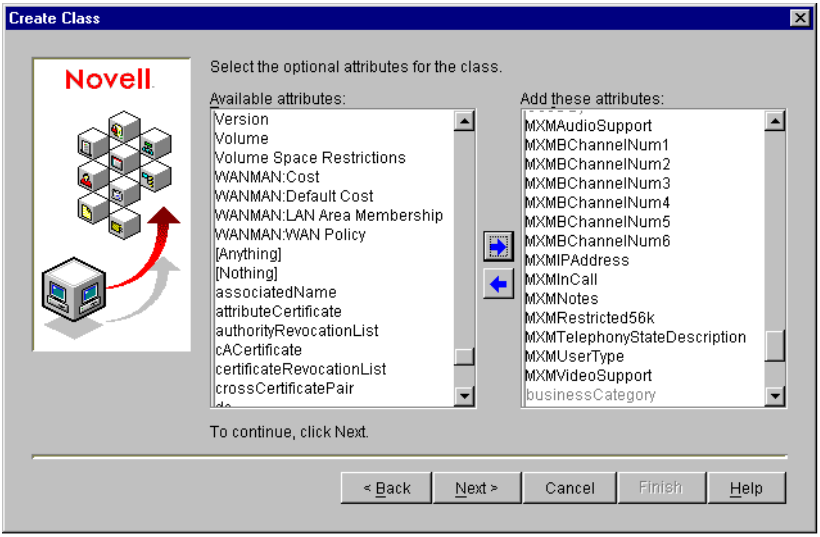
Inheriting Attributes from Existing Classes

5 In the **Available Attributes** list, do not add mandatory attribute(s) for the new class. By default, the class already includes the attributes **CN**, **Object Class** and **Surname**. Click **Next**.



Selecting Mandatory Attributes

6 Choose optional attribute(s) for the new class. From the **Available Attributes** list, choose all the attributes that you created earlier in this procedure (named **MXM**...). Click **Next**.



Selecting the Optional Attributes

7 For the naming attributes, click **Next** without adding more attributes. For the Container Classes, click **Finish** without adding more classes.

8 Restart the server and then run the NDS management application again.

Creating an MXM Container

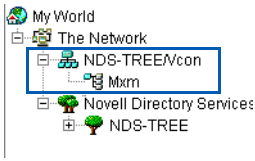
A separate container on the NDS Services tree keeps the MXMNode objects apart from the other NDS objects.

➤ To create a separate MXM container

1 Select the organization or organizational unit to which you want to place the MXMNode class and its objects.

2 Right-click, point to **New** and then click **Organizational Unit**.

3 Type **MXM** as the Organization Unit's name and click **OK**.



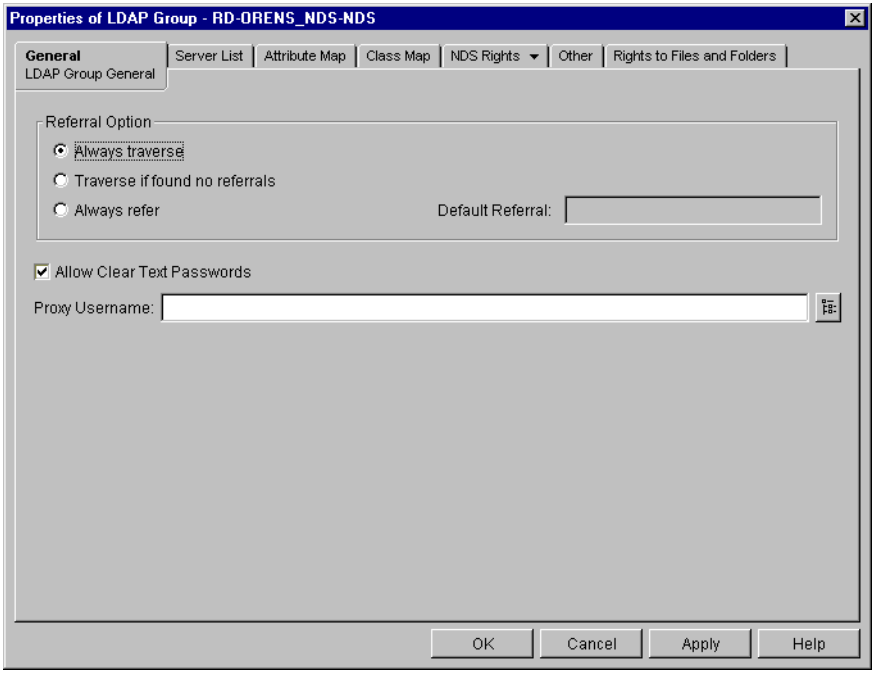
New MXM Container on Tree

Setting Up the LDAP Group Object Configuration

The LDAP Group contains the class and attribute mappings and security policies for one or more LDAP servers. If you plan to use the same configuration on more than one LDAP server, it's easier to set up one LDAP Group object and assign it to each LDAP server in the LDAP Group Server List Properties.

➤ To set up the LDAP Group Object configuration

1. In the container that holds the NetWare Server object, double-click **LDAP Group**.
2. In the LDAP Properties **General** tab, select **Allow Clear Text Passwords**. This option enables the exchange of passwords over nonencrypted connections, and is required for the MXM's normal operation with the NDS Service.

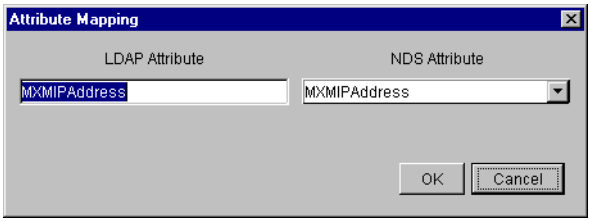


LDAP Group General Properties Setting for MXM

3. Click the **Attribute Map** tab, where you will map the NDS schema names of the new MXM attributes (created in the section, "Creating MXM Attributes" on page 290) to corresponding LDAP names.

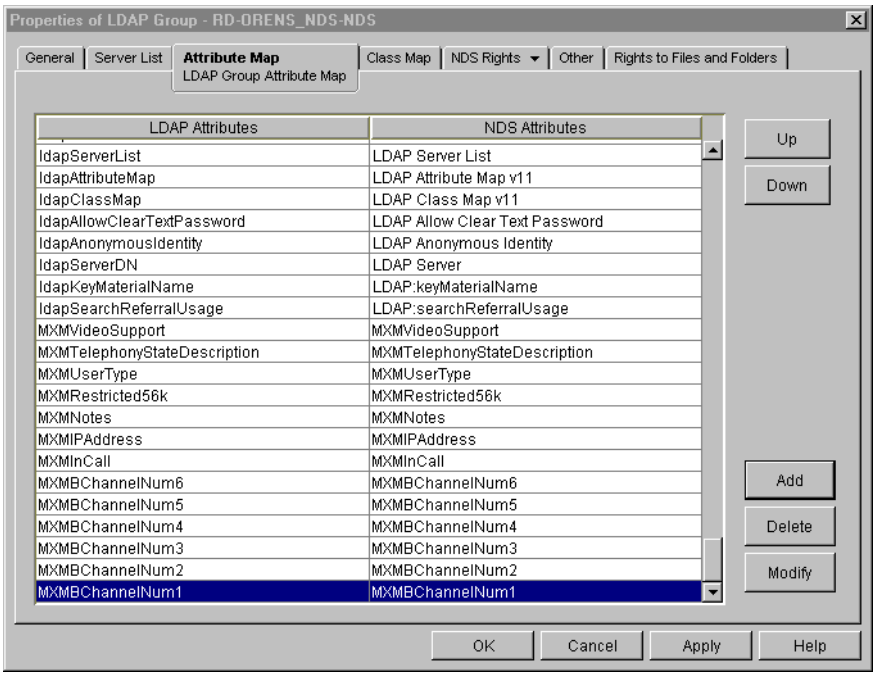
4 Click **Add**. In the Attribute Mapping dialog box, choose a new MXM attribute from the **NDS Attribute** list. Enter that same name into the **LDAP Attribute** box and click **OK**.

Repeat this step for all new MXM attributes.



Mapping the MXM Attributes to LDAP Attributes

The new MXM attributes are now part of the LDAP Group configuration.



Mapped MXM Attributes

5 Click **OK** and restart the server and then run the NDS management application again.

Adding a Trustee for the MXMNode Container

To use the MXMNode container, you have to set up a user with rights for creating and updating objects in the container. Other than the administrator with Super User privileges, who has full rights on the whole NDS Service tree, it is recommended to designate an MXM user as a Trustee, who has rights for creating and deleting objects in the MXMNode container.

➤ To add a trustee for the MXMNode container

1. Right-click the MXMNode organizational unit, point to **Trustees of this object** and then click **Add Trustees**.
2. Browse the NDS tree to find the MXM user that will be the trustee and click **OK**.
3. For this user's Entry Rights and Attribute Rights, select **Create** and **Delete** (if you want, you can select additional rights).
4. Click **OK**.

Setting Up the LDAP Configuration in the MXM Administrator

Finally, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server). The recommended value is **30** (seconds).
- Default Directory - Path as created in NDS Tree, reflecting the assigned organization ("o") and organizational unit ("ou"). For example, "**ou=MXM, o=vcon**".
- Domain - keep this space blank.
- User - Valid user in the Exchange Server domain, with access rights to its MXM default directory. For example, "**su, ou=MXM, o=vcon**."
- Password - Password as defined in the NDS.

To edit an entry, click in the relevant cell(s), then delete and type.

15.6 Registering the MXM with Site Server ILS on Windows 2000

Site Server ILS on Windows 2000 is a service used for publishing H.323 videoconferencing and telephony users and IP multicast conferences on the network. Site Server ILS may be installed during Microsoft Windows 2000 Server setup.

When registering the MXM with Site Server ILS and subsequent listing of users, Site Server ILS' default configuration is suitable.

Setting Up the LDAP Configuration in the MXM Administrator

After registering with Site Server ILS, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - **1002**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server). The recommended value is **30** (seconds).
- Default Directory - Path as created in the Site Server directory tree, reflecting the assigned object class. For example, "**objectClass=RTPerson**".
- Domain, User, Password - keep these spaces blank.

To edit an entry, click in the relevant cell(s), then delete and type.

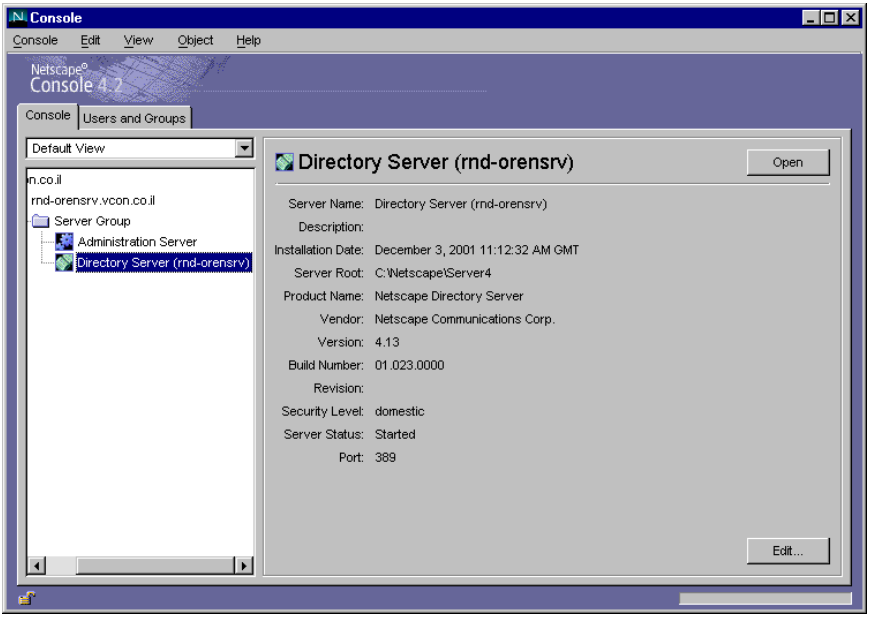
15.7 Registering the MXM with Netscape Directory Server

Netscape Directory Server provides an embeddable, extensible directory for users of a company's extranet or e-commerce site.

This section provides the required configuration information, exact attribute names, and values for registering the MXM and its users in a Netscape Directory Server. Follow the procedure below (for more details about setting up Organizational Units, see the Netscape Directory Server user documentation).

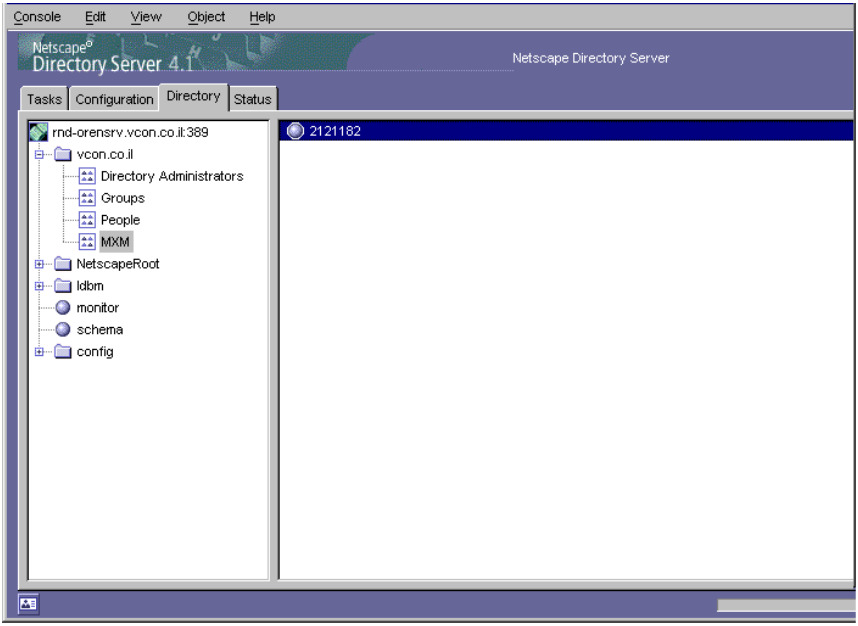
➤ To set up the MXM's configuration in the Netscape Directory Server

1 Run the Netscape Console.



Netscape Console

2 From the folder tree in the left pane of the console, open the Directory Server.



Netscape Directory Server

3 In the Directory Server, expand the tree.

4 Create a new Organizational Unit (for example, companyname.co.il).

5 Set access permissions for one user that has full read-write privileges for the LDAP configuration.

6 Add the organization's users under the Organizational Unit. Create relevant branches in accordance to your organization's departmental structure or other organizational criteria.

Setting Up the LDAP Configuration in the MXM Administrator

After registering with the Netscape Directory Server, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server). The recommended value is **30** (seconds).
- Default Directory - Path as created in Network Directory Server, reflecting the assigned organization ("o") and organizational unit ("ou"). For example, "**ou=MXM, o=yourcompany.com**".
- Domain, User, Password - keep these spaces blank.

To edit an entry, click in the relevant cell(s), then delete and type.

15.8 Registering the MXM with Sun ONE Directory Server

Sun ONE Directory Server (also known as iPlanet) is a scalable distributed directory server for running an enterprise-wide directory containing lists of people and resources. Administrators can manage a single user-repository for their organization that can be used by multiple applications to both authenticate and retrieve stored information for users such as access levels and user profiles.

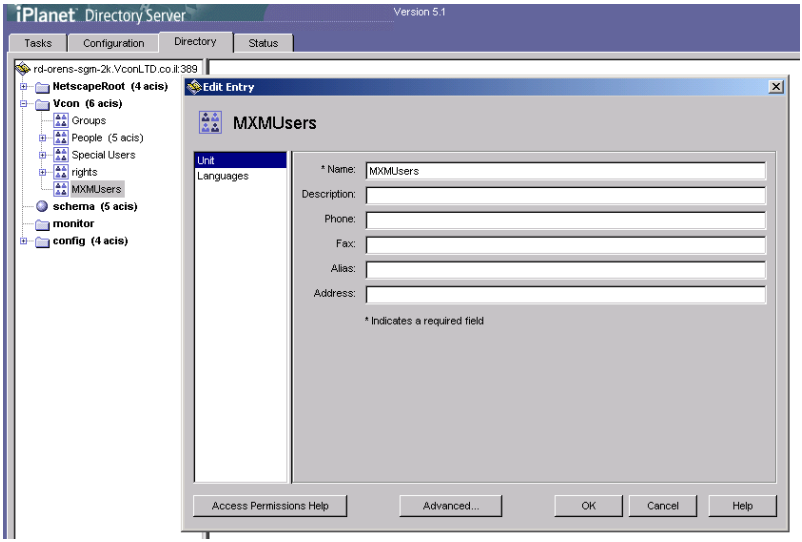
This section provides the required configuration information and values for registering the MXM and its users in a Sun ONE Directory Server. Follow the procedure below.

Generating a Database of MXM Users in the Directory Server

The MXM uses Sun ONE's default schema (*RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3*) user presentation to create end point entries for MXM users on the Sun ONE directory server. It is not required to extend the schema. MXM end points are created using the *inetorgperson* object class.

➤ To generate a user database in the Sun ONE Directory Server

1. In the Sun ONE manager console, open an organizational container for the MXM entries.



Opening a New Organizational Container

In the previous example, an Organizational Unit Container named MXMUsers was added under VCON (**dc=vcon,dc=com**).

2 To work with the newly created container, assign Full Edit rights for the container to any Sun ONE User.

It is recommended to create a special user for binding the MXM into the Sun ONE Directory Server. This user's information is required for your MXM's registered end points to access the Sun ONE server.

Setting Up the LDAP Configuration in the MXM Administrator

After registering with the Sun ONE Directory Server, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table (Sun ONE's entry may appear as iPlanet):

- Host address - Exact host name or IP address of the LDAP server.
- Port - usually **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server).

- Default Directory - the *entrydn* attribute of the Organizational Unit Container created in the Directory Server, reflecting the organizational unit ("ou") and domain name ("dc"). For example, "**ou=mxmusers,dc=vcon,dc=com**".
- Domain - keep this space blank.
- User - the *entrydn* attribute of the MXM User with Full Edit rights, as defined in the Directory Server.
- Password - Password of the MXM User with Full Edit rights, as defined in the Directory Server.

To edit an entry, click in the relevant cell(s), then delete and type.

15.9 Registering the MXM with OpenLDAP Directory Server

OpenLDAP® is an open source implementation of LDAP. If your organization does not currently employ an LDAP server, we recommend installing the OpenLDAP stand-alone LDAP server (*slapd*) from the MXM Setup CD-ROM. For documentation about the OpenLDAP server, see http://www.openldap.org.

The MXM uses OpenLDAP's default schema (*RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3*) user presentation to create end point entries for MXM users on an OpenLDAP directory server. It is not required to extend the schema.

Setting Up the LDAP Configuration in the MXM Administrator

After registering with the OpenLDAP Directory Server, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - usually **389**

- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server).
- Default Directory - Path as created in the OpenLDAP Directory Server, reflecting the organizational unit ("ou") and domain name ("dc"). For example, "**ou=mxmusers,dc=vcon,dc=com**".
- Domain - keep this space blank.
- User - the name of the Manager (the MXM Administrator), as defined in the Directory Server.

The OpenLDAP installation program predefines a Super User with full edit rights named **Manager**. You do not need to change this parameter unless you want this user to be someone else.

- Password - Password of the Manager, as defined in the OpenLDAP installation. This password is **secret**.

To edit an entry, click in the relevant cell(s), then delete and type.

15.10Registering the MXM with ADAM Server

Microsoft's Active Directory® Application Mode (ADAM) is a Lightweight Directory Access Protocol (LDAP) directory service that runs on Microsoft Windows Server™ 2003

ADAM runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service means that multiple instances of ADAM can run concurrently on a single server, and each instance can be configured independently.

The MXM uses the X.500(96) User schema (*RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3*) to create end point entries for MXM users on the ADAM server. Extending the schema is required because ADAM does not include RFC 2256 in its default schema. *LDIF* (Lightweight Directory Interchange Format) files for RFC 2256 provide definitions for the user classes which are imported during the setup of the ADAM Server.

➤ To import the user classes supplied with ADAM

1. Open an ADAM tools command prompt. In the Windows Desktop, click **Start**, point to **All Programs** and **ADAM**, and then click **ADAM Tools Command Prompt**.
2. At the command prompt, type:

   ldifde -i -f *filename* **-s** *computername:port* **[-b** *username domain password***] -k -j . -c "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext**

filename	Represents the name of one of the *.ldf* files that is supplied with ADAM.
	It is recommended to import *ms-User.ldf* and *ms-InetOrgPerson.ldf*.
computername :port	Represents the computer name and port number of an ADAM instance.
username domain password	Represents the account with which to run the command.

The following table contains the parameters in step 2 and other commonly used *ldifde* parameters. For more information about *ldifde* parameters, type **ldifde /?** at a command prompt.

-i	Perform an import.
-f	File to import or export.
-s	Host name and port of the ADAM instance.
-b	Security credentials to use during the operation.
-k	Continue the operation in the event of errors.
-j	Create a log file in the specified directory. In this case, the current (".") directory.
-c "CN=Schema,CN=Configuration,DC=X" #schemaNamingContext	Do not modify this string. The -c parameter replaces a specified string in the .ldf file with a different string during import. The distinguished name that is specified in the .ldf file (for example, CN=Schema,CN=Configuration,DC=X) is replaced with the distinguished name of the schema directory partition for your particular ADAM instance, as passed by the #schemaNamingContext constant.

ADAM includes three .ldf files containing user classes that you can import. These files are *ms-User.ldf*, *ms-InetOrgPerson.ldf*, and *ms-UserProxy.ldf*, and they are located in the *%windir%\adam* directory.

As an alternative to using *ldifde*, you can import the optional ADAM user classes during ADAM setup. For more information, see the ADAM Server online help.

If you do not specify user credentials using the **-b** parameter, *ldifde* uses the credentials of the currently logged-on user.

Generating a Database of MXM Users in the Directory Server

MXM users are created using the *inetorgperson* object class.

➤ To generate a user database in the ADAM Server

1. In the ADAM Server management console, open an organizational container for the MXM entries.
2. To work with the newly created container, assign Full Edit rights for the container to any ADAM User.

Setting Up the LDAP Configuration in the MXM Administrator

After registering with the ADAM Server, you have to set up the LDAP Server configuration for the MXM in the MXM Administrator.

➤ To set up the LDAP Configuration of the MXM

1 In the MXM Administrator, click the **LDAP Servers View** button.

Server Type	Server Name	Host Address	Host Port	Refresh Connection	Default Directory	Domain	User	Password
ILS	ILS1	Default_ILS_Server	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange	Default_Exchange_Serv	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
NDS	NDS	Default_NDS_Server	389	0	ou=MXM,o=Vcon		Default_User	********
Win2000	W2K	Default_W2K_Server	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
ILS	ILS2	Default_ILS2	389	0	o=Microsoft,objectClass=RTPerso			
ILS	ILS3	Default_ILS3	389	0	o=Microsoft,objectClass=RTPerso			
Exchange	Exchange2	Default_ExchangeServe	389	0	cn=MXM,cn=recipients,ou=Default	Default_Domain	Default_User	********
Win2000	W2K-2	Default_W2K_Server_2	389	0	ou=Organization_Unit,dc=Default_		Default_User,	********
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	Iplanet5 Server	Default_IPLANET_SERV	389	0	ou=default_organization,dc=Defau			
Netscape	Netscape 4	Default_NETSCAPE_SER	389	0	ou=default_organization,o=compa			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
Site Server	Site Server ILS Se	Default_Site_Server_ILS	1002	0	objectClass=RTPerson			
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	OpenLdap Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
Web Server	DCTS Server	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=vcon,dc=com		Manager,dc=	********
IPlanet	ADAM Server1	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server2	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********
IPlanet	ADAM Server3	Default_OPEN_LDAP_SE	389	0	ou=vcon,dc=my-domain,dc=com		Manager,dc=	********

LDAP Servers View

2 Make sure that the following information appears in the table:

- Host address - Exact host name or IP address of the LDAP server.
- Port - usually **389**
- Refresh Connection Interval - number of seconds. This value must be greater than **0** ("**0**" indicates that there is no connection with the LDAP server).
- Default Directory - the *entrydn* attribute of the Organizational Unit Container created in the Directory Server, reflecting the organizational unit ("ou") and domain name ("dc"). For example, "**ou=mxmusers,dc=vcon,dc=com**".
- Domain - keep this space blank.
- User - the *entrydn* attribute of the MXM User with Full Edit rights, as defined in the ADAM Server.
- Password - Password of the MXM User with Full Edit rights, as defined in the ADAM Server.

To edit an entry, click in the relevant cell(s), then delete and type.

16 MANAGING SIP NETWORKS

The Session Initiation Protocol (SIP) is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. The MXM supports management of SIP end points (called *User Agents*) within its network, in a similar manner as for H.323 end points.

By employing proxy interfaces (H.323 Gatekeeper for H.323 end points, SIP Proxy for SIP user agents), the MXM provides similar services to systems of either protocol. Administrators can initiate calls between two SIP user agents and between a SIP user agent and an H.323 end point. The MXM provides gateway-like services when connecting calls between H.323 and SIP networks.

The MXM's SIP system server combines the roles of an SIP Proxy, SIP Redirect Server, and SIP Registrar.

16.1 SIP User Agents

SIP user agents are end points, such as SIP phones and Windows XP Messenger applications, that initiate and receive communication and collaboration over a SIP network. They can initiate requests (UAC client) and respond to requests (UAS server). User agents communicate with other user agents directly or through a server.

For communication between two SIP user agents using Windows XP Messenger , the MXM supports the following:

- Video conversation
- Voice conversation
- Instant messaging
- Sending file or photo
- Asking for remote assistance
- Whiteboard
- Application sharing

For communication between a SIP user agent using Windows XP Messenger and an H.323 end point or other SIP user agent, the MXM supports the following:

- Video conversation
- Voice conversation

SIP user agents logged into the MXM may also use the supported telephony functions by entering the appropriate TUI number before the destination address (see "Dial Plan" on page 67):

- Call Pickup and Specific Pickup
- Call Forwarding
- Simplified Gateway Dialing

Additionally, a SIP user agent may also be the recipient of a call transfer or ad-hoc conference although it cannot initiate these functions.

16.2 SIP Servers

The MXM fulfills a multi-faceted role in managing SIP user agents. Its SIP server functions interchangably as an SIP Proxy, SIP Redirect Server, and SIP Registrar. This section discusses each role.

SIP Proxy

The SIP Proxy relays requests from user agents to other servers or user agents within the network. The SIP Proxy also "forks" requests to several destinations sequentially or in parallel.

It also retains information for billing/accounting purposes.

The SIP Proxy is represented in the MXM Administrator under the System Servers branch of the Main View. Its Properties configuration indicates the same types of information as the local MXM gatekeeper, except that it does not have a zone prefix assigned to it.

SIP Proxy's Location in the Main View

SIP Redirect Server

A SIP Redirect Server responds to SIP client requests and either informs them of the requested server's address or forwards the calls. The forwarding requests can travel in several hops until they reach the final destination.

To determine user or routing policies, a SIP Redirect server contacts a location server (in the MXM), thereby providing users with more than one method to locate users.

SIP Registrar

A SIP Registrar receives login requests from SIP user agents and stores this information in a location service. The MXM handles the login requests according to its Security policy, such as Open/Closed mode, and License limits (see "Security Properties" on page 79). After the login information is stored, the Registrar sends the appropriate response back to the user agents.

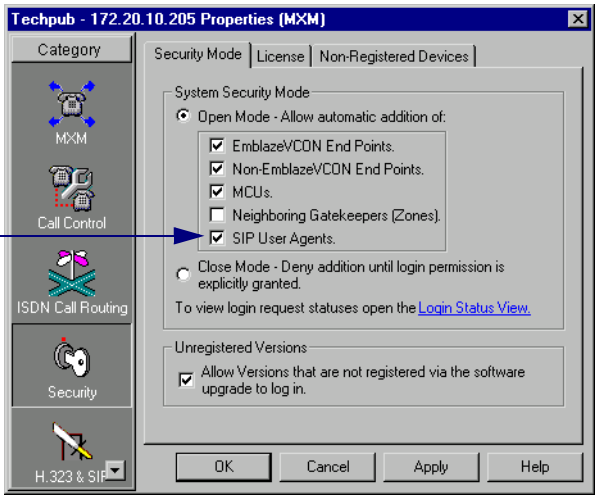
When the SIP Redirect server has to route a SIP request to a user it queries the location service for the destination's current location. Using the data received from the location service, the SIP Redirect server then routes the SIP request (or provides routing information) to the destination.

16.3 Logging in New SIP User Agents

If the MXM is in Open Mode for SIP user agents, any user agent that attempts to register is automatically logged in (see "Security Mode" on page 79).

If the system is in Closed Mode, a SIP user agent must be granted login permission by an administrator with Super User privileges. During this process, the administrator must define or confirm the user agent's MXM properties, as for H.323 end points (see "Granting Login Permission" on page 28).

Select to automatically log in SIP user agents.



Setting Open Mode for SIP User Agents

16.4 Setting the MXM SIP Advanced Settings

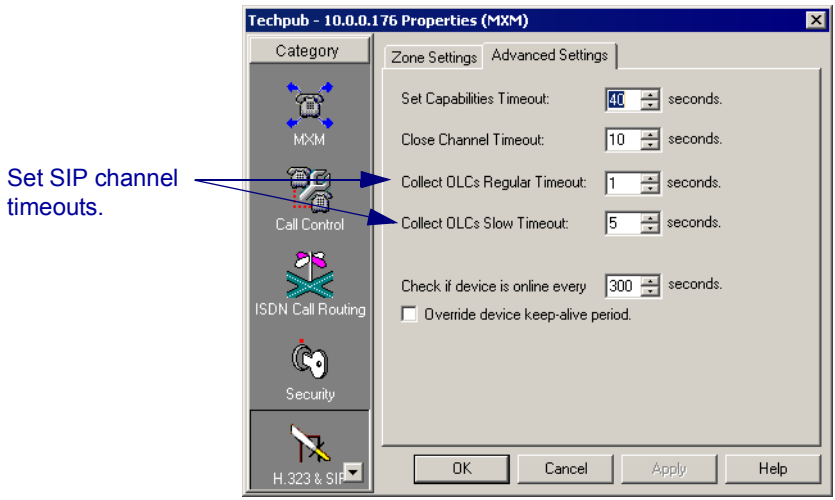
If a SIP user agent and an H.323 end point are engaged in a conversation, the multimedia information sent by the H.323 end point takes longer to reach the SIP user agent than the transmission in the opposite direction. To enable the MXM to synchronize their conversation, the MXM collects all information sent by the H.323 end point and routes it to the SIP user agent before the user agent transmits again. The period of collecting transmitted data is called the OLC timeout.

➤ To set the SIP channels' timeout

1. In the Administrator window, right-click the MXM node at the top, point to **Property** and **H.323 _SIP**, and then click **Advanced Settings**.
2. If necessary, change the following properties or keep the default values:

Collect OLCs Regular Timeout — The maximum period that the MXM collects information transmitted by H.323 devices (except gateways) in order to synchronize a SIP-H.323 conversation.

Collect OLCs Slow Timeout — The maximum period that the MXM collects information transmitted by H.323 gateways in order to synchronize a SIP-H.323 conversation.



Setting Advanced SIP Settings

16.5 Registering a Windows XP Messenger SIP User Agent to the MXM

To register with the local MXM, a Windows Messenger (in Windows XP) user must perform the following procedure. The procedure and interface described below are correct for version 4.7 of Windows Messenger for Windows XP.

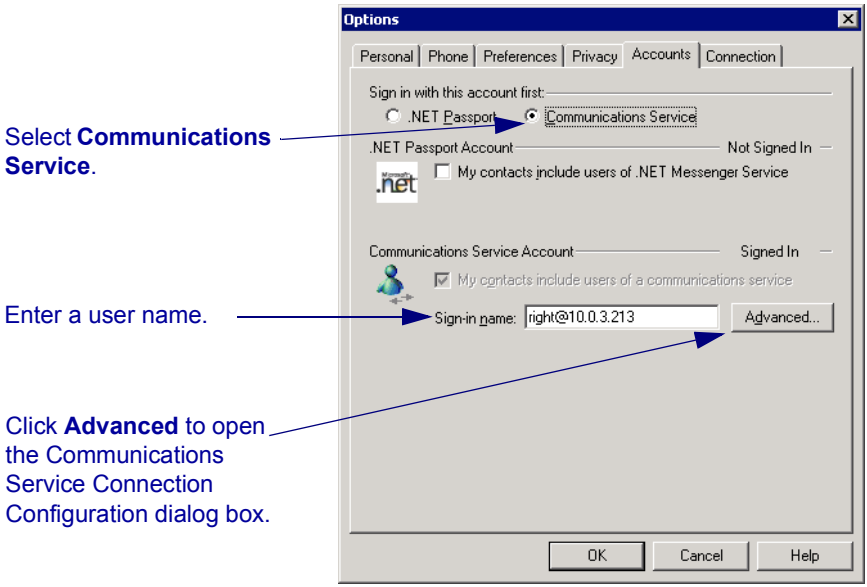
➤ To register into the MXM

1. In the Windows XP Messenger application, open the **Tools** menu and click **Options**. Click the **Accounts** tab.
2. Define the following:

Sign in with this account — Select **Communications Service**.

Sign-in name — Enter a user name using the following syntax: [*alias*]@[*IP address of SIP Proxy*]

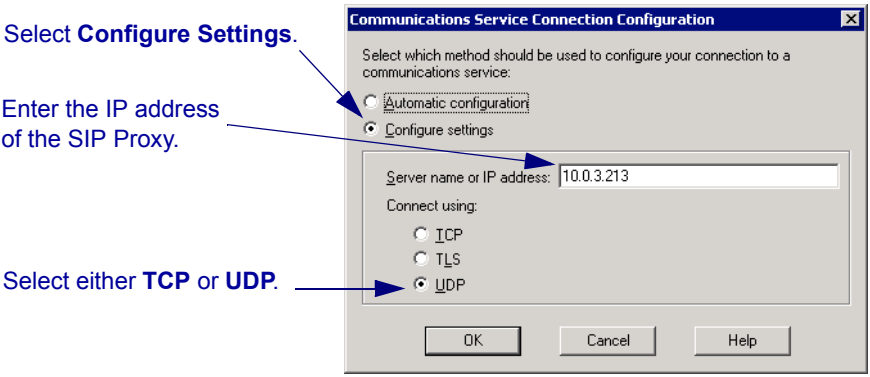
The SIP Proxy may be located in the same computer as the MXM Server.



Setting Up the Windows XP Messenger Client Account

3 Click **Advanced**. In the Communications Service Connection Configuration dialog box, define the following:

Configure settings	Select this method to configure the user agent system's connection to a communications service.
Server name or IP address	Enter the IP address of the SIP Proxy.
Connect using	Select either **TCP** or **UDP**, depending on the network's specifications.



Setting the Communications Service Connection Configuration

4 Click **OK** in both open dialog boxes to implement the configuration.

16.6 Dialing Unlisted Users in Windows XP Messenger

MXM end points (H.323) and SIP user agents other than Windows XP Messenger are not listed in the Windows XP Messenger address book. To dial these users, you must enter an MXM directory number (E.164), IP address, or alias in the Windows XP Messenger manual dialer.

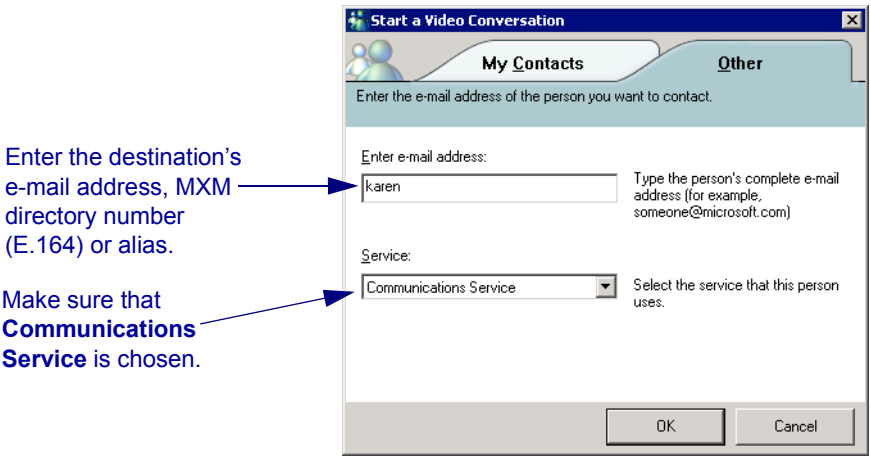
For communication between a Windows XP Messenger and an H.323 end point or other SIP user agent, the MXM supports the following:

- Video conversation
- Voice conversation

➤ To dial unlisted users from Windows XP Messenger

1. In the **Actions** menu, click **Start a Video** (or **Voice**) **Conversation** and then the **Other** tab.
2. Enter the following information:

Enter e-mail address	Enter the destination's e-mail address, MXM directory number (E.164) or alias.
Service	Make sure that **Communications Service** is chosen.



Dialing an Unlisted User

3. Click **OK**.

17 EMBLAZE-VCON CLUSTER MODULE

The Emblaze-VCON Cluster Module is available only for licensed users of the Emblaze-VCON High Availability Option. If you want to add this option to your MXM-based network, please contact your local Emblaze-VCON distributor.

The Emblaze-VCON Cluster Module enables your organization's conferencing network to stay online, even if the active MXM server goes down. In such a condition, a standby MXM takes over the MXM functions, continuing to provide conferencing and management services to logged-in nodes (during a takeover, open calls disconnect, but users can reconnect the calls within a few seconds).

A cluster configuration comprises two MXMs installed on different physical servers, one active and one standby, that share the same SQL Server database. The configuration requires that an IP address be reserved for all servers in the Cluster, which can be "transferred" to the standby MXM server during a takeover.

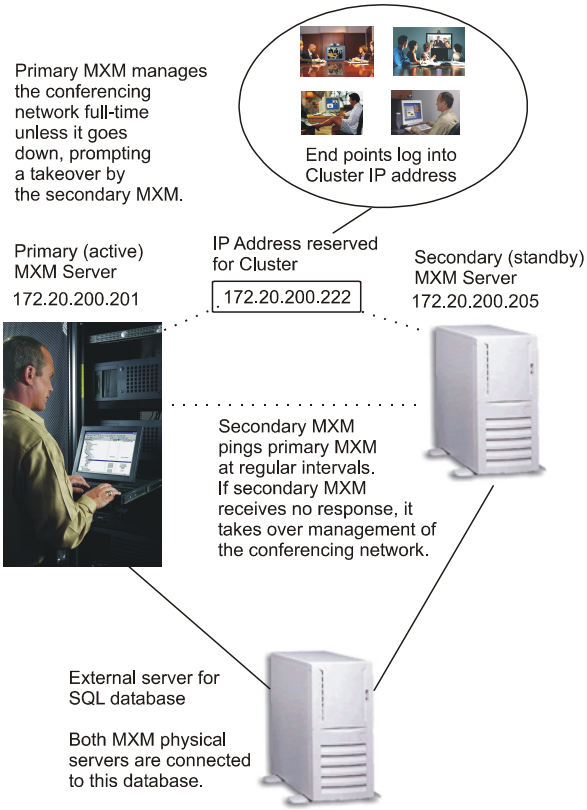
During normal operation, the standby MXM server pings the active MXM server at a defined interval. If the active MXM does not respond, the standby server becomes the "active MXM".

This chapter describes how to install and set up a Cluster configuration. The main stages of the setup are:

- Installing SQL Server on an External Server
- Installing the MXM Servers
- Verifying Correct Installation
- Installing the Cluster Application
- Customizing Cluster Operation

This chapter also describes the following operational issues:

- Takeover Events
- Shutting Down the Cluster Service
- Switching the Active MXM
- Licensing the Cluster MXMs



Example of a Cluster Configuration

17.1 Installing SQL Server on an External Server

Install the SQL Server database on a separate computer from the MXMs. If an SQL Server database for your conferencing section is already installed, you can skip this stage.

➤ To install the MXM database

1. Insert the MXM Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.

   Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file. The Installation program appears.

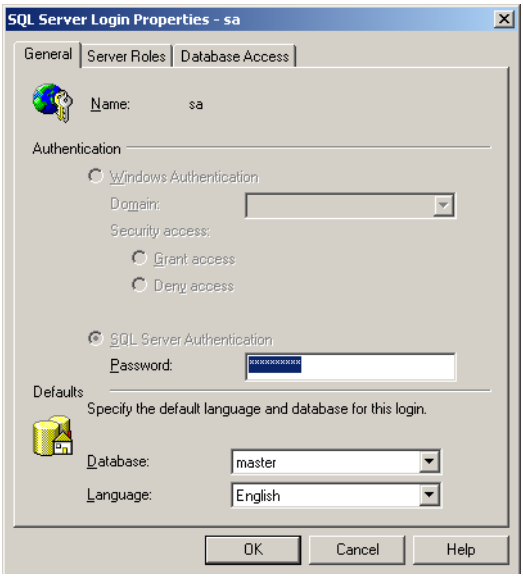
3 Select **MXM Server**.

If SQL Server is not detected on this computer, the Setup program installs it.

4 When prompted, restart the computer.

5 After the computer restarts, the MXM Setup Wizard opens. Click **Cancel** to stop the MXM installation and exit the Wizard (continuing the Wizard at this stage installs the MXM Server which is not wanted on this computer).

6 In the SQL Server Enterprise Manager, set up an administrator account with User Name **sa** and the SQL Server Authentication>Password **MXM#2004** (in UPPER CASE).



Setting up Login to SQL Server

17.2 Installing the MXM Servers

The installation process requires a primary MXM server and a secondary MXM server. However, once the configuration is up and running, either one can be the "active" server, while the other one is on "standby," waiting for a condition that initiates a takeover.

Before Installing the MXMs

Make sure that the servers meet the following requirements:

- Minimum requirements for running an MXM (see "Minimum System Requirements" on page 5).
- 1 network interface card (NIC) on each computer.
- Primary and secondary servers each have 1 unique IP address.
- 1 unused IP address reserved for the Cluster. This will be the gatekeeper or SIP proxy address for the registered end points.
- To reduce the chances of a condition where both MXMs fail to respond to client requests, each MXM physical server is connected to a different switch in your organization's network.

Installing the Primary MXM

During the Primary MXM installation, you have to connect it to the external SQL Server database.

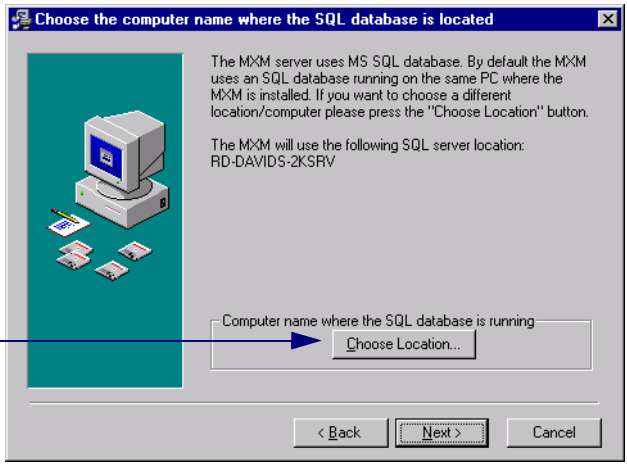
➤ To install the MXM on the "primary" server

1. Insert the MXM Setup CD-ROM in your computer's CD-ROM drive.
2. If Autorun is enabled, the Installation program appears automatically.

   Otherwise, click **Start** in the Windows taskbar and then click **Run**. Browse to the CD-ROM drive and double-click the *Setup.exe* file. The Installation program appears.
3. Select **MXM Server**.

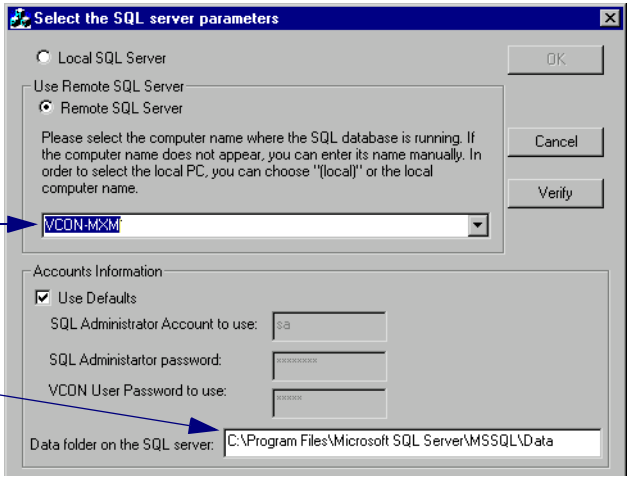
If the SQL Server database is not detected on this computer, the Setup program installs it as part of the MXM Setup program. Later, you will connect to the external SQL Server, despite its presence on this physical server.

4. Follow the instructions in the Setup Wizard, clicking **Next** to continue.
5. The Wizard asks where to connect to the SQL Server database. Click **Choose Location** and then enter the external SQL Server's computer name or IP address.



Click **Choose Location** to select the external SQL Server.

SQL Server Location



Choose the external SQL Server's computer from the list.

Enter the location of the SQL Server database file (**.mdf*).

Choosing the SQL Server's Computer

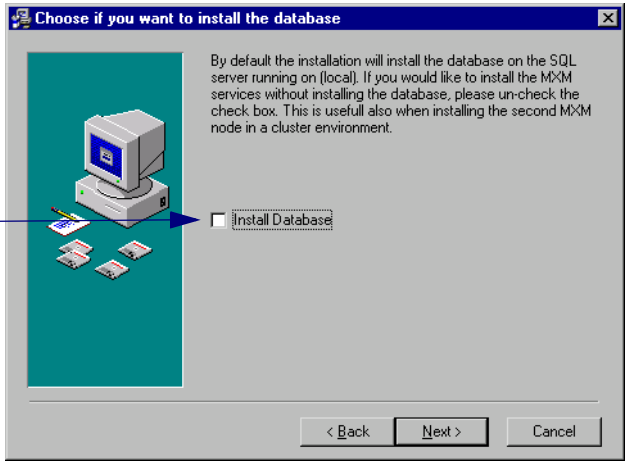
6. Keep the default account and password information.
7. Enter the location of the SQL Server database file (**.mdf*).
8. Click **Verify** to check for successful connection to the defined SQL Server
9. Click **OK**.
10. After finishing the MXM installation, shut down this server.

Installing the Secondary MXM

➤ To install the MXM on the secondary server

1. Perform steps 1 to 4 as described in the previous procedure.
2. The external SQL Server already has an MXM database image (from the Primary server). To avoid recreating this database, even though the MXM installation automatically creates one, you must connect to the SQL Server installed on this computer. In the SQL Database Installation page, deselect **Install Database** and click **Next**.

Disable SQL database installation for the secondary MXM Server.



Deselect SQL Database Installation

17.3 Verifying Correct Installation

At this stage, it is important to verify that the installations of the MXMs and their connections to the SQL database succeeded.

➤ To verify correct SQL database connection

1. Shut down the secondary MXM server.
2. Turn on the primary MXM server and log in to the MXM Administrator.
3. Register any end point to the MXM.
4. Stop the MXM services. In the Windows Desktop, click **Start**, point to **Programs**, **VCON**, **MXM**, and then click **Stop MXM Services**.
5. Turn on the secondary MXM server and log in to the MXM Administrator.
6. Check if the end point registered above appears in the Main View.

   If yes, the connections to the SQL database are correct.
   If no, the likeliest error is an incorrect path or name of the SQL database.

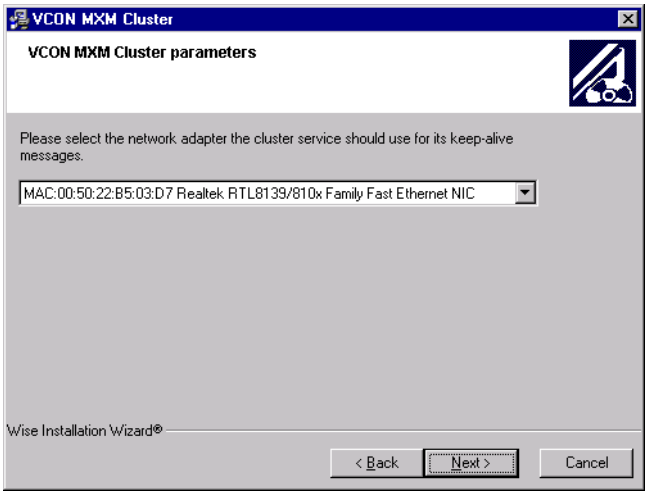
17.4 Installing the Cluster Application

During the installation of the Cluster module, you must define which network cards serve as the interfaces in the cluster configuration, and the IP address (same for both MXMs) to which end points and other devices register.

➤ To install the Cluster module

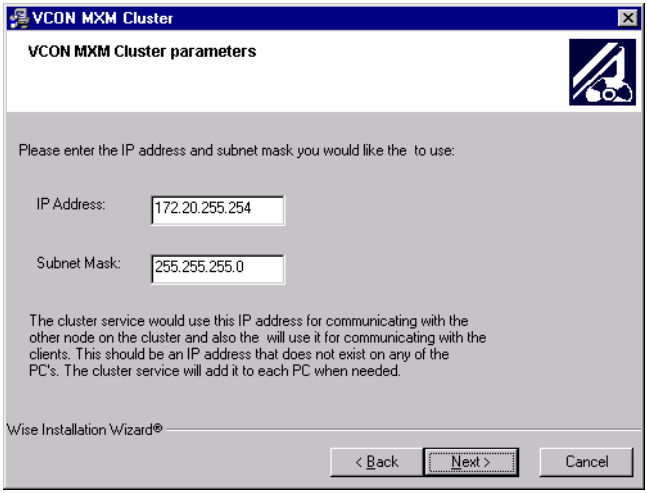
1. For both MXMs, define the MXM service's Startup Type as "**Manual**" instead of "**Automatic**". In the Windows Control Panel , double-click **Administrative Tools**, **Services**, and then **VCON MXM_1**.
2. In the **Startup Type** list, choose **Manual**.
3. Install Cluster application on the primary MXM computer. On the MXM Setup CD-ROM, browse to the *MXMCluster* folder and run the *Install_MXMCluster.exe* file.

   The Emblaze-VCON MXM Cluster Setup wizard appears.
4. Follow the instructions in the Setup Wizard, clicking **Next** to continue.
5. The Wizard asks you to choose the network adapter card through which the Cluster service sends Keep Alive messages. Choose one from the list and click **Next**.



Choosing Network Adapter Card for Sending Keep Alive Messages

6 Enter the reserved unused IP address (see "Before Installing the MXMs" on page 326) and a subnet mask which will be shared with the other MXM server as the Cluster IP. This IP address will likely be defined in the MXM client end points configurations as their MXM, Gatekeeper or SIP Proxy IP address. Click **Next** to continue.



Defining Cluster IP Address and Subnet Mask

7. When you finish the Cluster Setup wizard, click **Finish** and restart the Primary MXM computer.
8. Install the Cluster application on the secondary MXM computer.
9. As in step 5, choose the network card through which the Cluster service sends Keep Alive messages and click **Next**.
10. Choose the same IP address as was chosen for the Cluster application in the primary MXM computer (see step 6) and click **Next**.
11. When you finish the Setup Wizard, restart the secondary MXM computer.

➤ To verify successful Cluster application installation

1. Run the **ipconfig** DOS command to determine which computer is using the Cluster IP address.
2. Disconnect the network cable from the computer using the Cluster IP address.
3. After several seconds, run **ipconfig** on the other computer. If the response displays the Cluster IP address, the installation was successful.
4. Reconnect the first computer to the network.

17.5 Customizing Cluster Operation

You can customize the operation of the Cluster application by modifying the following registry entries
(in *HKEY_LOCAL_MACHINE\SOFTWARE\VCON\VCONCLUSTER*):

Operational Registry Entries

SleepTime — Interval at which the standby MXM pings active MXM. If the standby MXM does not receive a response to the ping, it initiates a takeover.

The default interval = **30** seconds.

StartServices — Batch file which runs during a takeover. You may edit this file to run other commands in addition to the takeover and relevant e-mail notification. For example, you can start other applications and/or initiate another batch file.

Setting Up E-mail Notification

In the registry, define the parameters for SMTP e-mail for sending e-mail notifications of takeover events.

EmailTo Address to send e-mail notifications, such as an administrator's address.

EmailFrom Address from which e-mail notifications are sent, such as the e-mail address of the MXM server.

EmailSubject Default title for the e-mail notifications, such as "Cluster Alarm."

EmailStartBody When the cluster service starts in the MXM server, it sends a "Starting" notification to the **EmailTo** address. Enter the text which appears in this notification, such as "**MXM Cluster starting in 172.20.1.2.**"

EmailStopBody When the cluster service is stopped in an "orderly"manner, such as a manual service stoppage in *My Computer\Manage\...\Services*, it sends a "Stopping" notification to the **EmailTo** address. Enter the text which appears in this notification, such as "**MXM Cluster stopping in 172.20.1.2.**"

If service is stopped abruptly, such as by a power stoppage, the "Stopping" notification is not sent immediately, although it may be sent when the cluster service starts again. However, if the previously standby MXM took over, you are likely aware that the first MXM's cluster service stopped because you received a "Starting" notification from the other MXM.

EmailServer Name of the e-mail server which handles the notifications.

17.6 Takeover Events

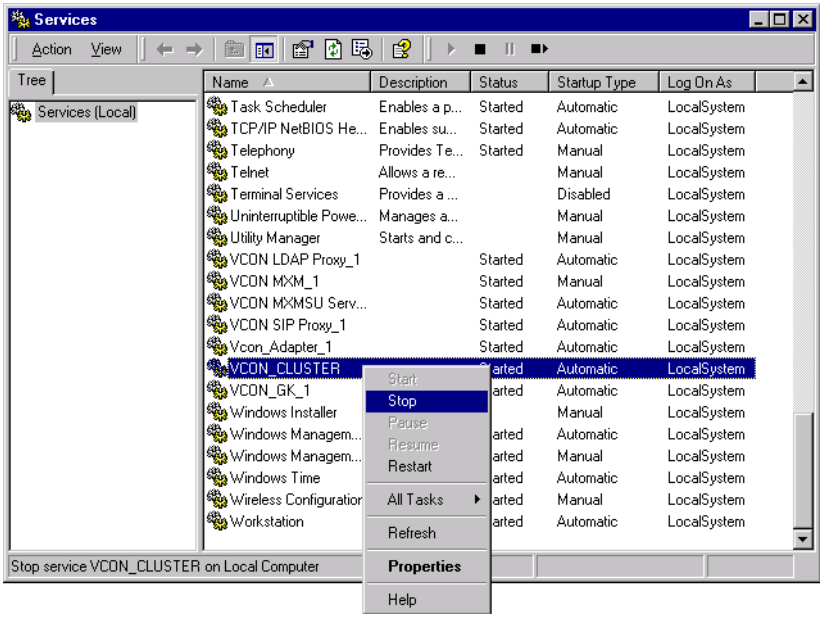
The standby MXM takes over if the active MXM does not respond to the ping. This condition is likely caused by a NIC failure. The administrator receives an e-mail alarm that a failure and takeover occurred (defined in the EmailStartBody and EmailStopBody registry entries).

If a General Protection Fault (GPF) occurs, the MXM restarts after about 10 seconds.

17.7 Shutting Down the Cluster Service

➤ To shut down the Cluster service

❑ Stop the active MXM's Cluster service. In the Windows Control Panel , double-click **Administrative Tools** and **Services**. Right-click **VCON_CLUSTER** and then click **Stop**.



Stopping the Cluster Service

17.8 Switching the Active MXM

To make the second MXM the active one, you simply need to stop the Cluster service in the active MXM PC.

➤ To make the standby MXM active

❑ Disconnect the cable from the active MXM.

-or-

Stop the active MXM's Cluster service. In the Windows Control Panel , double-click **Administrative Tools** and **Services**. Right-click **VCON_CLUSTER** and then click **Stop** (see the illustration above).

17.9 Licensing the Cluster MXMs

In a Cluster configuration, both MXMs have the same license key. Either PC can import the license key from the other PC (see "Replacing the MXM License Key" on page 11).

18 CUSTOMIZING THE MXM ADMINISTRATOR

In the MXM Administrator application, you may customize the application according to your personal preferences. A set of defined window, table, and layout properties for the Administrator application is called a *workspace*. This chapter explains the following customization tasks:

- Defining the Main View Options
- Setting Up the Workspace
- Customizing the Toolbar
- Customizing the Status Views

18.1 Defining the Main View Options

You can customize the following elements of the Main View through the Options dialog box.

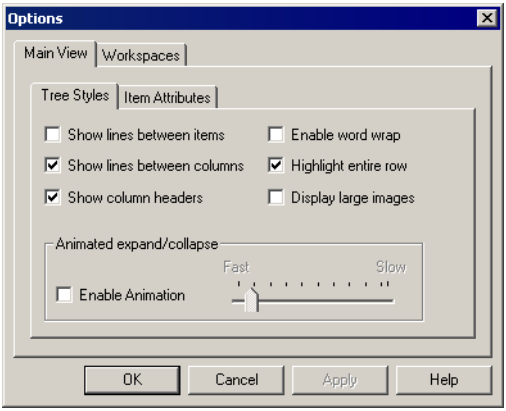
- ❑ Tree Styles - the appearance of the table format of the Main View.
- ❑ Item Attributes - the appearance (font, color, and so on.) of the various objects, such as end points and login requests.

Tree Styles

The Tree Styles Options control the appearance of tables in the main Administrator application window.

➤ To set Main View table properties

1. In the **View** menu, click **Options**. The Options dialog box appears with the **Tree Styles** tab open.
2. Change the appropriate properties. For descriptions of these properties, see "Tree Styles Properties" on page 336.
3. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.



Tree Styles Options

Tree Styles Properties

Set the Tree Styles properties according to your viewing preferences.

Enable Word Wrap Select this option to cause text in each column to continue automatically on the next line, after it reaches the end of each line. The line width is determined by the column borders.

If this option is not selected, sections of long phrases or names, that are not within the column borders, are not seen. However, a tooltip appears over those names.

Show Column Headers Select this option to display the column names that identify the information that appears in the Main View.

Main View Column Headers

Show Lines Between Columns Select this option to display the vertical borders between columns of the Main View.

Show Lines Between Items Select this option to display the horizontal borders between items.

Highlight Entire Row	Select this option to highlight the entire row when you select an item. In this case, you can click anywhere on the row. Deselect this option to highlight only the item name when you select it. In this case, you must click the name to highlight it.
Display Large Images	Select this option to view the workspace's details and images at a larger size.
Animated Expand/ Collapse	Select this option to expand and collapse the levels of the System tree in a graded, stuttering motion. To control the speed, drag the speed slider towards the left for faster motion or towards the right for slower motion. Deselect this option to expand and collapse the levels in one swift motion.

Item Attributes

In the **Item Attributes** tab, you can customize the way entries are indicated in the Main View. For example, you can change the color of the characters in order to differentiate between Emblaze-VCON end points, MCUs, hunting groups and so on. Also, you can assign sounds to indicate occurrences such as login requests.

To use the factory-set indication styles, do not make any changes. Keep **Use Default Attributes** selected for all entries.

➤ To customize the indications for entries in the Main View

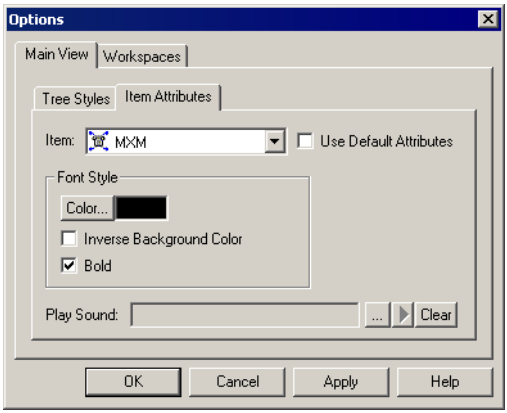
1. In the **View** menu, click **Options**. Click the **Item Attributes** tab.
2. From the **Item** list, select the entry type you want to customize.
3. Deselect **Use Default Attributes**.

4 Customize items, according to your own specifications, as follows:

Font Style

Color	Click and choose another color from the palette. If you want, you can also create colors that don't appear on the original palette.
Inverse Background Color	Select to add a highlight background to the item in the Main View.
Bold	Select to display the item name in bold letters in the Main View.
Play Sound	If you want, associate a sound with the item. Click this button to browse and locate Wave (*wav*) files. For example, you can find login request indication files in the *\\Vcon\Administrator* folder. Otherwise, you can use a *wav* file from another source.

5 Click **OK**.



Main View Item Attributes

18.2 Setting Up the Workspace

Several options are available for customizing the MXM Administrator's workspaces in accordance with your operating preferences.

Defining Workspace Options

The Options dialog box **Workspaces** tab contains options for storing the data and appearance that are associated with a specific Workspace.

➤ **To define Workspace options**

1. In the **View** menu, click **Options**. The Options dialog box opens to the **Workspaces** tab.
2. Change the appropriate properties. For descriptions of the properties, see "Workspace Properties" on page 339.
3. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.

Workspace Properties

Set Workspace properties as follows:

Save the active workspace when exiting — Select this option to automatically save all the current Workspace properties whenever you close the Workspace or the Administrator application.

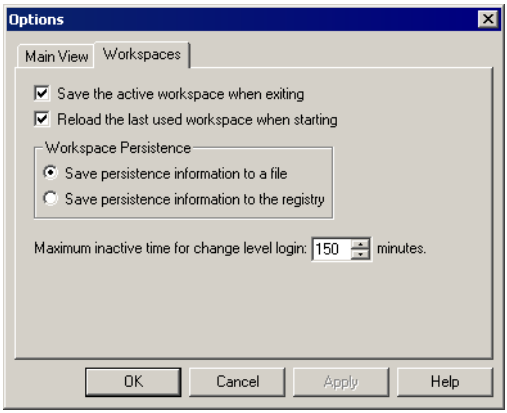
Reload the last used workspace when starting — Select this option to open the previously used Workspace whenever you start the Administrator application.

Workspace Persistence — Persistence information includes the customization properties defined for the workspace and the data about devices and other nodes that are defined within that workspace.

- ❑ Select **Save Persistence Information to a file** to store all of the current workspace's data in a file located in the Administrator application's root directory (Default is *C:\Program Files\Vcon\Admin*).
- ❑ Select **Save Persistence Information to the registry** to store all of the current workspace's data in the system Registry

Maximum inactive time for change level login

For administrators with "Change" privileges, this is the maximum amount of time that the MXM administrator remains idle. When this interval passes, a message asks you to disconnect or stay connected. If you do not respond, the administrator disconnects from the system.



Workspace Options

Managing Workspaces

The MXM Administrator application provides functions for managing and storing workspaces. These functions include:

- Saving a workspace
- Renaming a workspace
- Deleting a workspace
- Opening a workspace
- Reorganizing the Workspace list.

Saving a Workspace

A workspace may be saved in different formats:

❑ As a file - this is advantageous if you may log in to the MXM and use the same workspace from other computers.

❑ As information stored in the system registry - this is advantageous if more than one administrator may log in to the MXM from the same computer.

➤ To save a workspace as a file

In order to save workspaces as files, the **Save persistence information to a file** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Save Workspace Now**. The Save Workspace dialog box appears.
2. To create a new workspace file, type the name in the **File Name** box and click **Save**. The system automatically adds a *.paw* extension to the filename.

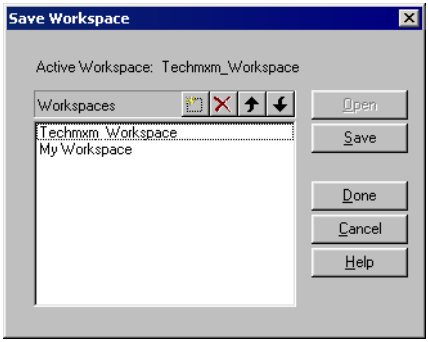
   -or-

   To update a previous workspace file, double-click the name of the file from the list. Then, click **Yes** to confirm.

➤ To save a workspace in the system registry

In order to save workspaces in the registry, the **Save persistence information to the registry** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Save Workspace As**. The Save Workspace dialog box appears.
2. Click the **New (Insert)** button.
3. Type the name of the new workspace.
4. Click in the free space of the dialog box. A confirmation request appears.
5. Click **Yes** to save the new workspace.



Saving a Workspace to the Registry

Renaming a Workspace

The procedure for renaming a workspace depends on whether you save workspaces to files or to the registry.

➤ To rename a workspace file

In order to rename a workspace file, the **Save persistence information to a file** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Click the workspace file that you want to rename. After 1 second, click again. The filename is highlighted for editing.
3. Type the new name and then click outside the new name area. The workspace file is now renamed.

➤ To rename a workspace that is stored in the registry

In order to rename a workspace in the registry, the **Save persistence information in the registry** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Double-click the workspace that you want to rename.The name is highlighted for editng.
3. Type the new name and then click below the list.
4. Click **Done** to exit the dialog box.

Opening a Workspace

The procedure for opening a workspace depends on whether you save workspaces to files or to the registry.

➤ To open a workspace file

In order to open a workspace file, the **Save persistence information to a file** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Double-click the file that you want to open. The Login To [*MXM name*] dialog box appears.
3. Type the required password and then click **Login**. The workspace opens in the Administration window.

➤ To open a workspace from the registry

In order to open a workspace from the registry, the **Save persistence information in the registry** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Click the workspace that you want to open and then click **Open**. The Login To [*MXM name*] dialog box appears.
3. Type the required password and then click **Login**. The workspace opens in the Administration window.

Deleting a Workspace

The procedure for deleting a workspace depends on whether you save workspaces to files or to the registry.

➤ To delete a workspace file

In order to delete a workspace file, the **Save persistence information to a file** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.
2. Right-click the workspace file that you want to delete and then click **Delete**. Click **Yes** to confirm.

   The workspace file is deleted from the system.

➤ To delete a workspace from the registry

In order to delete a workspace from the registry, the **Save persistence information in the registry** option of the Options dialog box must be selected. For more details, see "Defining Workspace Options" on page 339.

1. In the **File** menu, point to **Workspaces** and click **Open Workspace**. The Open Workspace dialog box appears.

2. Click the workspace that you want to delete and then click the **Delete** button.

   The workspace is deleted from the system. No confirmation is requested.
3. Click **Done** to exit the dialog box.

18.3 Customizing the Toolbar

You can set the buttons of the toolbars according to your preferences.

Defining the Toolbar Display

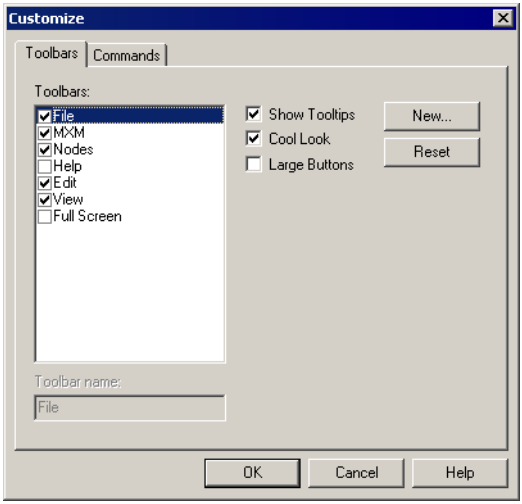
By default, the toolbars are docked in the Administrator window below the menu bar. You can choose any or all toolbars to be part of the application display. In addition, you can select among a number of other appearance options.

➤ To define the toolbar display

1. In the **View** menu, click **Customize**. The Customize dialog box opens to the **Toolbars** tab.
2. To display a particular toolbar on the screen, select it in the **Toolbars** list. To hide a toolbar, deselect it.
3. Set the toolbar display properties according to your preferences. The toolbar display changes as you change each setting. For a description of these properties, see "Toolbar Display Properties" on page 347.

   To return a toolbar to its default formation, select it in the **Toolbars** list and then click **Reset**.
4. Click **OK** to complete the change. To discard the change, click **Cancel**.

If you want to change the buttons on the toolbars, click **Apply** to implement the toolbar display property changes. Then, click the **Commands** tab.



Customizing Toolbar Display Properties

Toolbar Display Properties

Set toolbar display properties as follows:

Toolbars	In this list, select any or all of the various toolbars that will appear in the Administrator application window. Only toolbars that are marked with a ✓ will appear.
Show Tooltips	Select this option to display tool tips when you hold the pointer over a button for about 1 second.
Cool Look	Select this option to cause each button to display a raised effect when the pointer points it. When deselected, the buttons are static with clear borders.
Large Buttons	Select this option to increase the size of the buttons by 400% (4x).

Adding and Removing Toolbar Buttons

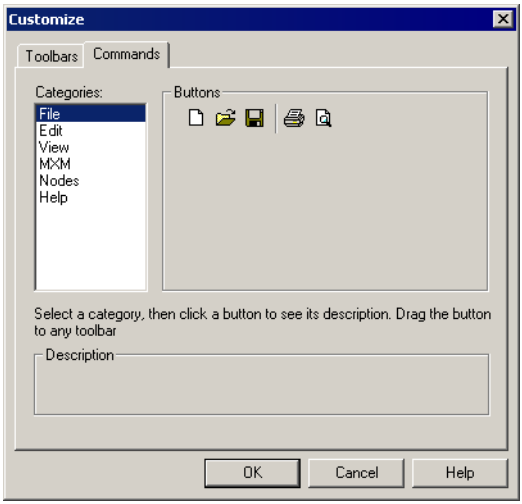
You can control the contents of each toolbar by adding or removing buttons, or moving buttons among the various toolbars.

➤ To control the contents of the various toolbars

1. In the **View** menu, click **Customize**. The Customize dialog box opens to the **Toolbars** tab.
2. Click the **Commands** tab.
3. To add a button to any toolbar, select a category from the **Categories** list. Drag the appropriate button to any toolbar in the Administrator window that you want.

   To remove a button from any toolbar, drag the button to the Customize dialog box.

   To move a button to another toolbar, drag the button to the new location.



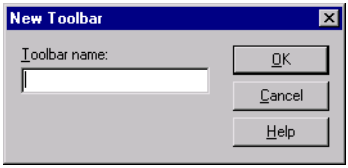
Customizing Toolbar Button Contents

Creating a Custom Toolbar

You can add a toolbar other than the standard ones provided by the Administrator application.

➤ **To add a custom toolbar**

1. In the **View** menu, click **Customize**. The Customize dialog box opens to the **Toolbars** tab.
2. Click **New**. The New Toolbar dialog box appears.



Adding a Custom Toolbar

3. Type the name of the new toolbar and click **OK**. The new toolbar appears in the Administrator window and its name appears in the **Toolbars** list.
4. Click the **Commands** tab.
5. Switching **Categories** according to your preference, drag any number of toolbars to the new toolbar.
6. Click **OK** to close the dialog box.

18.4 Customizing the Status Views

According to your preferences, you can customize the way that the Administrator displays information in the various status view tables. Design functions are available for:

- ❑ Displaying the various views
- ❑ Style formats for table elements or types of information.
- ❑ Style formats for printed tables.

Setting Table On-Screen Display Properties

This section provides instructions for customizing the on-screen display of the Administrator application's various table views. You can control the appearance of table elements such as gridlines and column heads, colors, and current cell.

The display properties affect only the active table view. To set the display properties of another specific table, you must enter that particular view.

➤ To set table on-screen display properties

1. In the View toolbar, click the table view that you want to format.

View Command Buttons

2. In the **View** menu, click **Display Properties**. The Display Settings dialog box appears.
3. Set the display properties according to your preferences. For a description of these properties, see "Table Display Settings" on page 351.

   In the **Preview** area of the dialog box, you can preview the effects of your changes.
4. Click **OK** to implement the settings.

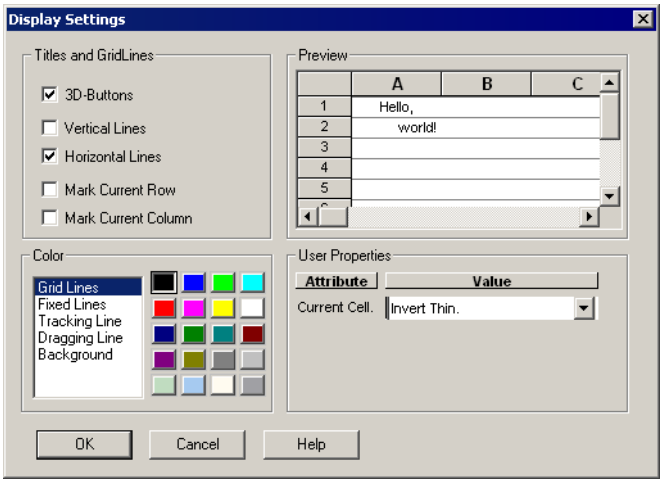


Table Display Settings

Table Display Settings

Set the table display properties as follows:

Titles and Gridlines

Select **3D Buttons** to display column and row titles inside borders.

Select **Vertical Lines** to display borders between columns.

Select **Horizontal Lines** to display borders between rows.

Select **Mark Current Row** and/or **Mark Current Column** to provide a 3-D pressed appearance to the selected row/column heading.

Color

Click any item in the Color list and then click the required color from the adjacent palette.

- **Grid lines** are the borders between columns and rows.
- **Fixed lines** are rows that are in a specific location permanently. They cannot be sorted.
- **Tracking Line** is the border that is being dragged during a Resize Column/Row action.
- **Background** represents the empty area behind and around the table.

User Properties

In the **Value** list, select the option that determines the appearance of the adjacent **Attribute**.

Style Formats for Table Elements or Types of Information

You can customize the display styles of various table elements, such as column headers and standard cells. For example, you can change the font style and colors of particular information that must be quickly recognizable.

The style formats affect only the active table view. To set the style formats of another specific table, you must enter that particular view.

➤ To change the formatting of a table element

1. In the View toolbar, click the table view that you want to format.

2. In the **Format** menu, click **Styles**. The Styles dialog box appears.
3. In the **Names** list, click the element that you want to format and then click **Change**.

   A style formatting dialog box appears for the selected element. By default, the **Font** tab is open.
4. Set the style properties according to your preferences. For a description of these properties, see "Style Format Properties" on page 353.
5. Click **OK** to complete the change. If you want to discard the change, click **Cancel**.

Table Element Styles Dialog Box

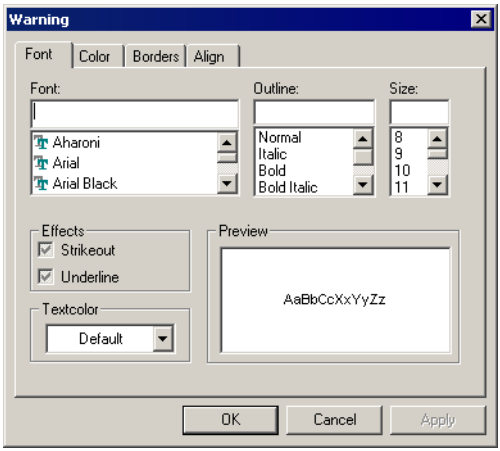
Style Format Properties

The following categories make up a table element style:

- Font
- Color
- Borders
- Align

Font Properties

For the table's text, you can select the font, its size, and any special characteristics such as **Bold** or **Underlined**.

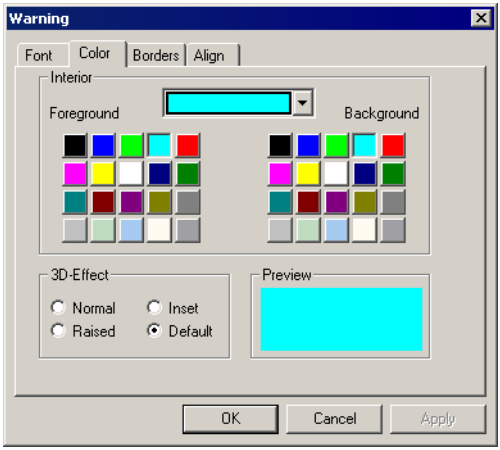


Font Properties

Color Properties

In the style changing dialog box, click the **Color** tab.

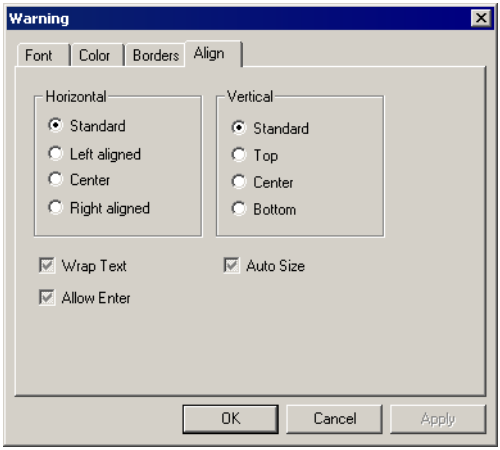
- ❑ To change the color of the table element, click a color in the **Foreground** group.
- ❑ To change 3-D effect (such as raised, pressed, or normal flat) of the table element, select one of the options in the **3-D Effect** group.



Color Properties

Borders Properties

1. In the style changing dialog box, click the **Borders** tab.
2. In the **Border** group, select the side(s) of the cells that you want to change.
3. In the **Type** group, select a type of line and/or thickness. If necessary, select a different color from the **Color** list.

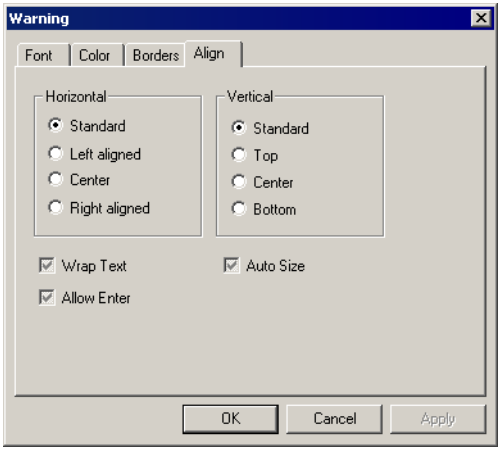


Borders Properties

Align Properties

To change Align properties of the selected table element, click the Align tab in the style changing dialog box.

- In the **Horizontal** group, select left, center or right text alignment in the cells.
- In the **Vertical** group, select top, center, or bottom text alignment in the cells.
- Select **Wrap Text** to display cell text on a new line if the text exceeds the cell's borders.
- Select **Auto Size** to set the size of the columns automatically according to the column's content.



Align Properties

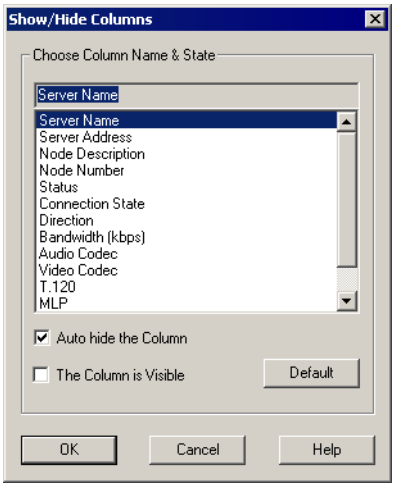
Showing and Hiding Columns

By default, some of the Node Status View table's columns always appear and some appear only if the node is connected to ISDN. In the Show/Hide Columns dialog box, you can change these settings to display or hide the columns of your choice.

This feature is applicable only to the Node Status View.

➤ To show and hide columns

1 In the **Format** menu, click **Show/Hide Columns**. The Show/Hide Columns dialog box appears.



Show/Hide Columns Dialog Box

2 In the **Column Name & State** list, choose the column whose display status you want to change.

3 Select Properties as follows:

Auto Hide the Column	The column is displayed if relevant to the node's current status, and hidden in other situations. If deselected, the column is constantly displayed or not displayed according to the **The Column is Visible** option below.
The Column is Visible	The column is displayed in the Table View on the screen. If deselected, the column is hidden.
Default	Click **Default** to return to the default Table View, according to the nodes listed in the table.

4 Click **OK** to implement the new settings.

A vPoint HD End Point Properties

From the MXM Administrator application, the administrator may view and control various properties of vPoint HD end points. vPoint HD is a high-quality software-based videoconferencing client.

For explanations about end point MXM Properties, see "Setting End Point MXM Properties" on page 91 to 106.

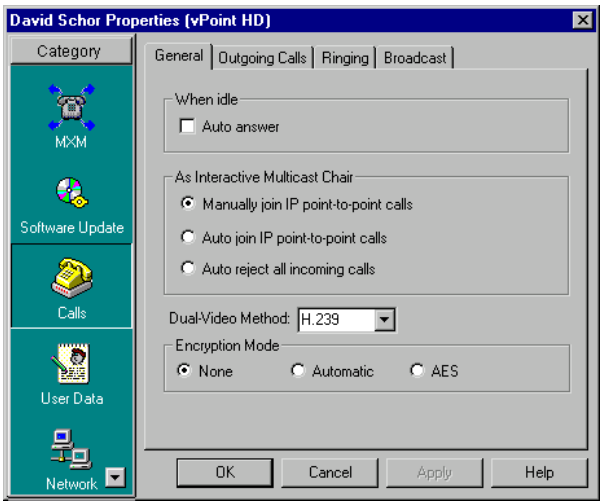
For explanations about end point Software Upgrade Properties, see "Node Software Upgrade Properties" on page 122 to 128.

A.1 Calls Properties

The Calls Properties dialog box may be used for viewing and controlling incoming and outgoing call properties of vPoint HD end points.

General

In the **General** tab, customize how the vPoint HD end point indicates and accepts incoming calls. Also, enable or disable H.239 dual-video transmission and H.235 encryption protocol.



vPoint HD End Point - General Properties

When Idle

Auto answer Select to turn automatic acceptance of calls on. If the system is idle when a videoconferencing call arrives, the session starts automatically.

As Interactive Multicast Chair

If the selected user's system supports VCON's Interactive Broadcast, it may sometimes be the Chair of Broadcast sessions. If another party tries to call it while it chairs a conference, that call may be accepted or rejected according to the selected option :

Manually join IP point-to-point calls Enable the selected user to either join or reject callers to an ongoing Broadcast.

Auto join IP point-to-point calls Enable the selected user to automatically join callers to an ongoing Broadcast.

Auto reject all incoming calls Enable the selected user to automatically reject incoming calls to an ongoing Broadcast.

Dual-Video Method Define the permitted method for transmitting dual video streams during a conference managed through this service.

The H.239 standard enables end points to convert data into a separate media stream and transmit it parallel to the video stream. Video systems supporting H.239 display shared data and live video in separate windows. Systems not supporting H.239 display only the shared data in a single window.

- Choose **None** to block all dual video transmission.
- Choose **Non-H.239** to allow a different method of dual video transmission than H.239.
- Choose **Auto** to allow either H.239 dual video transmission or another method.

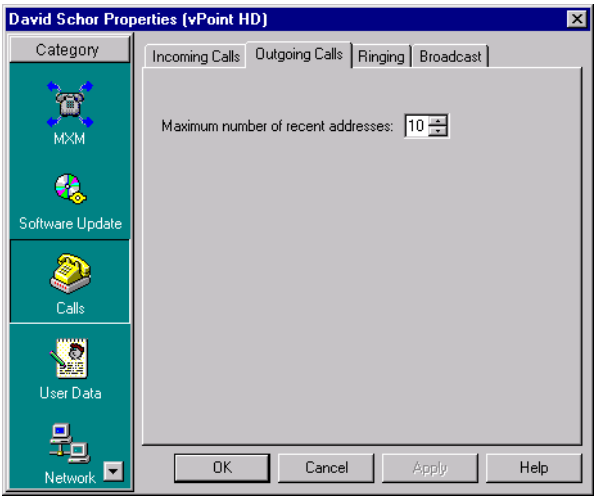
Encryption Mode

If calls from this end point will be encrypted, choose the type of encryption from the list.

- Choose **None** to allow unencrypted calls.
- **AES** (Advanced Encryption Standard) is a standard encoding method for encrypting data transmissions in commercial and government sectors of the USA and its use is growing worldwide.
- **Auto** enables the vPoint HD to select among any installed and supported encryption type.

Outgoing Calls

In the **Outgoing Calls** tab, define properties for calls initiated by the selected vPoint HD end point.

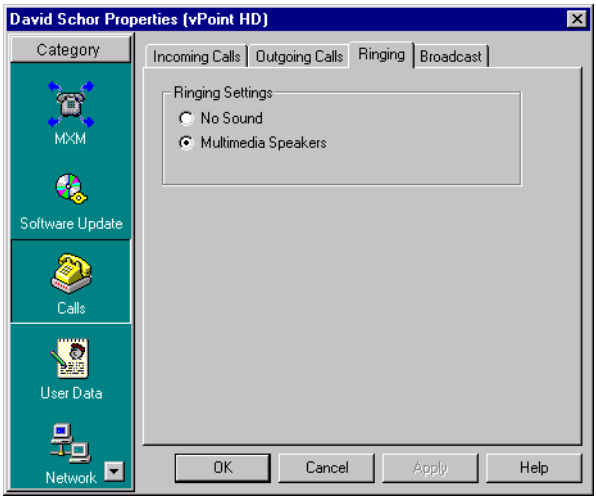


vPoint HD End Point - Outgoing Calls Properties

Maximum Number of Recent Addresses — The maximum number of recently dialed addresses that can appear in the vPoint HD Manual Dialer's Call Log.

Ringing

In the **Ringing** tab, define the sounds used by the selected end point to indicate incoming and outgoing videoconference calls.



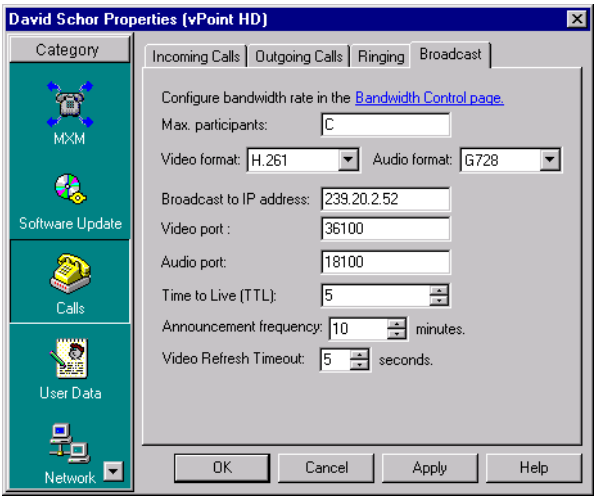
vPoint HD End Point - Ringing Properties

No Sound — Select to disable all audio ringing. Only the Incoming Call and Outgoing Call messages visually indicate calls.

Multimedia Speakers — Select to enable ringing sounds to indicate calls.

Broadcast

In the **Broadcast** tab, set the default configuration for this end point's Interactive Broadcasts.



vPoint HD End Point - Broadcast Properties

The default Broadcasting settings are recommended for most Broadcasting conditions.

Configure Bandwidth Rate in the Bandwidth Control page

Click the link to jump to the MXM Properties - Bandwidth Control dialog box, where you can set the Default Bandwidth for broadcast sessions.

Max. Participants

The maximum number of Participants allowed in a Broadcast initiated and chaired by this end point.

Video Format

The video coding standard that all parties in the Broadcast are capable of using - H.264, H.261 and H.263. H.264 provides much greater compression and sharper quality, while using less bandwidth, than its predecessor standards.

However, some video systems do not support H.264. If at least one Participant's system does not support H.264, or you are not sure, select H.261 or H.263.

Audio Format The audio standard that all parties in the Broadcast are capable of using.

- **G.711 U-law/A-law**
  This standard gives the lowest quality results, but it must be selected if you want broadcast viewers to be able to join a broadcast session. Select **G.711 U-law** if you're in the U.S. or Japan, or **G.711 A-law** if you're in Europe. For other regions, consult with your local Emblaze-VCON technical support representative.
- **G.722**
  This standard gives the best quality. Select it if you know that the remote parties support it and if you think that the connection will be over high bandwidths.
- **G.728**
  This standard gives the best possible quality with the smallest possible bandwidth cost. Select this standard if you know that the remote parties support it and that the connection will be over low bandwidths.

If you select either G.728 or G.722, and a remote party's system does not support it, that party will not be able to participate in the session.

Broadcast to IP Address The destination IP address for the Broadcast. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of **224.0.0.0** to **239.255.255.255**.

Video port The ID of the port used for the video connection.

Audio port The ID of the port used for the audio connection.

Participants must use the same video and audio ports. Make sure that the ports you choose are available for every participant.

Time to Live The maximum number of routers that the session's packets may pass through.

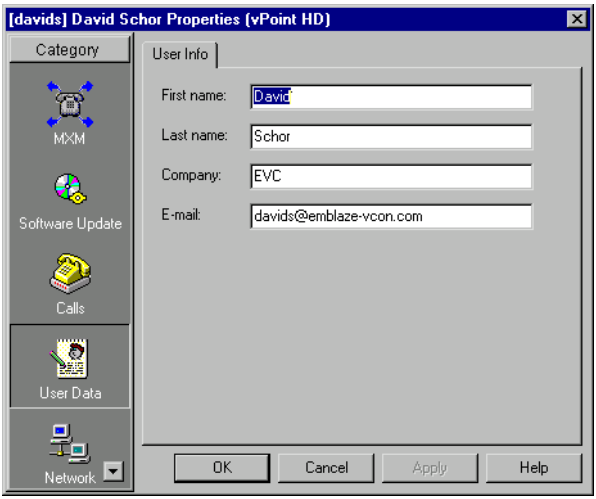
Announcement Frequency The interval between announcements of Broadcast sessions in the third-party viewer's schedule.

Video Refresh Timeout The maximum number of seconds required until the video broadcast is synchronized for all viewers. If the refresh value is low, the quality is lowered. If the refresh value is high, it will take a longer time to see the video display when the viewers connect. Use the default setting as a guide.

A.2 User Data Properties

The **User Info** settings provide identification of the vPoint HD end point user. This includes the following information:

- First Name
- Last Name
- Company or organization
- E-mail address



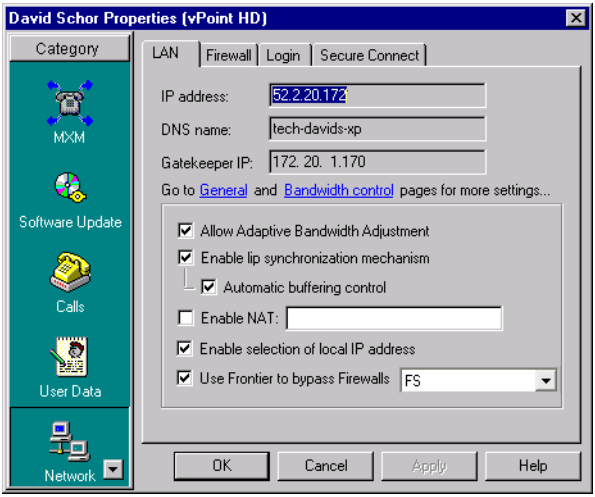
vPoint HD End Point - User Data Properties

A.3 Network Properties

The Network Properties dialog box may be used for viewing and controlling various network settings of vPoint HD end points.

LAN

The **LAN** tab contain the vPoint HD end point's identification configuration on the local network. Additional capabilities are provided for holding videoconferences over the connected network.



vPoint HD End Point - LAN Properties

IP Address — The selected end point's IP address.

DNS Name — The selected computer's name if it resides in a network that employs a DNS server (*DNS* stands for Domain Naming System, which enables computers on a network to be referred to by name in addition to IP Addresses).

Gatekeeper IP — The IP address of the MXM or gatekeeper from which this end point receives gatekeeper services.

Go to General and Bandwidth Control Pages for More Settings — Click the General link to display the selected user's MXM General Properties (see "General" on page 91).

Click the Bandwidth Control link to display the selected user's MXM Bandwidth Control Properties (see "Bandwidth Control Properties" on page 95).

Allow Adaptive Bandwidth Adjustment

Enables videoconferences to precede at reduced bandwidth if the network is congested. Deselecting this option maintains a constant quality to the session, but it may cause network problems.

Enable Lip Synchronization Mechanization

Enables adjustment of the video and the audio if they are out of sync with each other.

Automatic Buffering Control

- ❑ Enables the system to automatically control the amount of buffering required to maintain the consistency of the video and audio transmission. For example, if video packets are delayed for 1 or 2 seconds, the system will automatically synchronize the transmission so that the delay does not disturb the visible video.
- ❑ Deselect this option only if the automatic buffering is not sufficient — for example, if the quality of the video meeting is poor or there is a noticeable delay.

Enable NAT

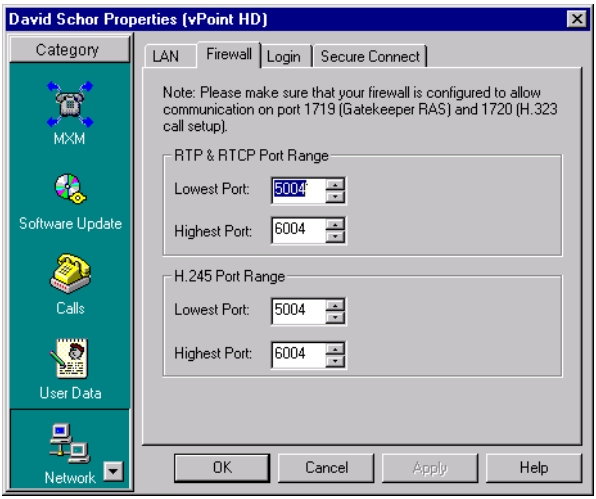
If your organization uses NAT (Network Address Translation) when communicating with parties in another LAN or WAN, type the external address for the selected user.

NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.

Enable Selection of Local IP Address	Enables the end point to receive its IP address configuration from the LAN's DHCP server. A DHCP server automatically assigns IP addresses to computers as they log on to the network, eliminating the need to assign IP addresses manually and locally.
Use Frontier to Bypass Firewalls	Enables the endpoint to be a Frontier Client. Emblaze-VCON's Frontier system provides conferencing security services, such as firewall traversal, address translation, and encryption. The MXM will add the end point to the User List of the Frontier Server specified in the adjacent list. The Frontier Server must be listed in the MXM's Frontier Servers View

Firewall

In the **Firewall** tab, enter the allocation of ports for communication through your organization's firewall.



vPoint HD End Point - Firewall Properties

RTP & RTCP Port Range — The MXM allocates a range of ports for video and audio during videoconferences.

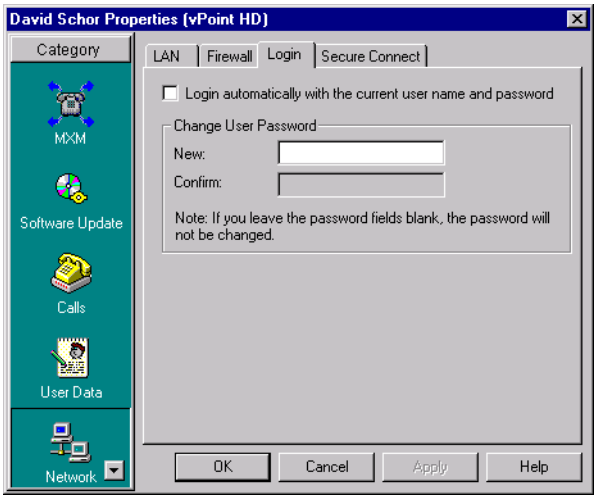
This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

H.245 Port Range — The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences.

This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

Login

In the **Login** tab, define how the end point logs into an MXM.



vPoint HD End Point - Login Properties

Login Automatically with the Current User Name and Password — The end point automatically logs in to the MXM during vPoint HD's startup using the current User Name and Password. If this option is selected, the user does not have to enter login details during vPoint HD's startup.

Change User Password

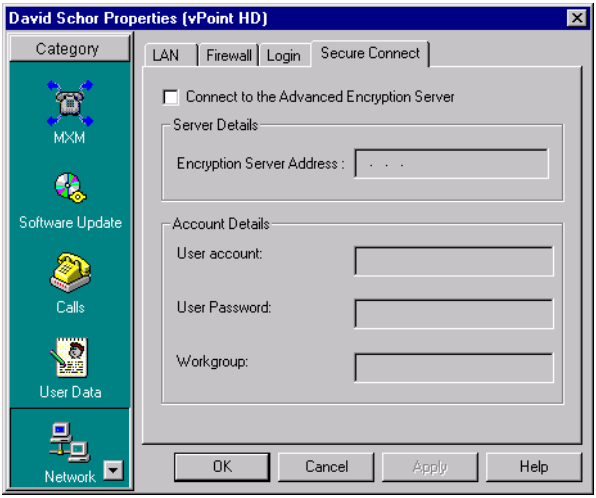
New — Password that replaces the current one.

Confirm — Confirmation of the new password.

If the Password boxes are blank, the current password remains valid.

SecureConnect

The SecureConnect Properties are applicable if the SecureConnect Encryption Client is installed in the end point's computer. The **SecureConnect** tab describes this system's Encryption Client identification configuration in a connected Emblaze-VCON Advanced Encryption Server (AES). The AES encrypts conferences and other data transmissions across public or private networks.



vPoint HD End Point - SecureConnect Properties

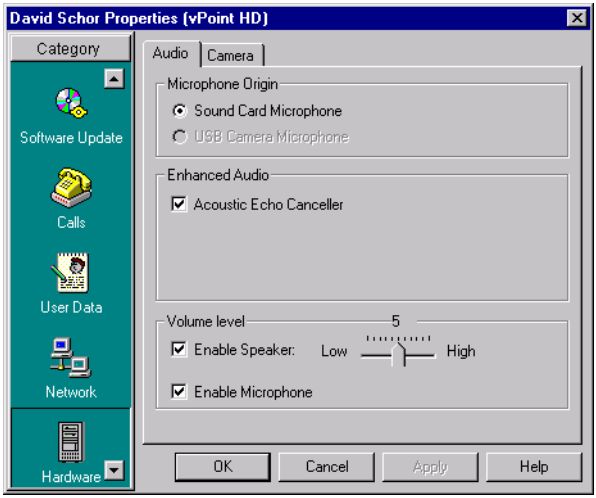
Connect to the Advanced Encryption Server	Select to enable the end point to register with the AES using the settings below.
Encryption Server Address	The IP address of the AES.
User Account	Username required for this end point to log in to the AES.
User Password	Password required for logging in to the AES.
Workgroup	User Group (defined in AES) to which this end point is assigned.

A.4 Hardware Properties

The Hardware Properties dialog box may be used for viewing and controlling various Audio and Camera settings of vPoint HD end points.

Audio

In the Audio Settings for the vPoint HD, you can define the audio configuration to be used during videoconferences.



vPoint HD End Point - Audio Properties

Microphone Origin

Sound Card Microphone — Use a microphone that's connected to your computer's sound card.

USB Camera Microphone — Use the camera's built-in microphone.

Enhanced Audio

Acoustic Echo Canceller (AEC) — Select to cancel the echo created when your microphone picks up audio from your speakers.

AEC is not available if you are using a **USB Camera Microphone**.

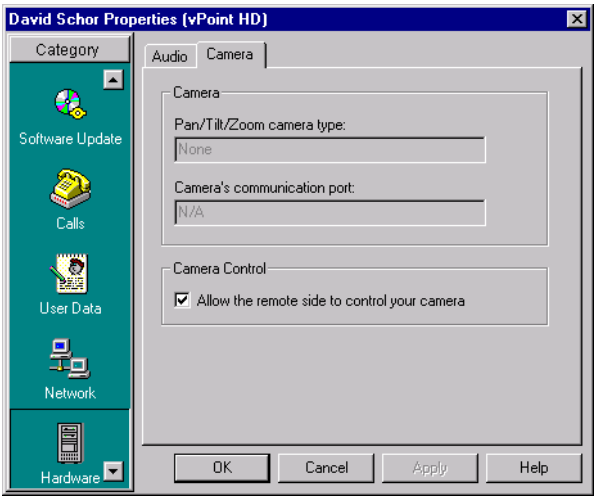
Volume level

Enable Speaker — Select to control the volume of the selected end point's speaker. Drag the slider accordingly.

Enable Microphone — Select to control the volume through the selected end point's microphone.

Camera

The Pan/ Tilt /Zoom Camera properties are applicable if a Pan/Tilt/Zoom-type (PTZ) camera is connected to the selected system. If a PTZ camera is not used, **None** appears as the PTZ camera type in the dialog box's top list and no communication port is required.



vPoint HD Properties - Camera

Pan/Tilt/Zoom camera type — The manufacturer and/or model of the PTZ camera.

Camera's communication port — The name of the computer port to which the camera is connected.

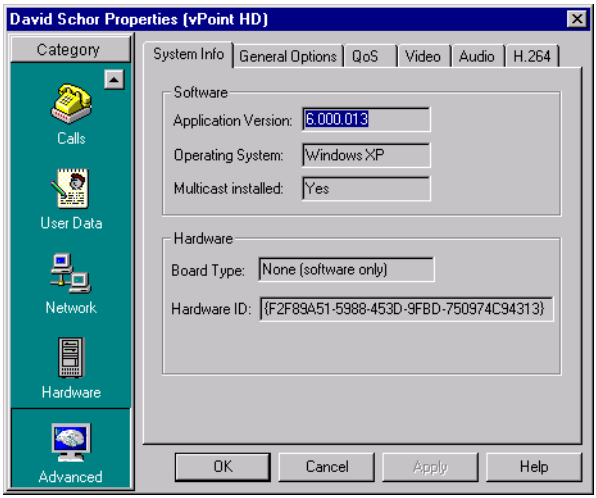
Allow the remote side to control your camera — Select to permit a remote party in a videoconference to control the positioning of the selected user's PTZ camera. If a PTZ camera is not used, this option is not relevant.

A.5 Advanced Properties

The Advanced Properties dialog box may be used for viewing end point system information and controlling various QoS, Intras, advanced Video, advanced Audio, and H.264 settings of vPoint HD end points.

System Info

The **System Info** tab displays information about the Emblaze-VCON videoconferencing system that's installed in the selected end point. If you contact Emblaze-VCON Technical Support (see "Emblaze-VCON Technical Support" on page vi before the Table of Contents) about a problem associated with this end point, include this information with your request.



vPoint HD Properties - System Information

Software

Application Version	Version number of the vPoint HD application running on the end point's computer.
Operating System	Operating system that's installed on the end point's computer.
Multicast installed	Indicates if the end point's videoconferencing system includes Emblaze-VCON's Interactive Multicast feature.

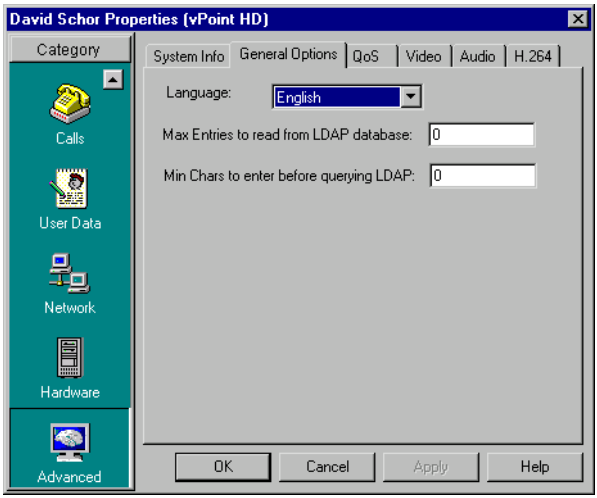
Hardware

Board Type Videoconferencing hardware installed in the end point's computer. For vPoint HD, this value should be **None**.

Hardware ID Unique identification number for the videoconferencing card's installation. This number is for Emblaze-VCON Technical Support use.

General Options

The **General Options** settings contains options for various system preferences. Set them according to your configuration requirements.



vPoint HD End Point - General Options Properties

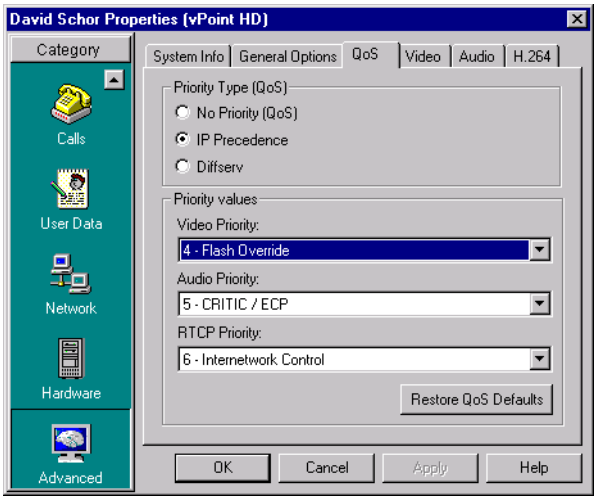
Language Select the language of the vPoint HD interface.

Max. Entries to read from LDAP database Maximum number of online directory entries that the end point will receive and display for the user.

Min Chars. to enter before querying LDAP Minimum number of characters that the user must type before the end point sends a search query to the online directory.

QoS

The **QoS** tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the specified vPoint HD end point.



vPoint HD End Point - QoS Properties (Default Settings)

Set QoS properties as follows:

Priority Type (QoS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

No Priority — Network transfers packets using normal Best-effort (or Routine) packet transmission.

IP Precedence — Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.

Diffserv — Network transfers packets according to specific needs of the sending application.

Priority Values

Video, Audio and RTCP Priority

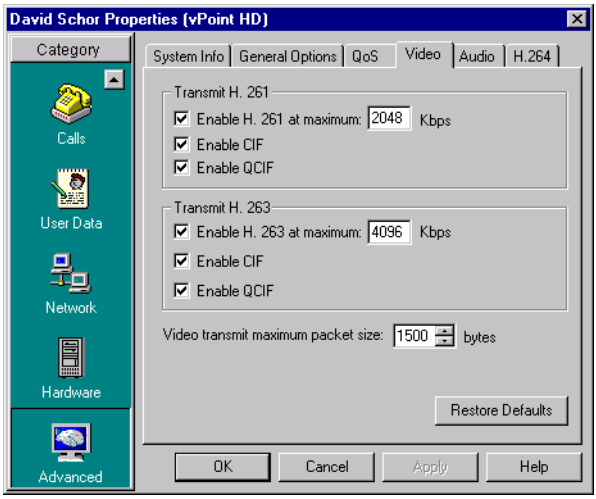
For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see "QoS Priority Values" on page 465.

To reset the Priority default values, click **Restore QoS Defaults**.

Advanced Video

The Advanced **Video** tab permits you to enable usage of H.261 and H.263 for video transmission and to control the bandwidth thresholds for switching between the two standards, if applicable.



vPoint HD Properties - Advanced Video

Transmit H.261/H.263

Enable H.261/ H.263 at Maximum

Select to enable the use of the specified video format coding from the specific vPoint HD end point. In the box, type the maximum transmission rate at which the specific coding may be used.

For example, for H.263 the default maximum transmission rate is 256 kbps. At higher rates, the H.263 coding is not available.

Enable CIF

Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth (at least 128 kbps) is available.

All Emblaze-VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.

Enable QCIF — Select to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF).

QCIF may be chosen if the remote party has a system that does not support CIF format, or if the bandwidth is low.

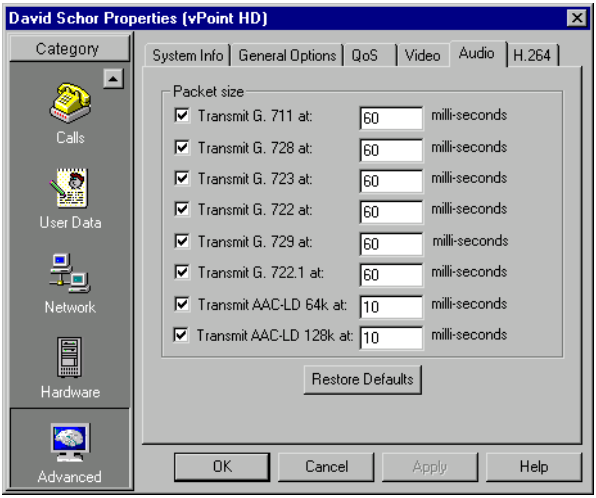
Video Transmit maximum packet size — Enter the maximum video packet size (in bytes) which the specified end point may transmit.

To reset the advanced Video default values, click **Restore Defaults**.

Advanced Audio

In the **Audio** tab, select the supported audio algorithms for transmitting audio from the specified end point. In addition, you can enter the audio transmit speed for all algorithms supported by the end point.

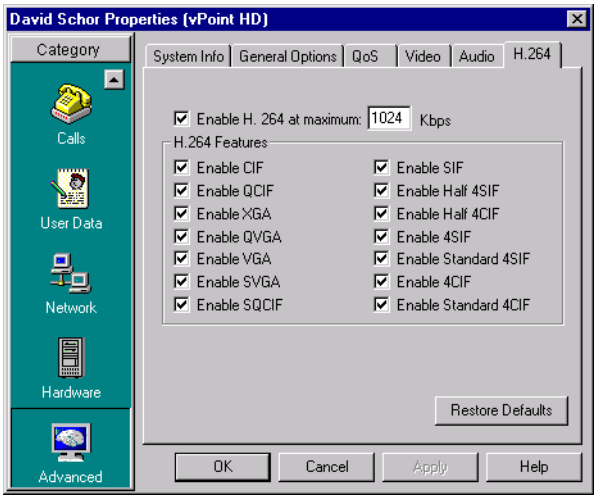
To reset the advanced Audio default values, click **Restore Defaults**.



vPoint HD End Point - Advanced Audio Properties

H.264

In the **H.264** tab, enable the use of the H.264 codec in this end point's video transmissions. You can enable and disable the use of any combination of the supported video formats in this end point's conferences.



vPoint HD End Point - H.264 Properties

Enable H.264 at Maximum — Select to enable the use of the H.264 codec by this end point up to the maximum bandwidth specified.

H.264 Features — Selected formats are activated for use by this end point. Deselect a feature to make it unavailable.

Restore Defaults — Click to return to the H.264 default selections.

B vPoint™ End Point Properties

From the MXM Administrator application, the administrator may view and control various properties of vPoint™ end points. vPoint is the videoconferencing application used by Emblaze-VCON's ViGO, and may also be used as a software-only application with various cameras.

For explanations about end point MXM Properties, see "Setting End Point MXM Properties" on page 91 to 106.

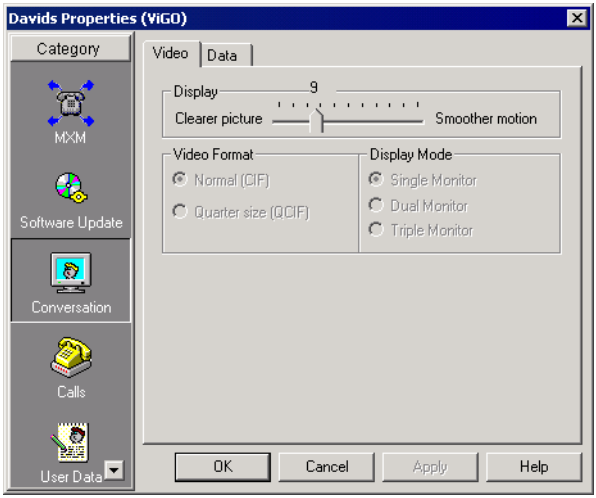
For explanations about end point Software Upgrade Properties, see "Node Software Upgrade Properties" on page 122 to 128.

B.1 Conversation Properties

The Conversation Properties dialog box may be used for viewing and controlling the Video and Data settings of vPoint end points.

Video

In the **Video** tab, you may control certain video features that improve the quality of the video transmission from the selected vPoint end point.



vPoint End Point - Video Properties

Display

Clearer Picture/ Smoother Motion

This control enables you to define the relationship between clear, sharp images and smooth uninterrupted motion during the video transmission. If the picture is clearer, the motion may be slower and more broken. If the motion is smoother, the picture may be less clear.

Drag the slider until you are satisfied with the image sharpness and the smoothness of motion. There are 30 possible settings on the slider – **1** represents the clearest picture but the most uneven motion; **30** represents the smoothest motion but the most blurry picture.

Video Format

The type of video format in which the current video meeting is broadcast. This setting affects the viewing quality for the remote party, and may only be changed during a call. The possible options are:

Normal (CIF)

Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.

All Emblaze-VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.

Quarter Size (QCIF)

Select to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF).

QCIF may be chosen if the remote party has a system that does not support CIF format, or if the bandwidth is low.

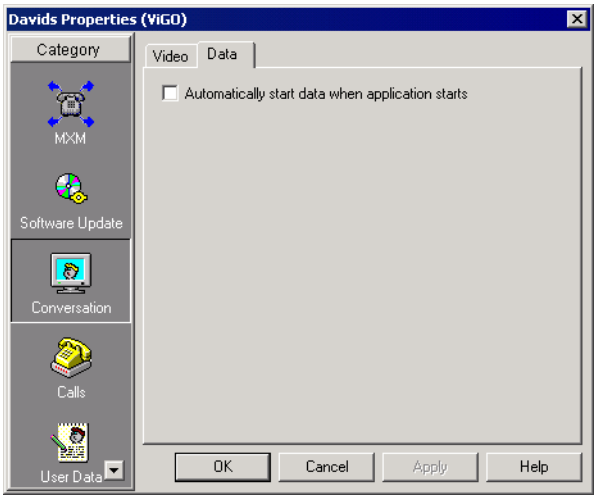
Display Mode

This setting is applicable if the end point is a MediaConnect 9000 system. The display mode determines how local video, remote video and software applications (such as vPoint) are displayed at this end point.

Single Monitor	Video and applications on the SVGA monitor only.
Dual Monitor	Video on the TV monitor, applications on the SVGA monitor.
Triple Monitor	Local video on one TV monitor, remote video on the second TV monitor, and applications on the SVGA monitor.

Data

In the **Data** tab, select **Automatically Start Data When Application Starts** to enable data receiving capability immediately AND to automatically enable it when vPoint starts again. In such a case, Microsoft® NetMeeting® runs minimized on the Windows Desktop and the end point user can use NetMeeting's data sharing features during the videoconferences.



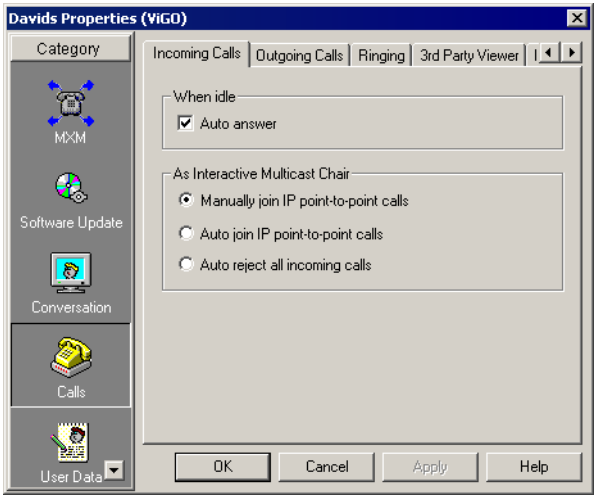
vPoint End Point - Data Properties

B.2 Calls Properties

The Calls Properties dialog box may be used for viewing and controlling incoming and outgoing call properties of vPoint end points.

Incoming Calls

In the **Incoming Calls** tab, customize how the vPoint end point indicates and accepts incoming calls.



vPoint End Point - Incoming Calls Properties

When Idle

Auto answer — Select to turn automatic acceptance of calls on. If the system is idle when a videoconferencing call arrives, the session starts automatically.

As Interactive Multicast Chair

If the selected user's system supports Emblaze-VCON's Interactive Multicast, it may sometimes be the Chair of multicast videoconferences. If another party tries to call it while it chairs a conference, that call may be accepted or rejected according to the selected option :

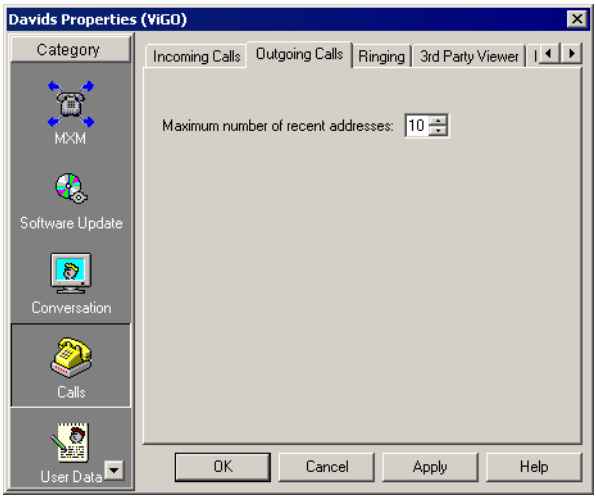
Manually join IP point-to-point calls — Enable the selected user to either join or reject callers to an ongoing Multicast conference.

Auto join IP point-to-point calls — Enable the selected user to automatically join callers to an ongoing Multicast conference.

Auto reject all incoming calls Enable the selected user to automatically reject incoming calls to an ongoing Multicast conference.

Outgoing Calls

In the **Outgoing Calls** tab, define properties for calls initiated by the selected vPoint end point.

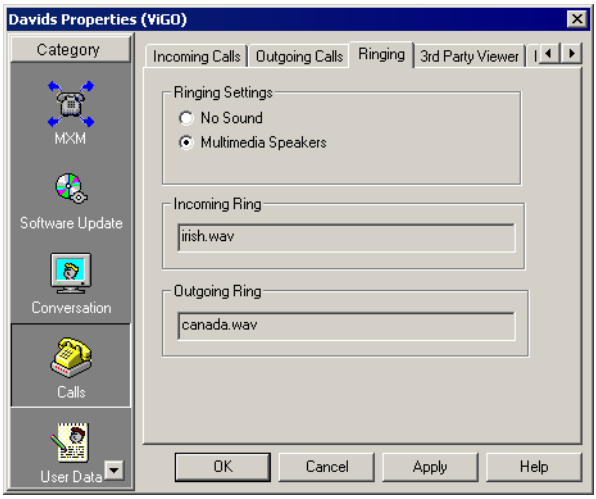


vPoint End Point - Outgoing Calls Properties

Maximum Number of Recent Addresses The maximum number of recently dialed addresses that can appear in the vPoint Manual Dialer's Call Log.

Ringing

In the **Ringing** tab, define the sounds used by the selected end point to indicate incoming and outgoing videoconference calls.



vPoint End Point - Ringing Properties

Ringing Settings

No Sound — Select to disable all audio ringing. Only the Incoming Call and Outgoing Call messages visually indicate calls.

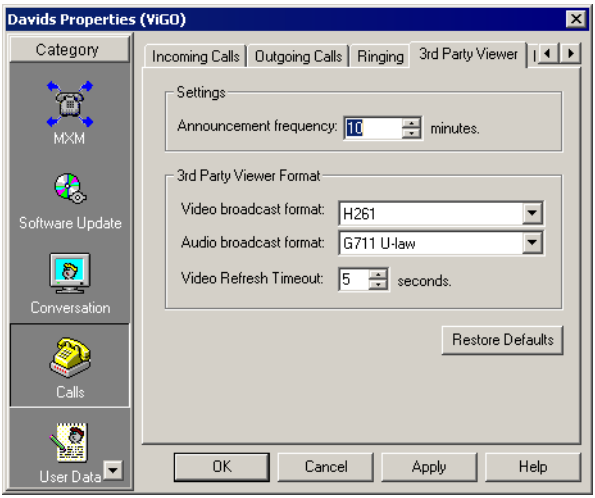
Multimedia Speakers — Select to enable ringing sounds to indicate calls.

Incoming Ring/ Outgoing Ring — Filenames of the sounds that indicate incoming and outgoing calls.

3rd Party Viewer

In the **3rd Party Viewer** tab, define the settings for transmission of an Interactive Multicast videoconference through third-party viewers.

CAUTION The default settings of this tab should be edited with caution.



vPoint End Point - 3rd Party Viewer Properties

Announcement Frequency The interval between announcements of Multicast sessions in the third-party viewer's schedule.

Video Broadcast Format The video coding standard that all parties viewing the Multicast sessions must be capable of using - H.261 and H.263. H.263 provides better video quality, especially at low bitrate transmissions.

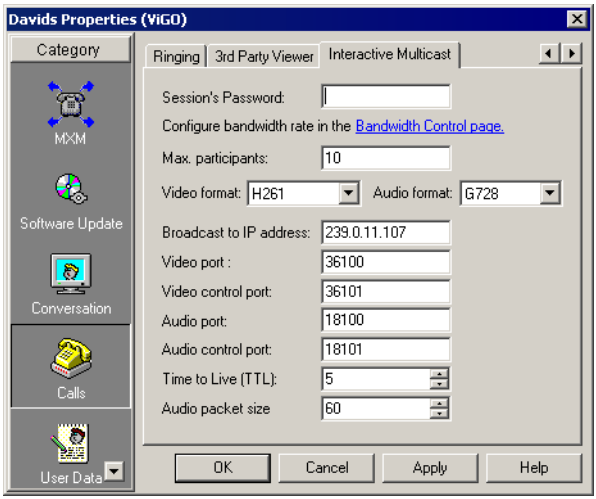
However, video systems that do not support H.263 will not be able to receive an H.263 broadcast.

Audio Broadcast Format The audio coding standard that all parties viewing the Multicast sessions must be capable of using.

G.711 U-law/ A-law	This standard gives the lowest quality results, but all third-party viewing systems will be able to receive the broadcast. Select **G.711 U-law** if you're in the U.S. or Japan, or **G.711 A-law** if you're in Europe. For other regions, consult with your local Emblaze-VCON technical support representative.
G.722	This standard gives the best quality. Select it if you know that the third-party viewing systems support it and if you think that the connection will be over high bandwidths.
G.728	This standard gives the best possible quality with the smallest possible bandwidth cost. Select this standard if you know that the third-party viewing systems support it and if you think that the connection will be over low bandwidths.
Video Refresh Timeout	The maximum number of seconds required until the video broadcast is synchronized for all viewers. If the refresh value is low, the quality is lowered. If the refresh value is high, it will take a longer time to see the video display when the viewers connect. Use the default setting as a guide.
Defaults	Return all options to the original preset third-party viewer settings.

Interactive Multicast

In the **Interactive Settings** tab, set the default configuration for this end point's Interactive Multicast broadcasts.



vPoint End Point - Interactive Multicast Properties

Session's Password

To restrict entry into the Interactive Multicast videoconferences that the end point initiates, define a security password. If you want to allow anyone who calls the end point to join the conference, leave this box blank.

The default Broadcasting settings are recommended for most Multicast conditions.

Configure Bandwidth Rate in the Bandwidth Control page

Click the link to jump to the MXM Properties - Bandwidth Control topic, where you can set the Default Bandwidth for multicast sessions.

Max. Participants

The maximum number of Participants allowed in a Multicast initiated and chaired by this end point.

Video Format

The video coding standard that all parties in the Multicast are capable of using - H.261 and H.263. H.263 provides better video quality, especially at low bitrate transmissions.

However, some video systems do not support H.263. If at least one Participant's system does not support H.263, or you are not sure, select H.261.

Audio Format

The audio standard that all parties in the Multicast are capable of using.

- **G.711 U-law/A-law**
  This standard gives the lowest quality results, but it must be selected if you want 3rd Party viewers to be able to join a multicast session. Select **G.711 U-law** if you're in the U.S. or Japan, or **G.711 A-law** if you're in Europe. For other regions, consult with your local Emblaze-VCON technical support representative.
- **G.722**
  This standard gives the best quality. Select it if you know that the remote parties support it and if you think that the connection will be over high bandwidths.
- **G.728**
  This standard gives the best possible quality with the smallest possible bandwidth cost. Select this standard if you know that the remote parties support it and if you think that the connection will be over low bandwidths.

If you select either G.728 or G.722, and a remote party's system does not support it, that party will not be able to participate in the session.

Broadcast IP Address

The destination IP address for the Interactive Multicast. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of **224.0.0.0** to **239.255.255.255**.

Video port

The ID of the port used for the video connection.

Video control port

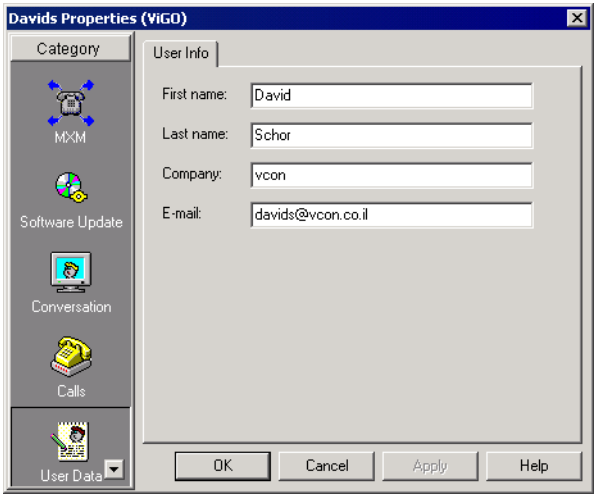
The ID of the port used for transferring control and synchronization information about the video transmission.

Time to Live	The maximum number of routers that the Session's packets may pass through.
Audio port	The ID of the port used for the audio connection.
Audio control port	The ID of the port used for transferring control and synchronization information about the audio transmission.
	Participants must use the same video, audio and control ports. Make sure that the ports you choose are available for every participant.
Defaults	Click to return to the original settings. These settings help you connect to the Interactive Multicast through the default ports and/or IP address that was defined automatically by your system.

B.3 User Data Properties

The User Info settings provide identification of the vPoint end point user. This includes the following information:

- First Name
- Company or organization
- Last Name
- E-mail address



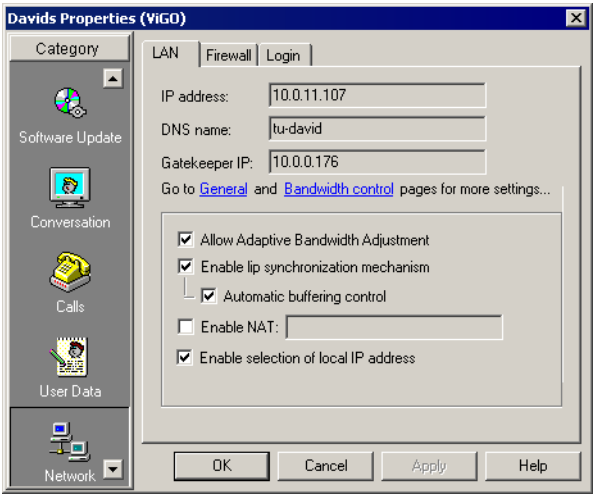
vPoint End Point - User Data Properties

B.4 Communication Properties

The Communication Properties dialog box may be used for viewing and controlling various network settings of vPoint end points.

LAN

The LAN Properties contain the vPoint end point's identification configuration on the local network. Additional capabilities are provided for holding videoconferences over the connected network.



vPoint End Point - LAN Properties

IP Address — The selected end point's IP address.

DNS Name — The selected computer's name if it resides in a network that employs a DNS server (*DNS* stands for Domain Naming System, which enables computers on a network to be referred to by name in addition to IP Addresses).

Gatekeeper IP — The IP address of the MXM or gatekeeper from which this end point receives gatekeeper services.

Go to General and Bandwidth Control Pages for More Settings — Click the General link to display the selected user's MXM General Properties (see "General" on page 91).

Click the Bandwidth Control link to display the selected user's MXM Bandwidth Control Properties (see "Bandwidth Control Properties" on page 95).

Allow Adaptive Bandwidth Adjustment

Enables videoconferences to precede at reduced bandwidth if the network is congested. Deselecting this option maintains a constant quality to the session, but it may cause network problems.

Enable Lip Synchronization Mechanization

Enables adjustment of the video and the audio if they are out of sync with each other.

Automatic Buffering Control

- Enables the system to automatically control the amount of buffering required to maintain the consistency of the video and audio transmission. For example, if video packets are delayed for 1 or 2 seconds, the system will automatically synchronize the transmission so that the delay does not disturb the visible video.
- Deselect this option only if the automatic buffering is not sufficient — for example, if the quality of the video meeting is poor or there is a noticeable delay.

Enable NAT

If your organization uses NAT (Network Address Translation) when communicating with parties in another LAN or WAN, type the external address for the selected user.

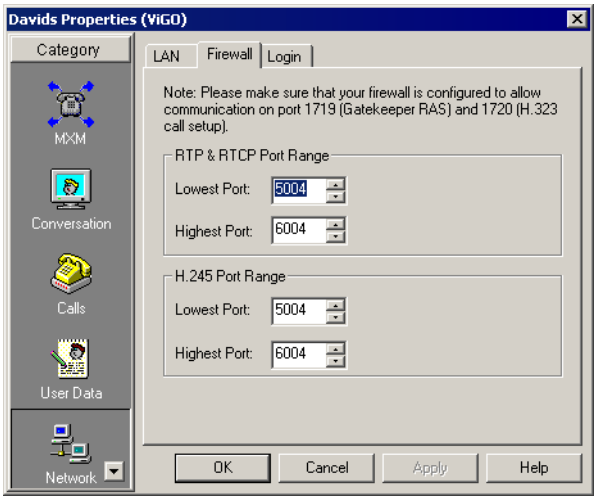
NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.

Enable Selection of Local IP Address

Enables the end point to receive its IP address configuration from the LAN's DHCP server. A DHCP server automatically assigns IP addresses to computers as they log on to the network, eliminating the need to assign IP addresses manually and locally.

Firewall

In the **Firewall** tab, enter the allocation of ports for communication through your organization's firewall.



vPoint End Point - Firewall Properties

RTP & RTCP Port Range

The MXM allocates a range of ports for video and audio during videoconferences.

This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

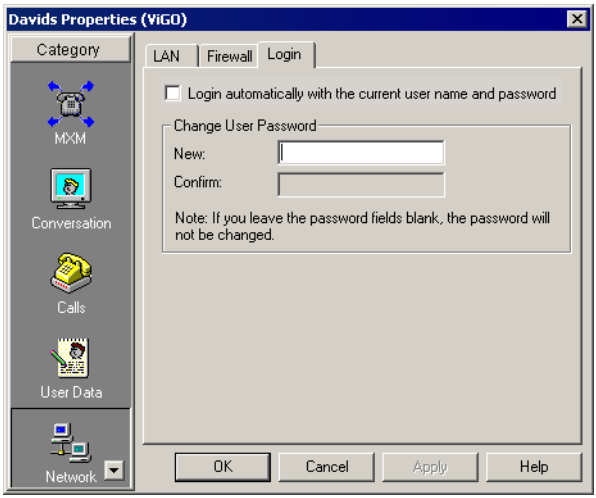
H.245 Port Range

The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences.

This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

Login

In the **Login** tab, define how the end point logs into an MXM.



vPoint End Point - Login Properties

Login Automatically with the Current User Name and Password	The end point automatically logs in to the MXM during vPoint's startup using the current User Name and Password. If this option is selected, the user does not have to enter login details during vPoint startup.

Change User Password

New	Password that replaces the current one.
Confirm	Confirmation of the new password.

If the Password boxes are blank, the current password remains valid.

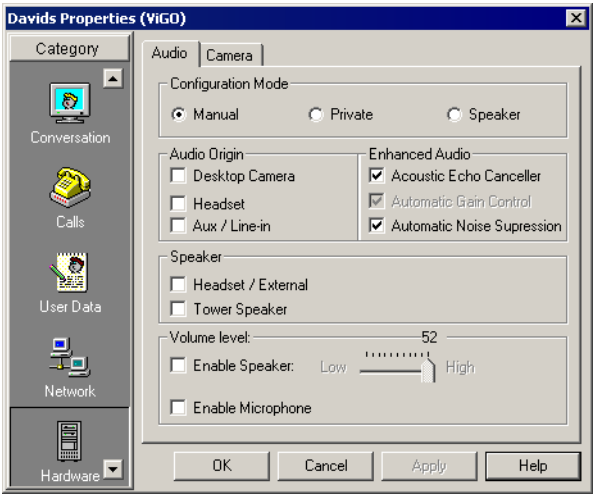
B.5 Hardware Properties

The Hardware Properties dialog box may be used for viewing and controlling various Audio and Camera settings of vPoint end points.

Audio

In the Audio Settings for ViGO, you can define the audio configuration to be used during videoconferences.

ViGO



vPoint Properties - Audio (ViGO)

Configuration Mode

Select a mode for manual or automatic audio settings.

Manual	Select to choose audio settings one by one. Select this option if the selected end point has a PTZ camera or other optional hardware.
Private	Select to automatically select settings for headset audio.
Speaker	Select to automatically select settings for tower audio (if connected) or speaker audio (if a tower is not connected).

Audio Origin

Active if Configuration Mode is **Manual**.

Select an available audio input source. The selected end point can speak or send audio through one, two, or all three possible sources.

Desktop Camera	Select to use the camera's built-in microphone.
Headset	Select to use the supplied headset.
Aux/Line In	Select to use a microphone that's connected to the Line Level Audio In connector on the ViGO rear panel. The source may be from a connected VCR or other external audio device.

Enhanced Audio

Acoustic Echo Canceller	Select to prevent the remote party from hearing themselves from their own speakers. This condition occurs if the speaker output is received by the local end point's microphone and sent back to the remote party.
Automatic Gain Control	Select to ensure that the remote parties hear the selected end point normally regardless of the speaker's distance from the microphone.
Automatic Noise Suppression	Select to mute surrounding noise. The result is that the remote parties only hear what the speaker says into the microphone.

Speaker

Active if Configuration Mode is **Manual**.

This end point emits audio through one or both of the following devices:

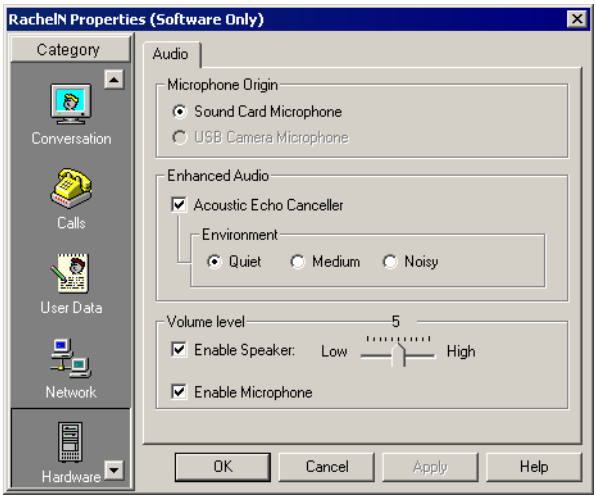
Tower Speaker	Select to emit audio from the ViGO tower's speaker.
Headset/ External	Select to emit audio from the headset or from another device connected to the Speaker connector on the ViGO's side panel.

Volume level

Enable Speaker	Select to control the volume of the selected end point's speaker. Drag the slider accordingly.
Enable Microphone	Select to control the volume through the selected end point's microphone.

Software Only

In the Audio Settings for the vPoint software-only application (not connected to ViGO), you can define the audio configuration to be used during videoconferences.



vPoint Properties - Audio (Software only)

Microphone Origin

Sound Card Microphone — Use a microphone that's connected to the Line Level Audio In connector on the installed videoconferencing card.

USB Camera Microphone — Use the camera's built-in microphone.

Enhanced Audio

Acoustic Echo Canceller (AEC) — Select to cancel the echo created when your microphone picks up audio from your speakers.

AEC is not available if you are using a **USB Camera Microphone**.

Environment — Select **Quiet**, **Medium**, or **Noisy**, as applicable, according to your surroundings. This setting controls the automatic adjustment to compensate for surrounding noise levels, so that they don't affect the outgoing audio.

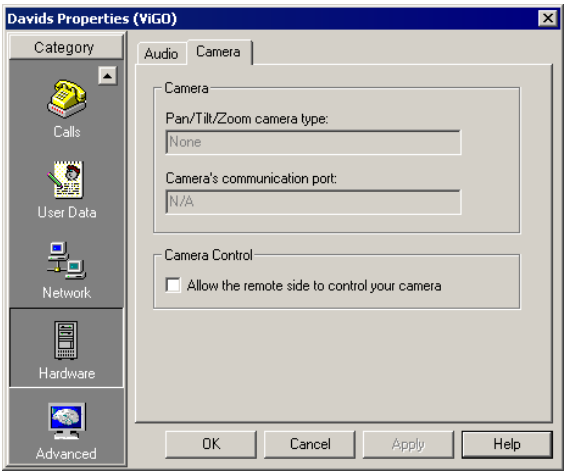
Volume level

Enable Speaker — Select to control the volume of the selected end point's speaker. Drag the slider accordingly.

Enable Microphone — Select to control the volume through the selected end point's microphone.

Camera

The Pan/ Tilt /Zoom Camera properties are applicable if a Pan/Tilt/Zoom-type (PTZ) camera is connected to the selected system. If a PTZ camera is not used, **None** appears as the PTZ camera type in the dialog box's top list and no communication port is required.



vPoint Properties - Camera

Pan/Tilt/Zoom camera type — The manufacturer and/or model of the PTZ camera.

Camera's communication port — The name of the computer port to which the camera is connected.

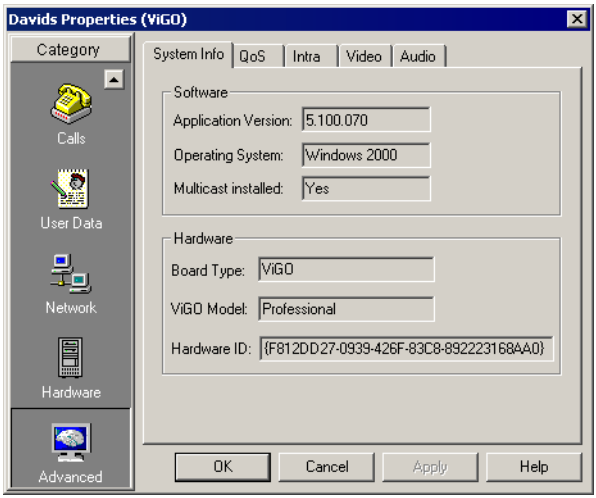
Allow the remote side to control camera settings — Select to permit a remote party in a video meeting to control the positioning of the selected user's PTZ camera. If a PTZ camera is not used, this option is not relevant.

B.6 Advanced Properties

The Advanced Properties dialog box may be used for viewing end point system information and controlling various QoS, Intras, advanced Video, advanced Data, and advanced Audio settings of vPoint end points.

System Info

The **System Info** tab displays information about the Emblaze-VCON videoconferencing system that's installed in the selected end point. If you contact Emblaze-VCON Technical Support (see "Emblaze-VCON Technical Support" on page vi before the Table of Contents) about a problem associated with this end point, include this information with your request.



vPoint Properties - System Information

Software

Application Version	Version number of the vPoint application running on the end point's computer.
Operating System	Operating system that's installed on the end point's computer.
Multicast installed	Indicates if the end point's videoconferencing system includes Emblaze-VCON's Interactive Multicast feature.

Hardware

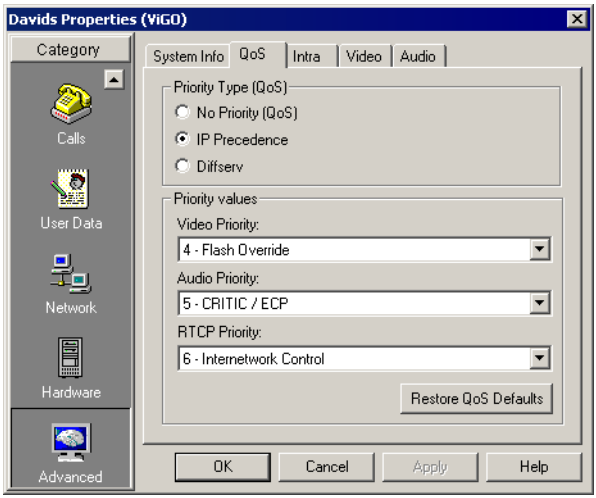
Board Type Videoconferencing system installed in the end point's computer.

ViGO Model Model name of the end point's ViGO (if applicable).

Hardware ID Unique identification number for the videoconferencing card's installation. This number is for Emblaze-VCON Technical Support use.

QoS

The **QoS** tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the specified vPoint end point.



vPoint Properties - QoS (Default Settings)

Set QoS properties as follows:

Priority Type (QoS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

No Priority Network transfers packets using normal Best-effort (or Routine) packet transmission.

IP Precedence Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.

Diffserv — Network transfers packets according to specific needs of the sending application.

Priority Values

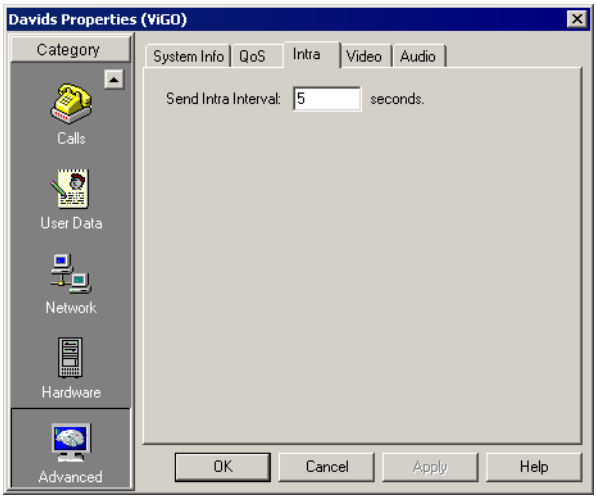
Video, Audio and RTCP Priority — For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see Appendix D, "QoS Priority Values".

To reset the Priority default values, click **Restore QoS Defaults**.

Intras

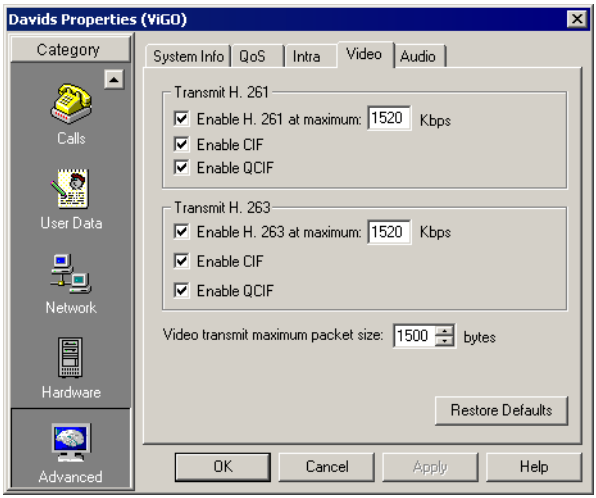
During videoconferences, vPoint end points send periodic intras (full video frames) in order to synchronize the video display at the receiving party. In the Send Intra Interval box, type the length of the interval (in seconds) between intra transmissions.



vPoint Properties - Intras

Advanced Video

The Advanced **Video** tab permits you to enable usage of H.261 and H.263 for video transmission and to control the bandwidth thresholds for switching between the two standards, if applicable.



vPoint Properties - Advanced Video

Transmit H.261/H.263

Enable H.261/ H.263 at Maximum

Select to enable the use of the specified video format coding from the specific vPoint end point. In the box, type the maximum transmission rate at which the specific coding may be used.

For example, for H.263 the default maximum transmission rate is 256 kbps. At higher rates, the H.263 coding is not available.

Enable CIF

Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.

All Emblaze-VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.

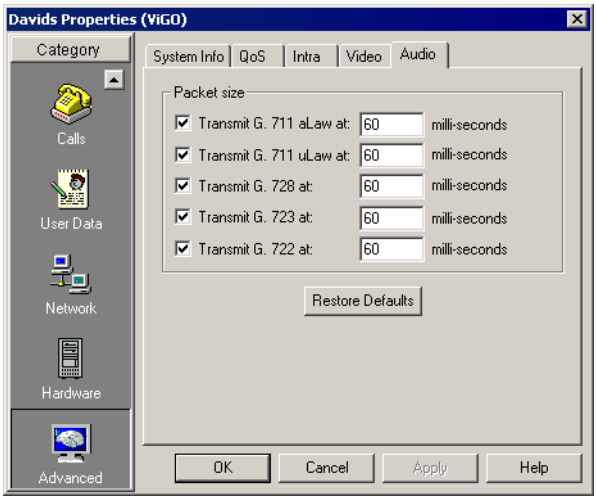
Enable QCIF	Select to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF). QCIF may be chosen if the remote party has a system that does not support CIF format, or if the bandwidth is low.
Video Transmit maximum packet size	Enter the maximum video packet size (in bytes) which the specified end point may transmit.

To reset the advanced Video default values, click **Restore Defaults**.

Advanced Audio

In the **Audio** tab, select the supported audio algorithms for transmitting audio from the specified end point. In addition, you can enter the audio transmit speed for all algorithms supported by the end point.

To reset the advanced Audio default values, click **Restore Defaults**.



vPoint Properties - Advanced Audio

C HD3000 End Point Properties

From the MXM Administrator application, the administrator may view and control various properties of HD3000 end points. In the HD3000 Properties dialog box, the properties are divided into various categories:

MXM	Properties defining how the HD3000 operates as parts of the MXM videoconferencing network (see "Setting End Point MXM Properties" on page 91).
Network	LAN, Streaming, Firewall, H.323, QoS
Video	Dual Monitor, Far End Camera Control, Intra Interval
Audio	Audio Input, VCR Audio Mix, Automatic Echo Cancellation, Microphone Gain Level
Options	General, Calls, MCU Calls, Monitor, Security, Version, Upgrade

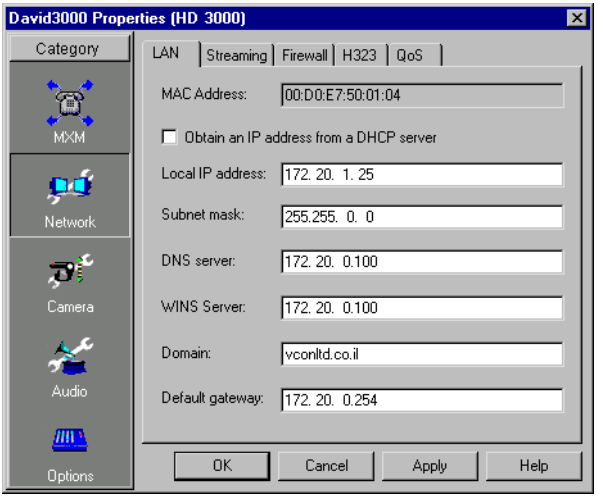
Properties cannot be changed while the HD3000 is engaged in a videoconference.

C.1 Network Configuration

This section explains how to set up the HD3000's network and connections configuration. Network options may be edited at any time.

LAN Connection and Registration

The **LAN** tab includes the HD3000's address and information about its connection to the LAN (Local Area Network).



HD3000 End Point - LAN Properties

MAC Address The unique Media Access Control (MAC) address of the HD3000 device.

Obtain an IP Address from a DHCP server Select to enable the HD3000 to receive its network configuration from the LAN's DHCP server and enter it automatically in the **LAN** tab.

If this option is not selected, you must define the LAN properties manually.

Local IP Address IP address of the HD3000.

If the HD3000 receives an address automatically, it is a temporary address which is liable to be changed when the network's users' IP addresses are updated periodically.

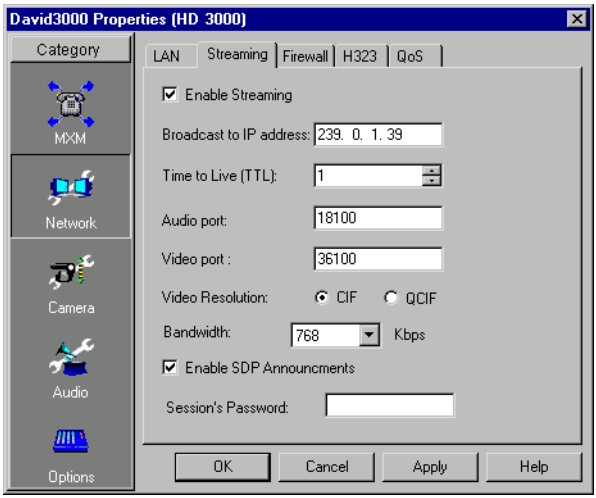
If you manually enter an IP address here, the address remains permanently.

Subnet Mask Your company's subnet mask.

DNS Server & WINS Server	IP Addresses of the DNS server and the WINS server. Registering with these servers enables the HD3000 to translate names to IP addresses.
Domain	DNS domain name of your company (for example, **yourcompany.com**).
Default Gateway	IP address of the network's Gateway router. The gateway helps the HD3000 send and receive calls between subnets.

Streaming

In the **Streaming** tab, define the configuration for transmitting streaming media from the HD3000.



HD3000 End Point - Streaming Properties

Enable Streaming Select this option to enable the transmission of multimedia streaming from this HD3000.

Broadcast to IP Address The destination IP address for a multicast streaming broadcast. The HD3000 defines this address internally. This address must be a class D address in the range of **224.0.0.0** to **239.255.255.255**.

The sender transmits the streams to this address and viewers receive the stream from this address.

Time to Live (TTL) The maximum number of routers through which the stream may pass.

Audio Port The ID of the port used for the audio connection.

Video Port The ID of the port used for the video connection.

Video Resolution

- Select **CIF** to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.
- Select **QCIF** to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF). Use QCIF if the viewers' systems do not support CIF format, or if you transmit over low bandwidth.

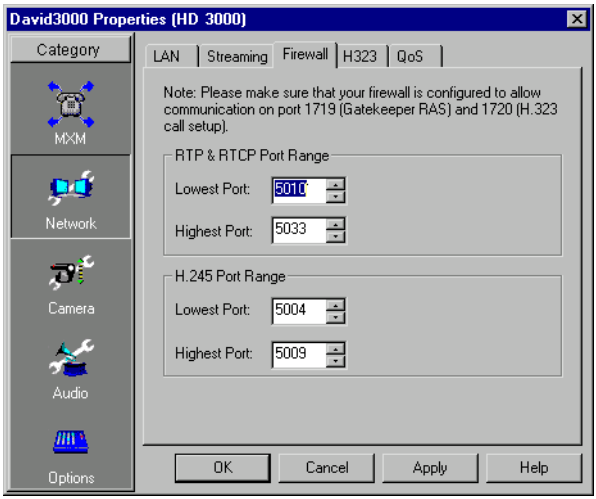
Bandwidth Click the right arrow to select the maximum bandwidth for the streaming media.

Enable SDP Announcements Select to send announcements of your streaming session over the network to client Viewer Programs other than HD3000 (such as Emblaze-VCON's Broadcast Viewer).

Session's Password To restrict access to stream viewing, enter a password. When they attempt to view the stream, users will need to type this password.

Firewall

In the **Firewall** tab, enter the allocation of ports for communication through your organization's firewall.



HD3000 End Point - Firewall Properties

RTP & RTCP Port Range

The MXM allocates a range of ports for video and audio during videoconferences.

This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

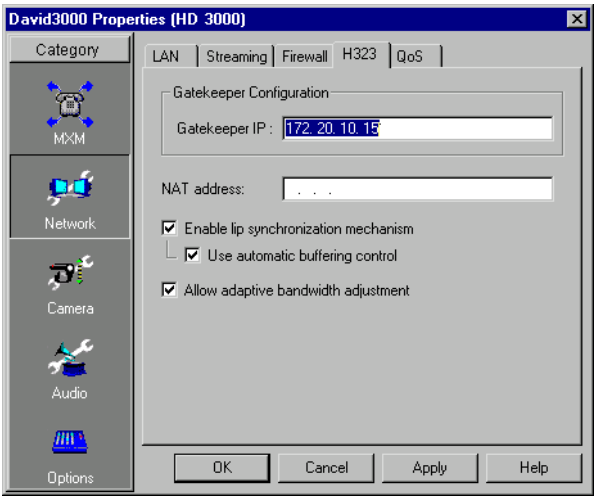
H.245 Port Range

The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences.

This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

H.323 Management

In the **H.323** tab, you can define how the HD3000 operates within a managed H.323 videoconferencing network.



HD3000 End Point - H.323 Properties

Gatekeeper IP Enter the IP address of the gatekeeper which manages the HD3000. This may be either the MXM's gatekeeper or another one used by your organization.

If the HD3000 is logged in to a non-Emblaze-VCON gatekeeper, the HD3000's status in the Main View is **Logged In to Management Server**.

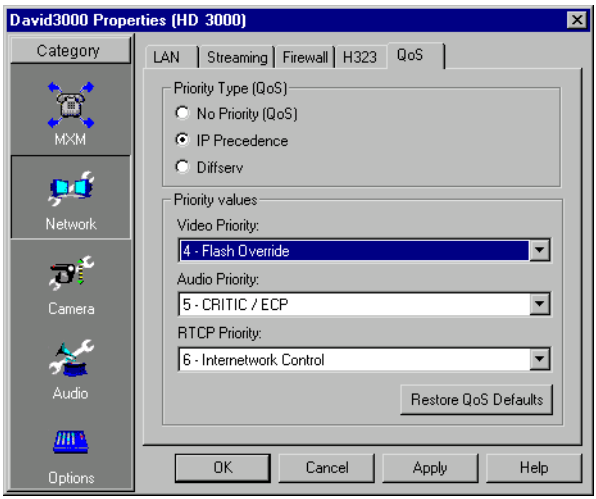
NAT Address If your organization uses NAT (Network Address Translation) to protect its network, type the external address for your computer.

NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.

Enable Lip Synchronization Mechanism	Select this option to synchronize the audio and video of a LAN conference.
Automatic Buffering Control	Buffer Control optimizes the transmission of the video for the available dynamic bandwidth. If network conditions require, the system holds back frame transmission before transmitting, in order to attain smooth playback and avoid "jumping". Select this option to make the buffer control automatic. Deselect it to make it adjustable during LAN conversations.
Allow Adaptive Bandwidth Adjustment	Enables videoconferences to precede at reduced bandwidth if the network is congested. Deselecting this option maintains a constant bandwidth during the session, but it may cause network problems.

QoS

The **QoS** tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the HD3000.



HD3000 End Point - QoS Properties

Priority Type (QoS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

No Priority	Network transfers packets using normal Best-effort (or Routine) packet transmission.
IP Precedence	Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.
Diffserv	Network transfers packets according to specific needs of the sending application.

Priority Values

Video Priority
Audio Priority
RTCP Priority

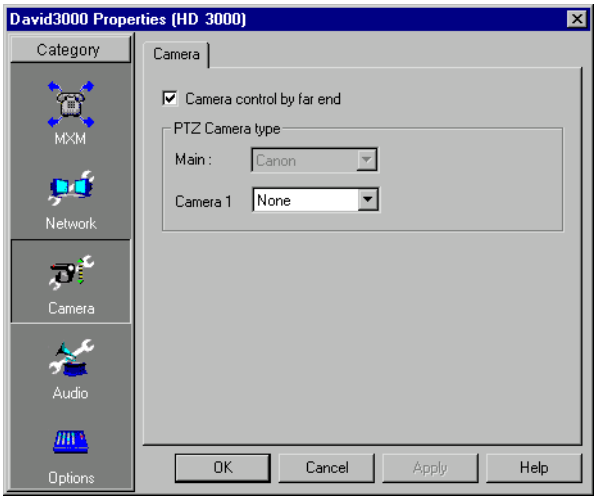
For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see Appendix F, "QoS Priority Values."

To reset the Priority default values, click **Restore QoS Defaults**.

C.2 Camera Properties

In the **Camera** tab, define the HD3000's camera configuration.



HD3000 End Point - Camera Properties

Camera Control by Far End Far End Camera Control (FECC) enables the remote party to control the local party's camera, so that they see views that are convenient for them. FECC provides control over the pan/tilt/zoom positioning and the adjustment of brightness, color, contrast and hue.

PTZ Camera Type

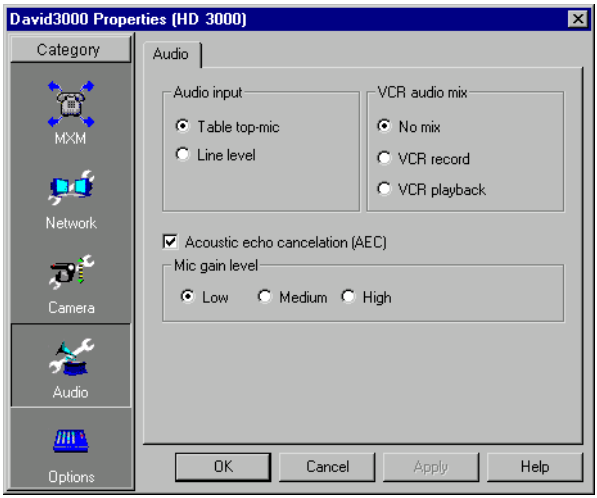
If at least one Pan/Tilt/Zoom (PTZ) camera is used by the HD3000, the camera's model is defined here.

Main In HD3000, the main camera is built-in.

Camera 1 If a second camera is connected, choose its type.

C.3 Audio Properties

In the **Audio** tab, you can select and activate various audio properties in the selected HD3000 end point.



HD3000 End Point - Audio Properties

Audio input

Tabletop Mic — To use a tabletop microphone or other audio source connected to the HD2000's **MIC** connector.

Line Level — To use a microphone or other audio source (such as VCR, mixer, etc.) connected to the HD2000's VCR AUD connector.

VCR audio mix

Mixing options determine how the audio from a DVD or VCR connected to the HD3000 is mixed and sent to the remote party or recorded to a VCR cassette. Select the appropriate VCR Audio Mix option:

No Mix — Both parties hear each other's audio only.

VCR Record — Both parties hear each other's audio while a VCR records the audio from both of them.

VCR Playback — Both parties hear each other's audio and records the audio from the remote party.

Other settings

Acoustic Echo Cancellation (AEC)

When the microphone picks up audio from your speakers, an echo is created. Acoustic Echo Cancellation (AEC) suppresses this effect. Select this option to prevent the remote party from hearing themselves from their own speakers.

You should disable AEC only if audio input comes through a Line Level connection from a playback device that does not capture sound from the conference room.

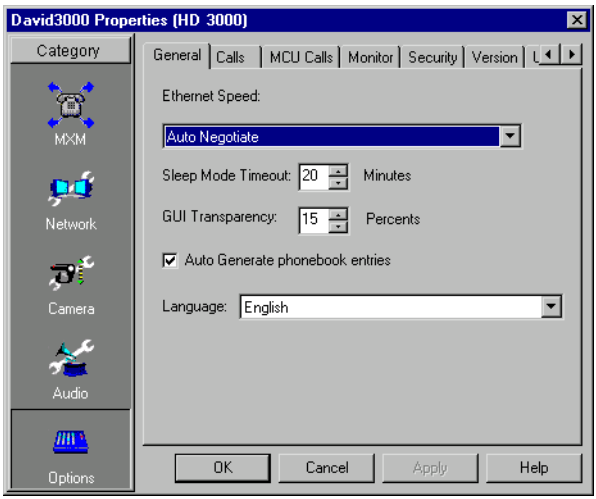
Microphone Gain Level

The gain level is the boost in signalling power when the audio signal is increased. Depending on your microphone or other audio input, adjust the gain to a suitable level.

C.4 Options

General Options

The **General** Options tab contains several options for defining how the selected HD3000 operates.

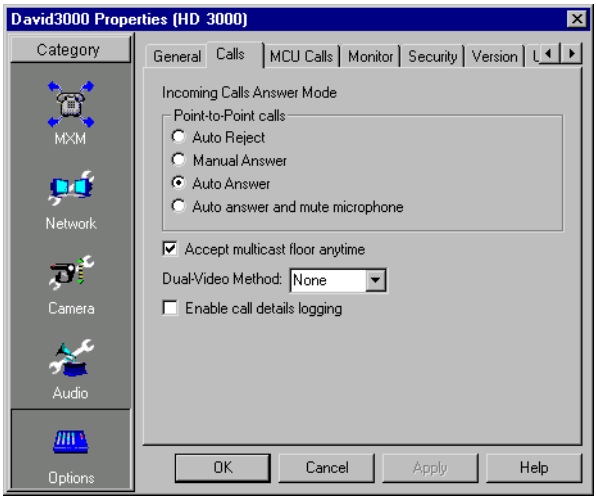


HD3000 End Point - General Options

Ethernet Speed	Define the speed of the network to which the HD3000 is connected. The HD3000 supports 10 MB and 100 MB half-duplex and full-duplex networks. Select **Auto-Negotiate** to allow the HD3000 to determine the common set of networking options supported between it and the remote parties in a conference.
Sleep Mode Timeout	Choose the amount of time that passes before the HD3000 hides the display.
GUI Transparency	The amount of transparency determines if you will see the video behind the HD3000's dialog boxes and menus. **0** percent transparency hides the video behind the interface elements. **5** to **60** percent shows the video behind the interface at various visibility levels.
Auto Generate Phonebook Entries	Select to add remote parties to the HD3000's Phone Book after a call ends.
Language	Select the language of the HD3000's interface. All menus and options appear in the selected language on the end point's monitor.

Calls

In the **Calls** tab, customize how the HD3000 end point indicates and accepts incoming calls.



HD3000 End Point - Calls Properties

Point to Point

Point-to-point conferences are calls between two end points.

Auto Reject — Select to automatically reject all incoming point-to-point calls (*Do-not-disturb*).

Manual Answer — Select to make the user accept or reject incoming calls.

Auto Answer — Select to accept all incoming calls automatically (unless the end point is already engaged in a call).

Auto and Mute Microphone — Select to automatically accept point-to-point incoming calls but to mute the outgoing audio at the beginning of the conference. After the conference begins, you may turn the audio back on.

Auto Accept Multicast Floor — During interactive multicast conferences, the *Floor* (one user's video and audio being broadcast to all participants at the same time) may be granted to you by the conference's organizer (*Chair*).

Select this option to enable the selected end point to automatically accept the floor when the Chair grants it.

Dual-Video Method

Define the method for transmitting dual video streams from this end point.

- ❑ Choose **None** to block all dual video transmission.
- ❑ Choose **DuoVideo** to allow dual video transmission from this end point using DuoVideo technology.
- ❑ Choose **H.239** to allow dual video transmission if the conference's end points support H.239.

Enable Call Details Logging

Select to enable the creation of call logs.

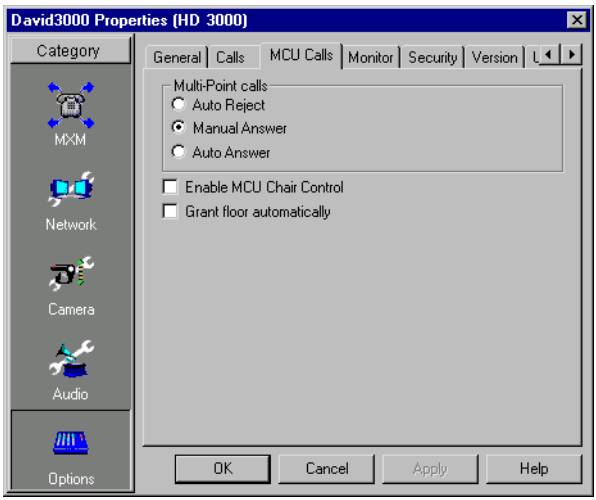
The Call Log enables your company or organization to keep a record of conferences that your HD3000 both dials and receives. The HD3000 generates a Call Details Report (CDR) which is accessible from the HD Web Management program. You can analyze this information in detail for departmental accounting or network planning purposes.

The CDR provides call duration, remote party identification, call direction, video and audio codecs and formats, and more.

MCU Calls

Multipoint conferences include more than two end points. They are managed by the HD3000's embedded MCU.

In the **MCU Calls** tab, customize how the HD3000 end point accepts and manages multipoint calls using its embedded MCU.



HD3000 End Point - MCU Calls Properties

Multipoint

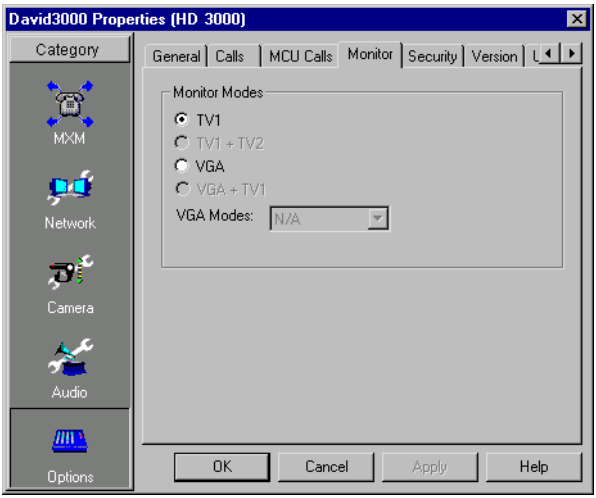
Multipoint conferences include more than two end points. They are managed by the HD3000's embedded MCU.

Auto Reject	Select to automatically reject all incoming multipoint calls, if the system is already engaged in another call.
Manual Answer	Select to answer multipoint calls by manually accepting an incoming call request.
Auto Answer	Select to answer multipoint calls automatically.
Enable MCU Chair Control	Select to enable this end point to apply Chair Control functions (through the end point's embedded MCU).
Grant Floor Automatically	Select to enable this end point to grant the floor automatically to every floor request during an MCU conference.

Monitor

To view video and HD3000 menus and dialog boxes, you must define the monitor configuration. If this configuration is not defined correctly, your monitor(s) will be blank.

The HD3000 supports the use of two monitors to display video and other media during conferences. Select this option only if two TV monitors are connected.



HD3000 End Point - Monitor Properties

TV1	Single TV monitor configuration, displaying video and the application interface.
TV1 + TV2	2 TV monitors - An S-Video TV monitor displays local video and the application interface, and a Composite TV monitor displays remote video.
VGA	Single VGA monitor configuration, displaying video and the application interface.
VGA + TV1	1 VGA-type monitor and 1 TV monitor - A VGA-type monitor displays local video and the application interface, and an S-Video TV monitor displays remote video.

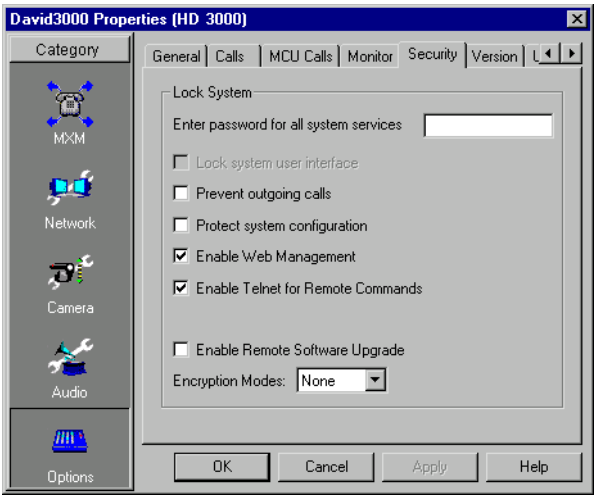
VGA Modes

Choose the resolution for the Main monitor of the configration.

- ❑ If your configuration uses only TV monitor(s), choose the monitor type connected to the TV1 connector on the rear panel.
- ❑ If your configuration includes a VGA-type monitor, choose the monitor type connected to the XVGA connector on the rear panel.

Security

The **Security** tab contains the options and properties for setting up a security configuration for the HD3000.



HD3000 End Point - Security Properties

Enter password for all system services

This password prevents unauthorized users from changing the system configuration, initiating videoconferences, and/or accepting videoconference calls. The password is also required for accessing remote configuration through the HD2000's Web-based Manager.

If you forget the password, contact your local Emblaze-VCON distributor's technical support.

This setting does not affect management through the Property dialog box in the MXM Administrator.

Lock System User Interface

Select to prevent access to HD3000 functions and menus by unauthorized users. Videoconferencing users will be unable to dial or receive calls, or change any configuration properties. A password is required to gain access to videoconferencing and configuration settings.

Prevent Outgoing Calls

Select to prevent users from initiating calls without authorization. The only way to initiate a call "from" this HD3000 is through the MXM (see "Initiating Videoconferences From the MXM Administrator" on page 107).

Protect System Configuration

Select to prevent unauthorized changes to the system configuration. The system's configuration is then disabled to videoconferencing users.

Enable Web Management

Select to enable remote access to the HD3000 through its web-based remote management site.

Enable Telnet for Remote Commands

Select to enable Telnet access for programming the HD3000 software, using the HDK API. This access is intended for software integrators.

Enable Remote Software Upgrade

Select this option to enable the transfer of upgrades and patches to the HD3000 unit.

1. For upgrading the HD3000 software through the HD Upgrade Utility.
2. For software integrators to send software patches, upgrades, and modifications to the HD3000.

Encryption Modes

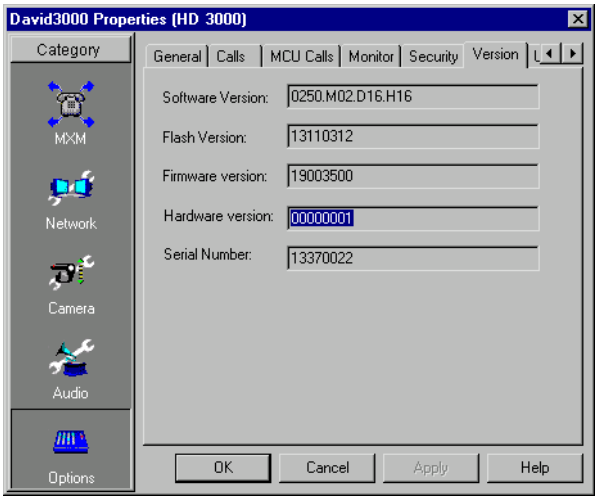
Choose the mode of encryption for this HD3000's conferences.

- ❑ Choose **None** to allow unsecured calls.
- ❑ **Auto** enables the HD3000 to encrypt a call if the remote side has also enabled encryption. If the remote side has not enabled encryption, an outgoing call will be unsecured.
- ❑ **AES** (Advanced Encryption Standard) is a standard encoding method for encrypting data transmissions in commercial and government sectors of the USA and its use is growing worldwide.

  Select this option to encrypt all of this HD3000's calls. If the remote side has not also enabled encryption, the call attempt will be unsuccessful.

Version

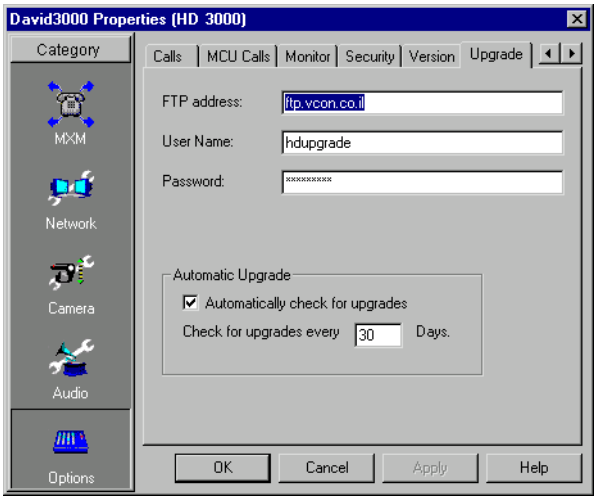
The **Version** tab displays hardware and software version information for the HD3000. If you contact Emblaze-VCON's Technical Support about this unit, provide the information on this page.



HD3000 End Point - Version Information

Upgrade

In the **Upgrade** tab, define the login information and enable checking for upgrade availability.



HD3000 End Point - Upgrade Properties

FTP Address	FTP site from where to download the upgrades when they're available.
User Name/ Password	Login information required to access the upgrade site.
Automatically Check for Upgrades	Select to enable the HD3000 to check the FTP site for a new software version whenever the system restarts.
Check for Upgrades Every ___ Days	This setting commands the HD3000 to check for the upgrade after a specific period, IF the system has not restarted during the interim. Enter the number of days in this period.

D HD5000 End Point Properties

From the MXM Administrator application, the administrator may view and control various properties of HD5000 end points.

For explanations about end point MXM Properties, see "Setting End Point MXM Properties" on page 91 to 106.

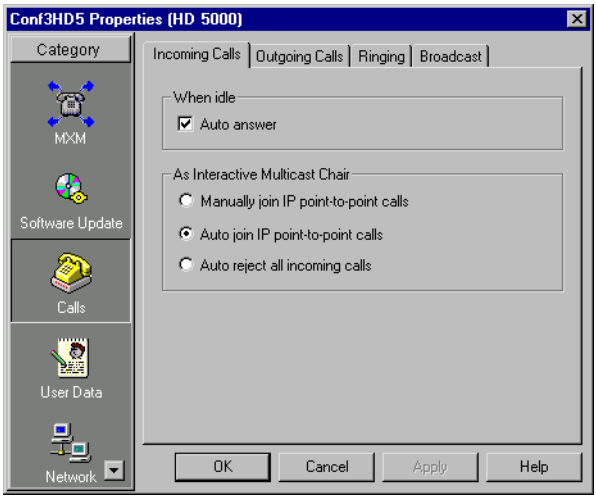
For explanations about end point Software Upgrade Properties, see "Node Software Upgrade Properties" on page 122 to 128.

D.1 Calls Properties

The Calls Properties dialog box may be used for viewing and controlling incoming and outgoing call properties of HD5000 end points.

Incoming Calls

In the **Incoming Calls** tab, customize how the HD5000 end point indicates and accepts incoming calls.



HD5000 End Point - Incoming Calls Properties

When Idle

Auto answer Select to turn automatic acceptance of calls on. If the system is idle when a videoconferencing call arrives, the session starts automatically.

As Interactive Multicast Chair

If the selected user's system supports Emblaze-VCON's Interactive Broadcast, it may sometimes be the Chair of broadcast conferences. If another party tries to call it while it chairs a broadcast, that call may be accepted or rejected according to the selected option :

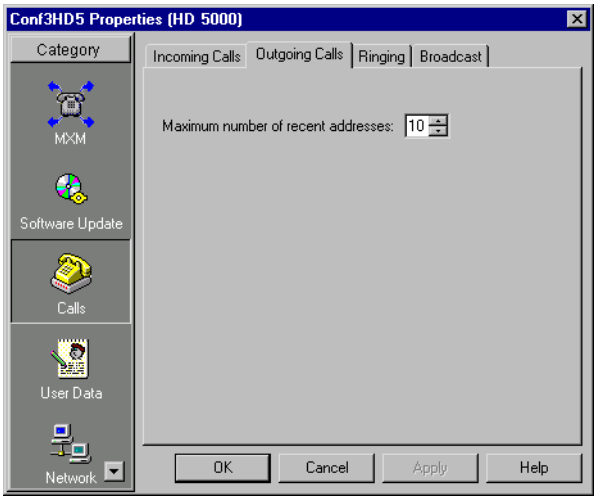
Manually join IP point-to-point calls Enable the selected user to either join or reject callers to an ongoing Broadcast conference.

Auto join IP point-to-point calls Enable the selected user to automatically join callers to an ongoing Broadcast conference.

Auto reject all incoming calls Enable the selected user to automatically reject incoming calls to an ongoing Broadcast conference.

Outgoing Calls

In the **Outgoing Calls** tab, define properties for calls initiated by the selected HD5000 end point.

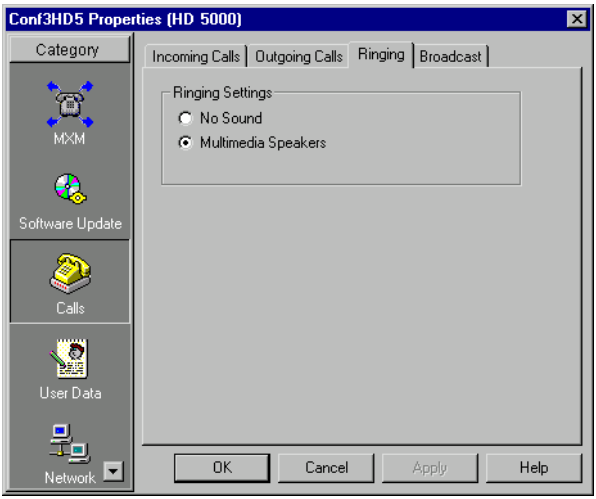


HD5000 End Point - Outgoing Calls Properties

Maximum Number of Recent Addresses — The maximum number of recently dialed addresses that can appear in the HD5000 Manual Dialer.

Ringing

In the **Ringing** tab, define the sounds used by the selected end point to indicate incoming and outgoing videoconference calls.



HD5000 End Point - Ringing Properties

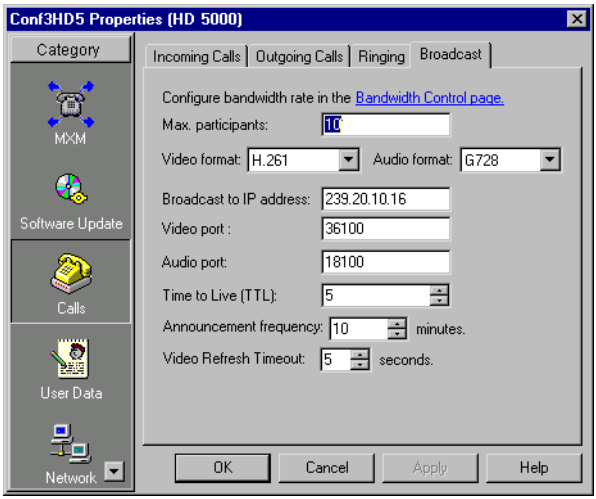
Ringing Settings

No Sound — Select to disable all audio ringing. Only the Incoming Call and Outgoing Call messages visually indicate calls.

Multimedia Speakers — Select to enable ringing sounds to indicate calls.

Broadcast

In the **Broadcast** tab, set the default configuration for this end point's Interactive Broadcasts.



HD5000 End Point - Broadcast Properties

The default Broadcasting settings are recommended for most Broadcasting conditions.

Configure Bandwidth Rate in the Bandwidth Control page

Click the link to jump to the MXM Properties - Bandwidth Control dialog box, where you can set the Default Bandwidth for broadcast sessions.

Max. Participants

The maximum number of Participants allowed in a Broadcast initiated and chaired by this end point.

Video Format

The video coding standard that all parties in the Broadcast are capable of using - H.264, H.261 and H.263. H.264 provides much greater compression and sharper quality, while using less bandwidth, than its predecessor standards.

However, some video systems do not support H.264. If at least one Participant's system does not support H.264, or you are not sure, select H.261 or H.263.

Audio Format The audio standard that all parties in the Broadcast are capable of using.

- **G.711 U-law/A-law**
  This standard gives the lowest quality results, but it must be selected if you want broadcast viewers to be able to join a Broadcast session. Select **G.711 U-law** if you're in the U.S. or Japan, or **G.711 A-law** if you're in Europe. For other regions, consult with your local Emblaze-VCON technical support representative.
- **G.722**
  This standard gives the best quality. Select it if you know that the remote parties support it and if you think that the connection will be over high bandwidths.
- **G.728**
  This standard gives the best possible quality with the smallest possible bandwidth cost. Select this standard if you know that the remote parties support it and that the connection will be over low bandwidths.

If you select either G.728 or G.722, and a remote party's system does not support it, that party will not be able to participate in the session.

Broadcast to IP Address The destination IP address for the Broadcast. All participants in the session transmit and receive from this common IP address. This address must be a class D address in the range of **224.0.0.0** to **239.255.255.255**.

Video port The ID of the port used for the video connection.

Audio port The ID of the port used for the audio connection.

Participants must use the same video and audio ports. Make sure that the ports you choose are available for every participant.

Time to Live (TTL) The maximum number of routers that the session's packets may pass through.

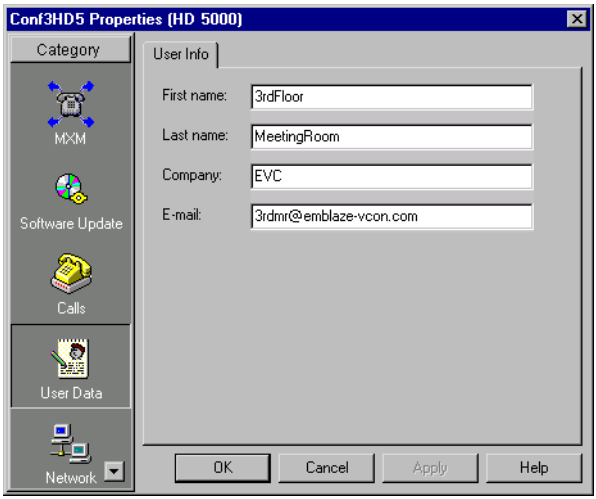
Announcement Frequency The interval between announcements of Broadcast sessions in the third-party viewer's schedule.

Video Refresh Timeout The maximum number of seconds required until the video broadcast is synchronized for all viewers. If the refresh value is low, the quality is lowered. If the refresh value is high, it will take a longer time to see the video display when the viewers connect. Use the default setting as a guide.

D.2 User Data Properties

The **User Info** settings provide identification of the HD5000 end point. This includes the following information:

- First Name
- Last Name
- Company or organization
- E-mail address



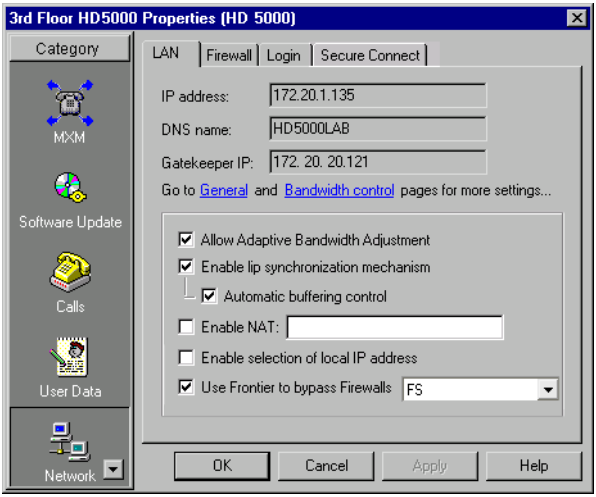
HD5000 End Point - User Info Properties

D.3 Network Properties

The Network Properties dialog box may be used for viewing and controlling various network settings of HD5000 end points.

LAN

The **LAN** tab contain the HD5000 end point's identification configuration on the local network. Additional capabilities are provided for holding videoconferences over the connected network.



HD5000 End Point - LAN Properties

IP Address — The selected end point's IP address.

DNS Name — The selected computer's name if it resides in a network that employs a DNS server (*DNS* stands for Domain Naming System, which enables computers on a network to be referred to by name in addition to IP Addresses).

Gatekeeper IP — The IP address of the MXM or gatekeeper from which this end point receives gatekeeper services.

Go to General and Bandwidth Control Pages for More Settings — Click the General link to display the selected user's MXM General Properties (see "General" on page 91).

Click the Bandwidth Control link to display the selected user's MXM Bandwidth Control Properties (see "Bandwidth Control Properties" on page 95).

Allow Adaptive Bandwidth Adjustment

Enables videoconferences to precede at reduced bandwidth if the network is congested. Deselecting this option maintains a constant quality to the session, but it may cause network problems.

Enable Lip Synchronization Mechanization

Enables adjustment of the video and the audio if they are out of sync with each other.

Automatic Buffering Control

- ❑ Enables the system to automatically control the amount of buffering required to maintain the consistency of the video and audio transmission. For example, if video packets are delayed for 1 or 2 seconds, the system will automatically synchronize the transmission so that the delay does not disturb the visible video.
- ❑ Deselect this option only if the automatic buffering is not sufficient — for example, if the quality of the video meeting is poor or there is a noticeable delay.

Enable NAT

If your organization uses NAT (Network Address Translation) when communicating with parties in another LAN or WAN, type the external address for the selected user.

NAT helps protect a LAN from exposure to unwanted traffic by providing one single external address to remote users. NAT uses a system of local and external addresses to hide a LAN's users from other networks. A NAT server translates local parties' addresses to an external address, which is then used to identify the local party to remote parties. Therefore, remote parties use this external address to call the local party, without knowing its actual local address.

Use Frontier to Bypass Firewalls

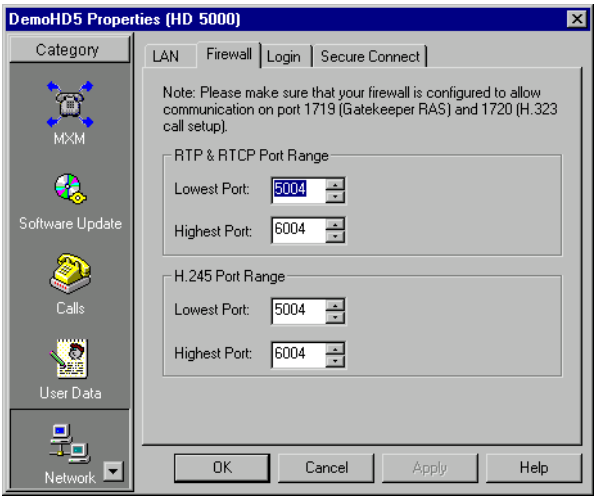
Enables the endpoint to be a Frontier Client. Emblaze-VCON's Frontier system provides conferencing security services, such as firewall traversal, address translation, and encryption.

The MXM will add the end point to the User List of the Frontier Server specified in the adjacent list.

The Frontier Server must be listed in the MXM's Frontier Servers View

Firewall

In the **Firewall** tab, enter the allocation of ports for communication through your organization's firewall.



HD5000 End Point - Firewall Properties

RTP & RTCP Port Range

The MXM allocates a range of ports for video and audio during videoconferences.

This allocation meets the Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) specifications, which enable applications to synchronize and spool audio and video information.

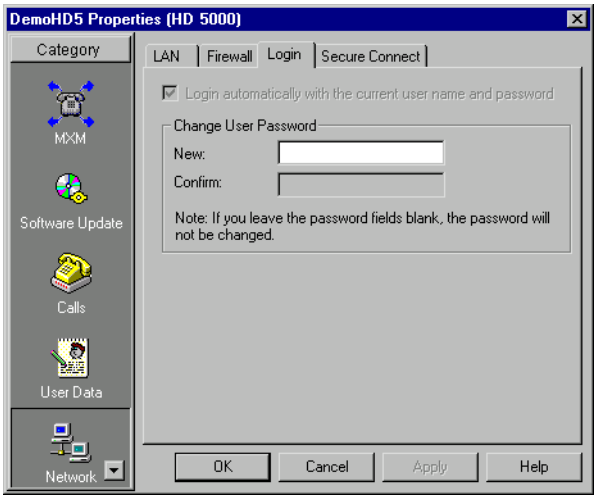
H.245 Port Range

The MXM allocates a range of ports for end-to-end signalling of multimedia during videoconferences.

This allocation provides for H.245 functions, such as capability exchange, signalling of commands and indications, and messages to open and fully describe the content of logical channels.

Login

In the **Login** tab, define how the end point logs into an MXM.



HD5000 End Point - Login Properties

Login Automatically with the Current User Name and Password — The HD5000 end point automatically logs in to the MXM during its startup using the current User Name and Password. If this option is selected, the user does not have to enter login details during HD5000 startup.

Change User Password

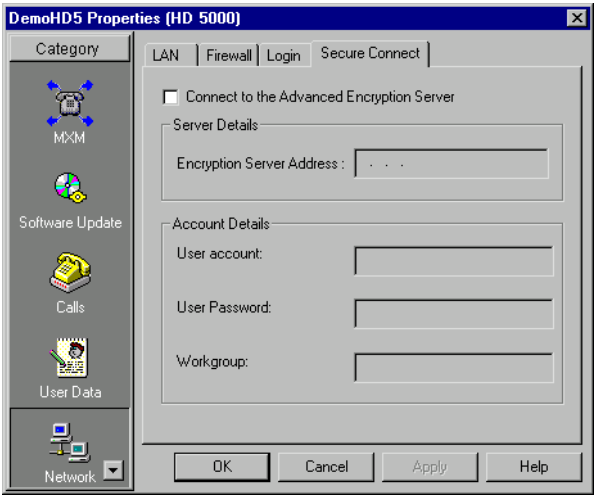
New — Password that replaces the current one.

Confirm — Confirmation of the new password.

If the Password boxes are blank, the current password remains valid.

SecureConnect

The SecureConnect Encryption Client is pre-installed in the HD5000's computer. The **SecureConnect** tab describes this system's Encryption Client identification configuration in a connected Emblaze-VCON Advanced Encryption Server (AES). The AES encrypts conferences and other data transmissions across public or private networks.



HD5000 End Point - SecureConnect Properties

Connect to the Advanced Encryption Server	Select to enable the end point to register with the AES using the settings below.
Encryption Server Address	The IP address of the AES.
User Account	Username required for this end point to log in to the AES.
User Password	Password required for logging in to the AES.
Workgroup	User Group (defined in AES) to which this end point is assigned.

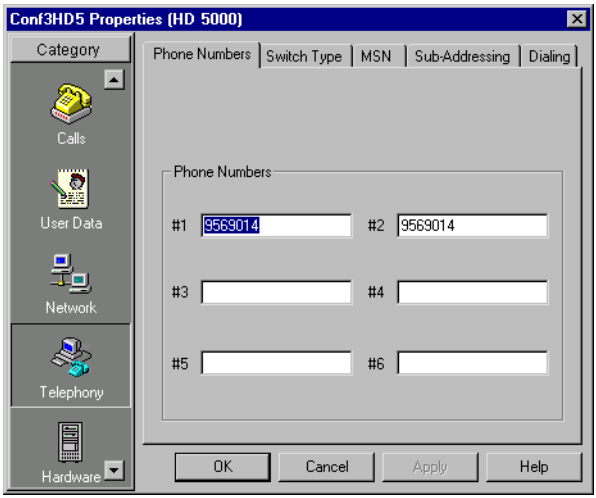
D.4 Telephony Properties

The Telephony Properties dialog box may be used for viewing and controlling various ISDN settings.

These properties are only applicable only to HD5000 end points that are set up for ISDN connection.

Phone Numbers

The **Phone Numbers** tab lists the end point's ISDN phone numbers, if applicable.

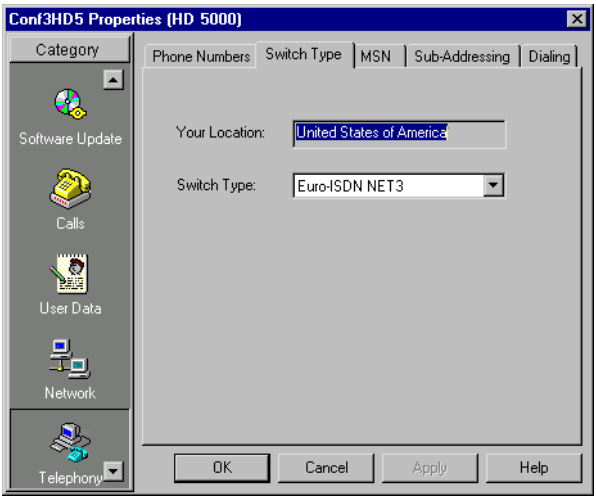


HD5000 End Point - Phone Numbers Properties

Phone Numbers — The ISDN numbers of each line. Do not include your own country's international code or your local area code.

Switch Type

The **Switch Type** tab contains information about the ISDN switch type used by the selected end point.



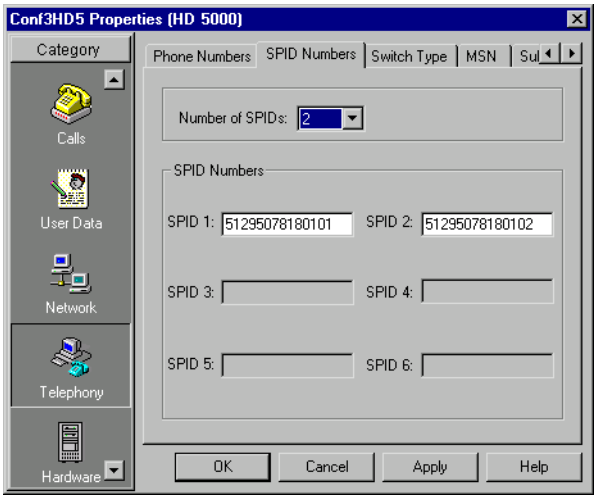
HD5000 End Point - Switch Type Properties

Your Location The country in which the selected user is located.

Switch Type If applicable, the most common switch type for the user's country appears automatically. If a different switch type is being used (according to your ISDN carrier), select it from the list.

SPID Numbers

If the selected ISDN Switch Type supports Service Profile Identifiers (SPID), the **SPID Numbers** tab lists them for the ISDN lines. A SPID number relates to the capabilities of the end point on the ISDN line. This information may be obtained from the end point's ISDN carrier.



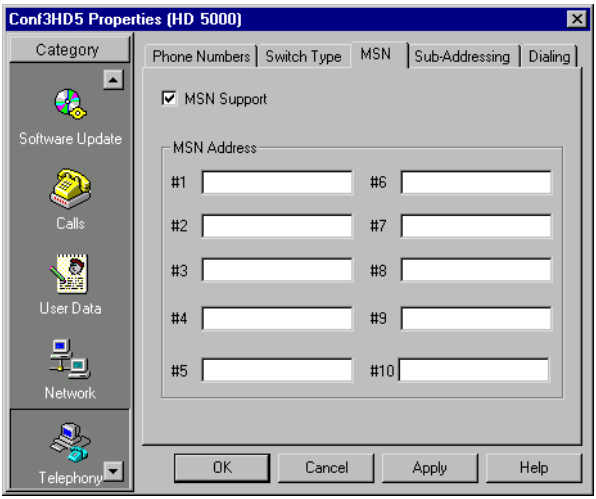
HD5000 End Point - SPID Propertie

Number of SPIDs — Select the number of SPID numbers that were specified by your ISDN carrier.

SPID Numbers 1,2,3,4,5,6 — Type the SPID numbers as your ISDN carrier specifies. If your ISDN provider gave the selected end point only one SPID number, enter it in **SPID 1**.

MSN

The **MSN** tab is relevant if the connected ISDN network supports Multiple Subscriber Numbering (MSN).

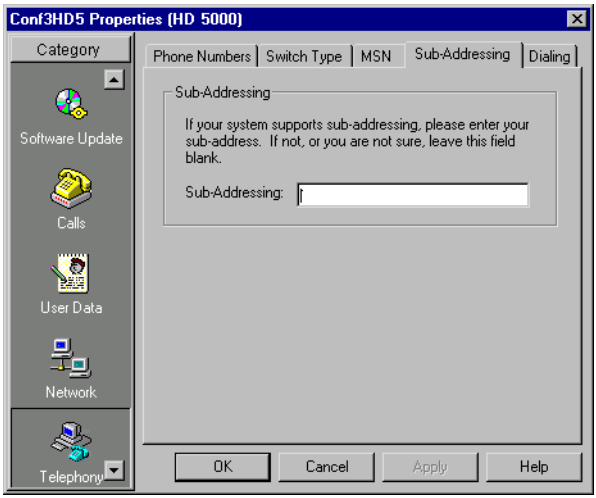


HD5000 End Point - MSN Properties

Select **MSN Support** to use MSN capabilities. In the MSN Address boxes, type the exact MSN numbers for the end point.

Subaddressing

Subaddressing is applicable if the selected system shares an ISDN BRI line with other equipment (such as other computers, fax machines, standard telephones, and so on). In such a case, the end point has an additional series of numbers and/or letters added to the end of its phone number.



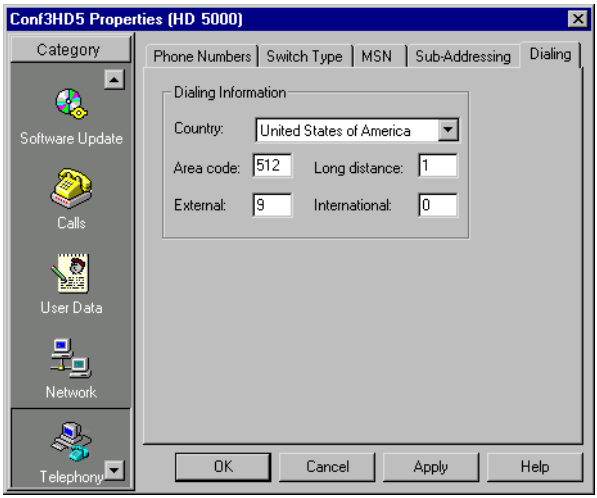
HD5000 End Point - Subaddressing Properties

Sub-Addressing Phone number followed by an "¦" character, and the series of numbers and/or letters making up the subaddress.

Dialing

The Dialing Information area displays the **Country** that the selected user is in, the area code, and the appropriate digits for dialing an outside line (**External**), a **Long Distance** call, or an **International** call.

If the user needs to dial a specific digit to receive an external line, you must type that digit before the digits required for a long distance or international call.
For example, if you must dial 9 to receive an external line, and then 01 to dial long distance, type **901** in the Long Distance box.



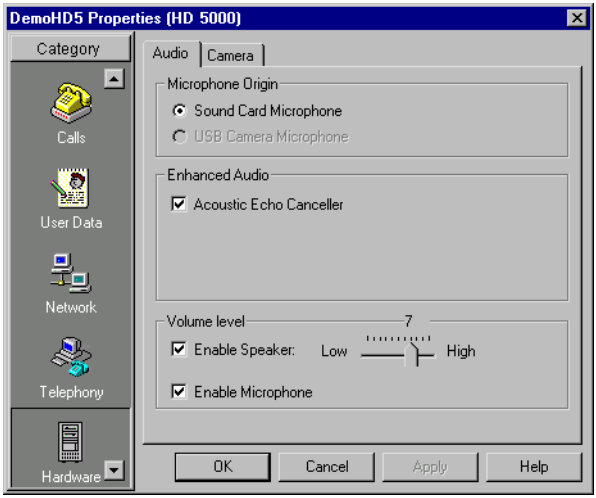
HD5000 End Point - Dialing Properties

D.5 Hardware Properties

The Hardware Properties dialog box may be used for viewing and controlling the Audio and Camera settings of HD5000 end points.

Audio

In the Audio Settings for the HD5000, you can define the audio configuration to be used during videoconferences.



HD5000 End Point - Audio Properties

Microphone Origin

Sound Card Microphone Use a microphone that's connected to your computer's sound card.

Enhanced Audio

Acoustic Echo Canceller (AEC) Select to cancel the echo created when your microphone picks up audio from your speakers.

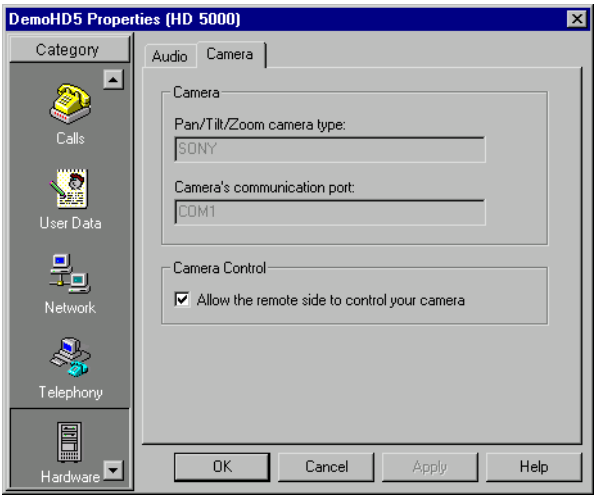
Volume level

Enable Speaker Select to control the volume of the selected end point's speaker. Drag the slider accordingly.

Enable Microphone Select to control the volume through the selected end point's microphone.

Camera

The Pan/ Tilt /Zoom Camera properties are applicable if a Pan/Tilt/Zoom-type (PTZ) camera is connected to the selected system. If a PTZ camera is not used, **None** appears as the PTZ camera type in the dialog box's top list and no communication port is required.



HD5000 End Point - Camera Properties

Pan/Tilt/Zoom camera type — The manufacturer and/or model of the PTZ camera.

Camera's communication port — The name of the computer port to which the camera is connected.

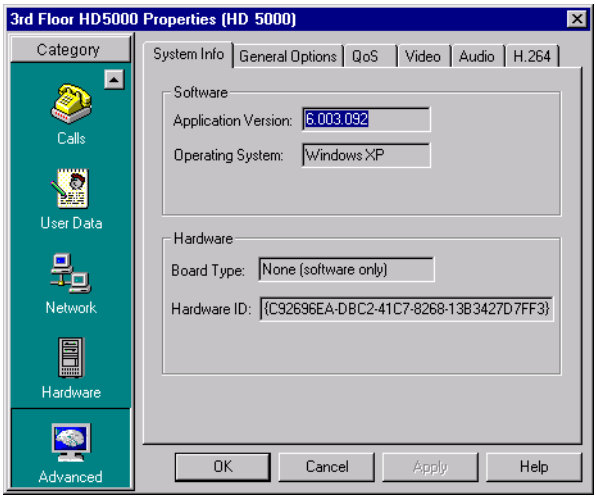
Allow the remote side to control camera settings — Select to permit a remote party in a conference to control the positioning of the selected user's PTZ camera. If a PTZ camera is not used, this option is not relevant.

D.6 Advanced Properties

The Advanced Properties dialog box may be used for viewing end point system information and controlling various QoS, Intras, advanced Video, advanced Audio, and H.264 settings of HD5000 end points.

System Info

The **System Info** tab displays information about the Emblaze-VCON videoconferencing system that's installed in the selected end point. If you contact Emblaze-VCON Technical Support (see "Emblaze-VCON Technical Support"on page vi before the Table of Contents) about a problem associated with this end point, include this information with your request.

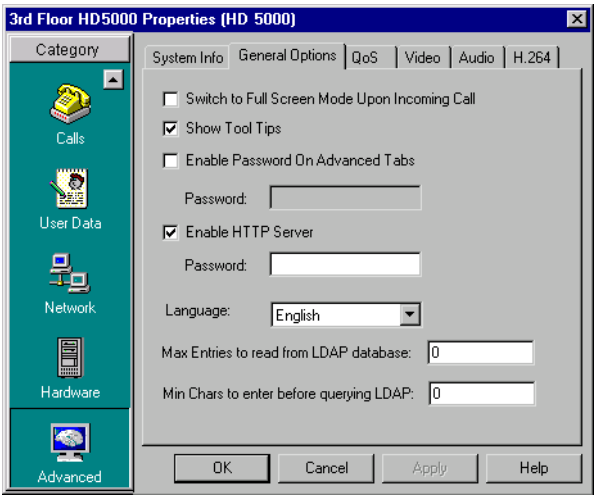


HD5000 End Point - System Information Properties

Application Version	Version number of the HD5000 application running on the end point's computer.
Operating System	Operating system that's installed on the end point's computer.
Board Type	Videoconferencing hardware codec (if applicable) installed in the end point's computer.
Hardware ID	Unique identification number for the videoconferencing card's installation. This number is for Emblaze-VCON Technical Support use.

General Options

The **General Options** settings contains options for various system preferences. Set them according to your configuration requirements.



HD5000 End Point - General Options Properties

Switch to Full Screen Mode Upon Incoming Call — Select to view video on a full monitor display after accepting an incoming call.

Show Tool Tips — Select to display tool tips on the HD5000 interface when the pointer pauses over a command icon.

Enable Password for Advanced Tabs — Select to restrict access to the HD5000's Calls and Network properties. In the **Password** box, type the password required to enter these settings dialog boxes.

Enable HTTP Server — Select to enable web-based remote management of the HD5000 end point. In the **Password** box, type the password for entering the management site.

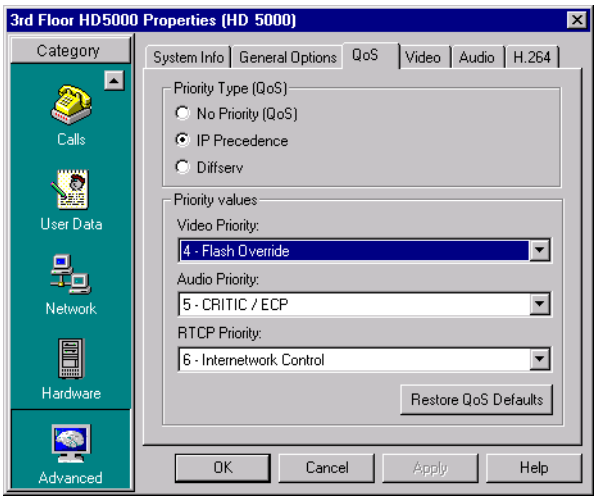
Select Language — Select the language of the HD5000 interface.

Max. Entries to read from LDAP database — Maximum number of online directory entries that the end point will receive and display for the user.

Min Chars. to enter before querying LDAP — Minimum number of characters that the user must type before the end point sends a search query to the online directory.

QoS

The **QoS** tab contains properties for controlling the type of Quality of Service that will be used for transmitting packets from the specified HD5000 end point.



HD5000 Properties - QoS (Default Settings)

Set QoS properties as follows:

Priority Type (QoS)

Select the type of QoS used for transmitting packets during heavy network congestion conditions.

No Priority — Network transfers packets using normal Best-effort (or Routine) packet transmission.

IP Precedence — Network gives priority to certain types of bits (video, audio, control) according to the eight levels of IP precedence.

Diffserv — Network transfers packets according to specific needs of the sending application.

Priority Values

Video, Audio and RTCP Priority

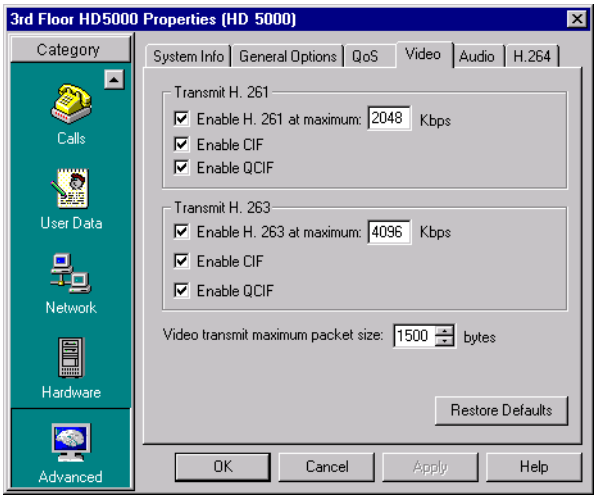
For each packet type, select an appropriate priority level. The item with the highest priority number will be sent first, the item with the next highest number will be sent second, and so on.

The priority levels vary, depending on whether the selected Priority Type is IP Precedence or Diffserv. For a list of Priority levels, see "QoS Priority Values" on page 465.

To reset the Priority default values, click **Restore QoS Defaults**.

Advanced Video

The Advanced **Video** tab permits you to enable usage of H.261 and H.263 for video transmission and to control the bandwidth thresholds for switching between the two standards, if applicable.



HD5000 Properties - Advanced Video

Transmit H.261/H.263

Enable H.261/ H.263 at Maximum

Select to enable the use of the specified video format coding from the specific HD5000 end point. In the box, type the maximum transmission rate at which the specific coding may be used.

For example, for H.263 the default maximum transmission rate is 256 kbps. At higher rates, the H.263 coding is not available.

Enable CIF

Select to transmit video at a higher resolution and lower frame rate, using Common Interchange Format (CIF). Usually, CIF provides better overall video quality, especially when a higher transmission bandwidth, such as 2 x BRI (at least 128 kbps) is available.

All Emblaze-VCON videoconferencing products support CIF. If the remote party's system supports CIF too, this option is the default setting for video transmission.

Enable QCIF — Select to transmit video at a medium resolution and higher frame rate, using Quarter Size Common Interchange Format (QCIF).

QCIF may be chosen if the remote party has a system that does not support CIF format, or if the bandwidth is low.

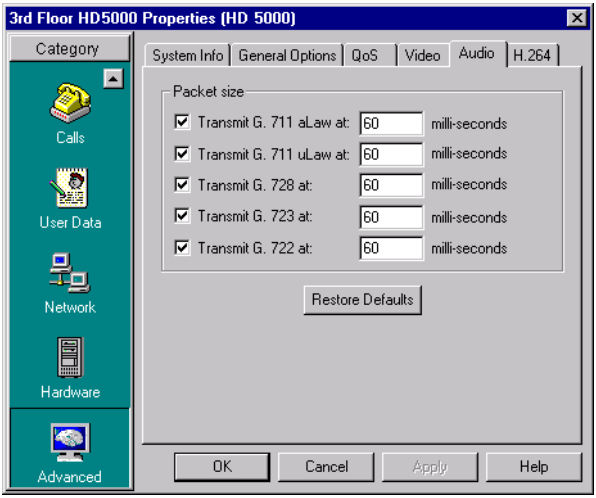
Video Transmit maximum packet size — Enter the maximum video packet size (in bytes) which the specified end point may transmit.

To reset the advanced Video default values, click **Restore Defaults**.

Advanced Audio

In the **Audio** tab, select the supported audio algorithms for transmitting audio from the specified end point. In addition, you can enter the audio transmit speed for all algorithms supported by the end point.

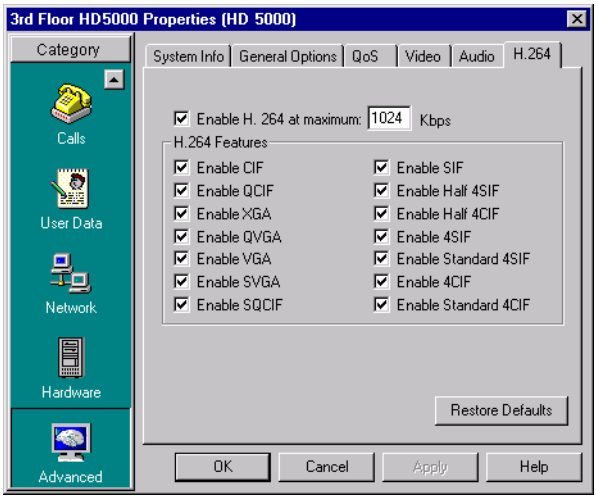
To reset the advanced Audio default values, click **Restore Defaults**.



HD5000 Properties - Advanced Audio

H.264

In the H.264, enable the use of the H.264 codec in this end point's video transmissions. You can enable and disable the use of any combination of the supported video formats in this end point's conferences.



HD5000 Properties - H.264

Enable H.264 at Maximum Select to enable the use of the H.264 codec by this end point up to the maximum bandwidth specified.

H.264 Features Selected formats are activated for use by this end point. Deselect a feature to make it unavailable.

Restore Defaults Click to return to the H.264 default selections.

E UPGRADING HD3000/2000 SOFTWARE UPGRADE

This appendix explains how to upgrade to new software versions of HD3000/2000 throughout your organization using the HD Upgrade Utility.

E.1 Upgrading From a Remote PC

The HD Upgrade Utility is a program that enables you to upgrade HD software from a remote PC, such as your MXM Administrator PC. You can download the utility from Emblaze-VCON's website.

Before Downloading

Before you upgrade the HD software, make sure that the following conditions are present:

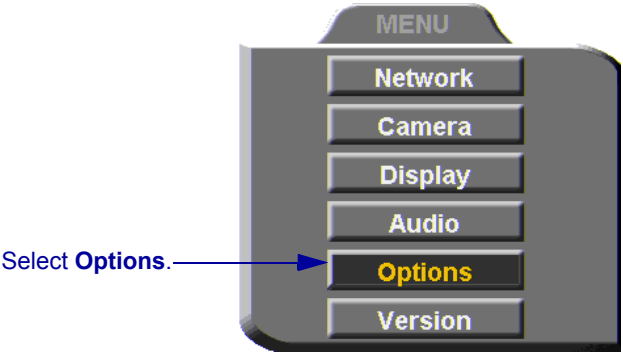
- ❑ A quiet period of the network. We recommend that you perform upgrading when activity on the network is low. Heavy network traffic may interfere with the procedure and cause upgrade failures.
- ❑ The possibility of electrical failure is at a minimum.
- ❑ The computer from which the upgrade will run (referred to throughout this chapter as **the remote PC**) fills the following requirements:
  - — Windows XP, 2000, or NT (with Service Pack 5.0).
  - — No other programs should run at the same time as the HD upgrade program.

Enable Remote Upgrade

To enable upgrading through the HD utility, you must enable remote upgrading in the HD3000/2000's Security dialog box.

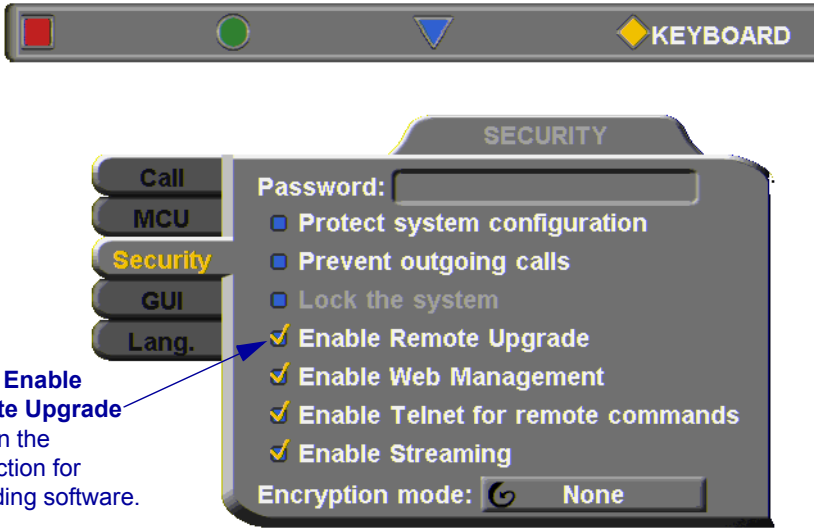
➤ To enable remote software upgrading of the HD

1 Press <Menu>. The main Menu appears. Select **Options**.



2 Navigate to the **Security** tab. If you previously set a security password, enter it in the Password dialog box.

3 Select **Enable Remote Upgrade**.



4 Press <OK>.

Downloading the HD Upgrade Utility

The latest software version is supplied from Emblaze-VCON's website (www.emblaze-vcon.com>Support>Downloads) or by your local Emblaze-VCON distributor.

➤ To download the Upgrade utility

1. On the Emblaze-VCON website's **Downloads** page, click the link for downloading the HD Upgrade utility.
2. Download the setup file to your PC.
3. Run the setup file to install the utility on the remote PC. Perform the steps in the Upgrade utility's installation wizard. Click **Finish** when the process is complete.

Downloading the New HD Software Version

After downloading the Upgrade Utility, return to the Emblaze-VCON website to download the new HD software version.

➤ To download the new HD software version

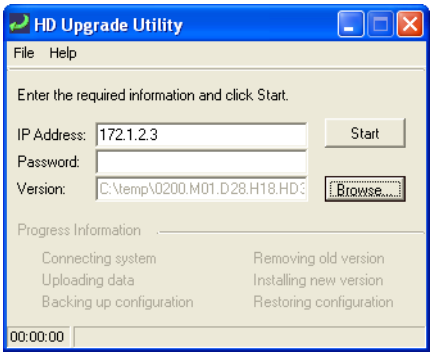
- ❑ On the Emblaze-VCON website's **Downloads** page, click the link for downloading the new HD3000 or HD2000 software version.

Installing the New Upgrade in the HD Device

Run the Upgrade Utility to install the new version in the HD device.

➤ To install the HD software upgrade

1. In the PC, run **Start>Programs>VCON>HD Utilities>Upgrade Utility**.



2. Type the **IP address** of the HD device.

3. If applicable, enter the **Password** defined in the HD's Security settings.
4. Click **Browse** to select the upgrade file that you previously downloaded from the Emblaze-VCON website.
5. Click **Start**.

CAUTION The entire procedure takes several minutes. During the upgrade, the remote PC will not respond to other programs. Do **not** restart the HD device until the upgrade process is complete!

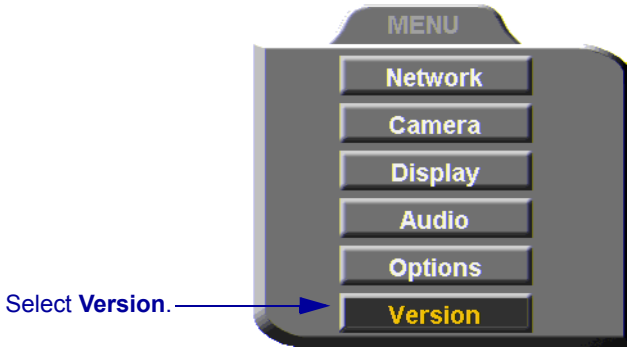
When the upgrade installation finishes, the HD device restarts. Wait until the Ready Screen appears.

E.2 Confirming Successful Upgrade

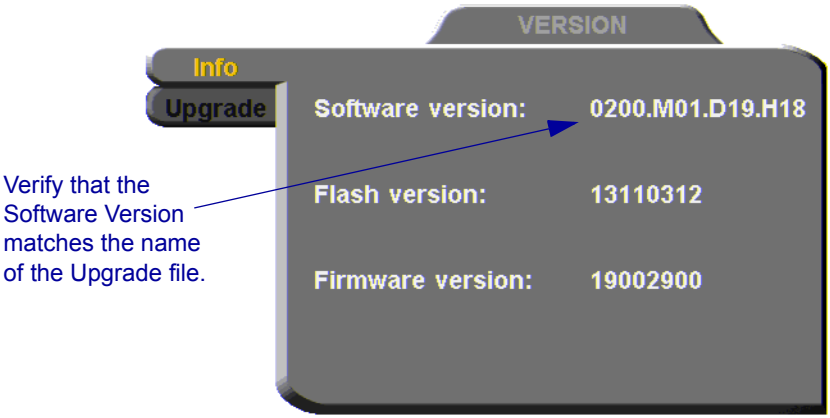
At this stage, confirm that the latest software is running on the HD.

➤ To check the version of the HD software

1 Press <Menu>. The main Menu appears. Select **Versions**.



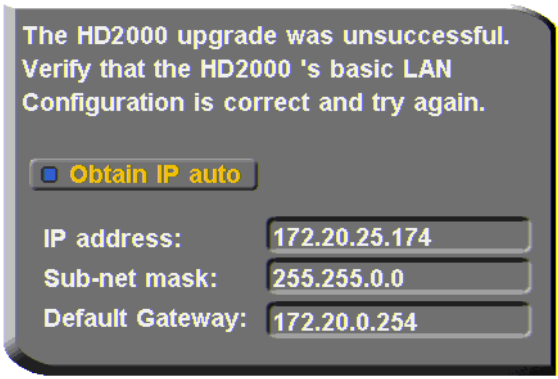
2 In the Info dialog box, verify that the **Software Version** matches the name of the upgrade file that you downloaded. If it does, the HD is ready for use!



E.3 Installer Mode

If for some reason the upgrade was not successfully completed, the HD enters Installer Mode after it restarts.

1. Verify that you've entered the correct Network information before running the upgrade program again.



2. Write down or copy the IP address of the HD device. Press <OK>.
3. Rerun the upgrade process from the HD Upgrade Utility. Be sure to enter the correct IP address for the HD device.

If this process is unsuccessful again, contact Emblaze-VCON's Technical Support (see "Emblaze-VCON Technical Support" on page vi).

F QoS Priority Values

The tables in this appendix list the available priority values for Quality of Service (QoS) configuration. The MXM Administrator application supports QoS configuration of Emblaze-VCON end points.

F.1 IP Precedence Values

Value	Description
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash Override
5	Critic/ECP
6	Internetwork Control
7	Network Control

F.2 DiffServ Values

Value	Description
000000	Probability Timely Forwarding 0
001000	Probability Timely Forwarding 1
010000	Probability Timely Forwarding 2
011000	Probability Timely Forwarding 3
100000	Probability Timely Forwarding 4
101000	Probability Timely Forwarding 5
110000	Probability Timely Forwarding 6
111000	Probability Timely Forwarding 7
101110	Expedited Forwarding
001010	Forward Class 1 Low Drop
001100	Forward Class 1 Mid Drop
001110	Forward Class 1 High Drop
010010	Forward Class 2 Low Drop
010100	Forward Class 2 Mid Drop
010110	Forward Class 2 High Drop
011010	Forward Class 3 Low Drop
011100	Forward Class 3 Mid Drop
011110	Forward Class 3 High Drop
100010	Forward Class 4 Low Drop
100100	Forward Class 4 Mid Drop
100110	Forward Class 4 High Drop

INDEX

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

W

Z