Notice

© 2000 RADVision Ltd. All intellectual property rights in this publication are owned by RADVision Ltd. and are protected by United States copyright laws, other applicable copyright laws and international treaty provisions. RADVision Ltd. retains all rights not expressly granted.

No part of this publication may be reproduced in any form whatsoever or used to make any derivative work without prior written approval by RADVision Ltd.

No representation of warranties for fitness for any purpose other than what is specifically mentioned in this guide is made either by RADVision Ltd. or its agents.

RADVision Ltd. reserves the right to revise this publication and make changes without obligation to notify any person of such revisions or changes. RADVision Ltd. may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this publication, it is furnished under a license agreement included with the product as a separate document. If you are unable to locate a copy, please contact RADVision Ltd. and a copy will be provided to you.

Unless otherwise indicated, RADVision registered trademarks are registered in the United States and other territories.

Microsoft and Windows are registered trademarks of the Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.


RADVision Ltd.:
24 Raul Wallenberg
Tel Aviv 69719, Israel
Tel: +972-3-645-5220
Fax: +972-3-647-6669
Video: +972-3-648-9010
email: HWsupport@tlv.radvision.com
http://www.radvision.com

RADVision Inc.:
575 Corporate Drive
Mahwah, NJ 07430, USA
Tel: (201) 529-4300
Fax: (201) 529-3516
Video: (201) 529-3714, (201) 529-1906
email: OnLANsupport@radvision.com
# Table of Contents

## About This User Guide
- Conventions Used in this Guide
- Finding Specific Information

## Overview
- Introduction
- MCU-323 Functionality
  - Immediate Conference Setup
  - Web Interface
  - Voice–activated Video Switching
  - Continuous Presence
  - Data Collaboration Using T.120
  - Audio Mixing
  - Audio Transcoding
- MCU-323 Topologies
  - Distributed MCU-323s
  - Cascaded Conferences
  - Bandwidth Considerations
- Summary of MCU-323 Features
- Summary of Built-in Gatekeeper Features
- Physical Description of the MCU-323
  - Front Panel
  - Rear Panel

## Installing the MCU-323
- Prepare the Site
- Make Cable Connections
  - Connect the Power
  - Connect to the LAN
Table of Contents

Mount the MCU-323 in a 19-inch Rack 2-3
Install the RADVision OnLAN Tools 2-4

Preparing for Configuration
Invoking the OnLAN Configure 323 Application 3-1
Selecting an MCU-323 for Configuration 3-1
Entering a New IP Address for a New MCU-323 3-2
Passwords 3-3
Changing the MCU-323 Password 3-4
Selecting a Configuration Source 3-5
Selecting the Unit Type and What You Want to Configure 3-6

Configuring the Built–in Gatekeeper
Accessing the Gatekeeper Configuration 4-1
Services Definition 4-2
Service Access Control 4-5
Single Number Access to a Group of Terminals 4-5
Editing the Gatekeeper Default Services 4-6
Deleting and Adding Gatekeeper Services 4-6
Saving the Service Definitions to a File 4-7
Zone Definition 4-8
Zone Access Control 4-8
Adding a New Endpoint 4-12
Defining the Properties of a New Endpoint 4-13
Specifying Allowed Services 4-14
Predefining Endpoints in a Dynamic IP Environment 4-15
Editing Endpoint Settings 4-16
Adding Predefined Properties to an Online Endpoint 4-19
Deleting an Endpoint 4-19
Saving or Loading Settings of the Zone Definition Table 4-20
Neighbor Gatekeepers 4-21
Adding a New Neighbor Gatekeeper 4-23
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing Neighbor Gatekeeper Settings</td>
<td>4-24</td>
</tr>
<tr>
<td>Deleting a Neighbor Gatekeeper</td>
<td>4-24</td>
</tr>
<tr>
<td>Saving and Loading Neighbor Gatekeepers Table Settings</td>
<td>4-24</td>
</tr>
<tr>
<td><strong>Network Topology</strong></td>
<td></td>
</tr>
<tr>
<td>Adding a New Subnet Address</td>
<td>4-28</td>
</tr>
<tr>
<td>Editing Subnet Setting</td>
<td>4-29</td>
</tr>
<tr>
<td>Deleting a Subnet Setting</td>
<td>4-29</td>
</tr>
<tr>
<td>Saving or Loading Network Topology Table Settings</td>
<td>4-29</td>
</tr>
<tr>
<td><strong>Network Control</strong></td>
<td></td>
</tr>
<tr>
<td>Disabling the Built–in Gatekeeper</td>
<td>4-34</td>
</tr>
<tr>
<td>Alias Assignment</td>
<td>4-34</td>
</tr>
<tr>
<td>Distance Settings</td>
<td>4-35</td>
</tr>
<tr>
<td>Saving or Loading Network Control Settings</td>
<td>4-36</td>
</tr>
<tr>
<td><strong>Supporting the H.323 Proxy</strong></td>
<td></td>
</tr>
<tr>
<td>The H.323 Proxy</td>
<td>5-1</td>
</tr>
<tr>
<td>Proxy Facilitated Call Flow</td>
<td>5-2</td>
</tr>
<tr>
<td>Configuring the Built–in Gatekeeper for Proxy Support</td>
<td>5-4</td>
</tr>
<tr>
<td><strong>Configuring the Unit</strong></td>
<td></td>
</tr>
<tr>
<td>Selecting the Unit Type and What You Want to Configure</td>
<td>6-1</td>
</tr>
<tr>
<td>Configuring a Single Station MCU-323</td>
<td>6-3</td>
</tr>
<tr>
<td>Identification Information</td>
<td>6-3</td>
</tr>
<tr>
<td>Date/Time Settings</td>
<td>6-4</td>
</tr>
<tr>
<td>Defining Conferencing Services</td>
<td>6-5</td>
</tr>
<tr>
<td>Adding, Editing, or Deleting Conferencing Services</td>
<td>6-10</td>
</tr>
<tr>
<td>Defining a Default Gatekeeper and Router</td>
<td>6-11</td>
</tr>
<tr>
<td>LAN Port Settings</td>
<td>6-12</td>
</tr>
<tr>
<td>Configuring a Distributed MCU-323</td>
<td>6-14</td>
</tr>
<tr>
<td>Identification Information</td>
<td>6-14</td>
</tr>
<tr>
<td>Date/Time Settings</td>
<td>6-14</td>
</tr>
<tr>
<td>Defining MPs for the Distributed MCU-323</td>
<td>6-15</td>
</tr>
<tr>
<td>Adding an MP Entry</td>
<td>6-16</td>
</tr>
<tr>
<td>Editing MP Entries</td>
<td>6-17</td>
</tr>
</tbody>
</table>
## Table of Contents

### Defining Conferencing Services for the Distributed MCU-323
- Defining Conferencing Services for the Distributed MCU-323 6-17
- Linking a Conferencing Service to an MP 6-18
- Defining a Default Gatekeeper and Router for a Distributed MCU-323 6-20
- LAN Port Settings for a Distributed MCU-323 6-21

### Configuring a Dedicated MP
- Identification Information 6-22
- Date/Time Settings 6-22
- Defining a Default Router for a Dedicated MP 6-23
- LAN Port Settings for a Dedicated MP 6-23

### Saving the Unit Setup
- Saving the Unit Setup 6-25
- File Extensions for Saved Configuration Files 6-27

### Using the MCU-323

#### Organizing a Conference
- Organizing a Conference 7-1
  - Joining a Conference 7-1
  - Inviting a Participant Into a Conference 7-1
  - Creating a Cascaded Conference 7-2

#### Using the Web Interface
- Using the Web Interface 7-4
  - Web Interface Requirements 7-4
  - Starting the Web Interface 7-4
  - Monitoring a Conference from the Web Interface 7-5
  - Function Buttons 7-6
  - Participants Table 7-6
  - Opening a Data Collaboration Session 7-8
  - Inviting Participants from the Web Interface 7-9

#### Taking Chair Control of a Conference
- Taking Chair Control of a Conference 7-11

#### Disconnecting a Participant
- Disconnecting a Participant 7-13

#### Locking the Conference to View One Participant
- Locking the Conference to View One Participant 7-14

### Using the T.120 Server

#### Overview
- Overview 8-1

#### Configuration Checklist
- Configuration Checklist 8-2

#### Tips and Considerations
- Tips and Considerations 8-3
# Table of Contents

## Using the Advanced Commands of the MCU-323
- Overview 9-1
- Using the Advanced Commands 9-1

## Troubleshooting the MCU-323
- LED Indications 10-1
- Initial Setup Problems 10-1
  - Console Port Access Problems 10-1
- Operation Tips 10-2

## Safety Considerations
- Safety Considerations A-1
  - Grounding A-1
  - High Voltage A-1

## Cable Connectors
- RS-232 9-pin Serial Port B-1
- Null Modem Cable B-1
- RJ-45 8-pin LAN Port B-2

## Uploading Files to the MCU-323
- Using the Software Upload Utility C-1
- Uploading Flash Files to the MCU-323 C-3

## Technical Specifications
- Interfaces D-1
- LED Indicators D-1
- Dimensions D-1
- Power Supply D-1
- Environment D-1
Table of Figures

Figure 1-1 – Typical Multipoint Conference Layout ................................................................. 1-1
Figure 1-2 – Continuous Presence Quadrant Distribution ......................................................... 1-4
Figure 1-3 – Distributed MCU-323s ...................................................................................... 1-6
Figure 1-4 – Typical conference over the LAN with one MCU-323. Four media streams are required, using four times the bandwidth ................................................................. 1-8
Figure 1-5 – Cascaded conference minimizing the use of network bandwidth. The MCU-323 processing toll is distributed among participating MCU-323s .................................................. 1-8
Figure 1-6 – MCU-323 Front Panel ....................................................................................... 1-13
Figure 1-7 – MCU-323 Rear Panel ...................................................................................... 1-14
Figure 2-1 – Attaching Rack Mounting Brackets ................................................................. 2-3
Figure 3-1 – Select Unit screen .......................................................................................... 3-1
Figure 3-2 – Enter Password screen .................................................................................. 3-3
Figure 3-3 – Change Password screen ............................................................................. 3-4
Figure 3-4 – Configuration Source screen ......................................................................... 3-5
Figure 4-1 – Application Parameters screen ........................................................................ 4-1
Figure 4-2 – Gatekeeper Services Definition Table screen ................................................ 4-3
Figure 4-3 – Services Definition screen ............................................................................. 4-4
Figure 4-4 – Zone Definition table ....................................................................................... 4-10
Figure 4-5 – Predefined Properties screen ........................................................................ 4-12
Figure 4-6 – Allowed Services screen .............................................................................. 4-14
Figure 4-7 – Online Properties screen .............................................................................. 4-17
Figure 4-8 – Supported Services screen for a Gateway ...................................................... 4-18
Figure 4-9 – Neighbor Gatekeepers Table screen ............................................................... 4-22
Figure 4-10 – Neighbor GK Parameters screen .................................................................. 4-23
Figure 4-11 – Network Topology Table screen .................................................................. 4-27
Figure 4-12 – Subnet Parameters screen ........................................................................... 4-28
Figure 4-13 – Network Control screen ............................................................................. 4-30
Figure 4-14 – Advanced Settings screen ......................................................................... 4-33
Figure 5-1 – Obtaining Address Information via GK .............................................................. 5-2
Figure 5-2 – Call Completion Facilitated by Proxies ............................................................... 5-3
Figure 6-1 – Unit Identifications screen ............................................................................. 6-3
Figure 6-2 – Date/Time Settings ......................................................................................... 6-4
Figure 6-3 – Service Definition Table ............................................................................... 6-5
Figure 6-4 – Service Settings screen with Continuous Presence enabled .......................... 6-7
Figure 6-5 – Miscellaneous Settings screen .................................................................... 6-11
Figure 6-6 – LAN Port Settings ......................................................................................... 6-12
Figure 6-7 – LAN Parameters ............................................................................................ 6-13
Figure 6-8 – MP Definition Table......................................................................................................... 6-15
Figure 6-9 – MP Settings screen........................................................................................................ 6-16
Figure 6-10 – Services Definition Table for the Distributed MCU-323.............................................. 6-17
Figure 6-11 – Service Settings screen for a Distributed MCU-323 ...................................................... 6-19
Figure 6-12 – Miscellaneous Settings screen for a Dedicated MP ..................................................... 6-23
Figure 6-13 – Save Setup for MCU-323 Parameters ....................................................................... 6-25
Figure 6-14 – Confirm......................................................................................................................... 6-26
Figure 7-1 – The Web Interface starting page ................................................................................... 7-5
Figure 7-2 – Participants Table........................................................................................................... 7-6
Figure 7-3 – Opening a data collaboration session with another terminal........................................ 7-8
Figure 7-4 – Inviting a new participant from the web interface....................................................... 7-9
Figure 7-5 – Obtaining Chair Control............................................................................................... 7-12
Figure 7-6 – Disconnecting a participant from the conference........................................................... 7-13
Figure 7-7 – Locking the conference video broadcast on a participant............................................ 7-14
Figure 9-1 – Advanced Commands screen....................................................................................... 9-1
Figure B-1 – Null modem cable connectors ...................................................................................... B-1
Figure C-1 – Software Upload Utility screen..................................................................................... C-2
About This User Guide

The OnLAN MCU-323 User Guide describes the RADVision MCU-323 functionality and how to install and configure the unit for operating with an IP network.

This user guide is intended for a Network Administrator or a user with equivalent network experience. The OnLAN 323 Configuration software is a Windows application. This manual assumes you have knowledge of Windows 95/98/NT. The chapters are organized in a procedural format to instruct you how to install, configure, and use the MCU-323.

Conventions Used in this Guide

The following table lists the notation conventions used throughout this guide.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway/gateway; Gatekeeper/gatekeeper</td>
<td>When capitalized, Gateway and Gatekeeper refer to the RADVision L2W-323 Gateway and the RADVision Gatekeeper. Otherwise, they refer to H.323 gateways and gatekeepers in general.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Information note that describes important features or instructions.</td>
</tr>
<tr>
<td><strong>Warning</strong></td>
<td>Information that alerts you to potential danger to yourself or the MCU-323.</td>
</tr>
<tr>
<td>Menu commands, buttons and text-boxes</td>
<td>Menu commands, button names and text-boxes appear in <strong>bold</strong>.</td>
</tr>
<tr>
<td>Glossary terms</td>
<td>The first time a Glossary entry appears in the text, it is <strong>bolded</strong>.</td>
</tr>
</tbody>
</table>
# Finding Specific Information

This table shows where to find specific information in this guide.

<table>
<thead>
<tr>
<th>If you are looking for...</th>
<th>Go to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>An introductory overview of the MCU-323, a summary of its features, and its physical description</td>
<td>Overview</td>
</tr>
<tr>
<td>Physical Setup and cabling of the MCU-323</td>
<td>Installing the MCU-323</td>
</tr>
<tr>
<td>Installing the OnLAN Tools configuration software</td>
<td>Installing the RADVision OnLAN Tools</td>
</tr>
<tr>
<td>Beginning Configuration</td>
<td>Preparing for Configuration</td>
</tr>
<tr>
<td>Procedures for configuring the built-in Gatekeeper</td>
<td>Configuring the Built-in Gatekeeper</td>
</tr>
<tr>
<td>Configuring support for the Cisco H.323 Proxy</td>
<td>Supporting the H.323 Proxy</td>
</tr>
<tr>
<td>Procedures for configuring the MCU-323</td>
<td>Configuring the Unit</td>
</tr>
<tr>
<td>Setting up a conference using the MCU-323</td>
<td>Using the MCU-323</td>
</tr>
<tr>
<td>Description and configuration for the T.120 server</td>
<td>Using the T.120 Server</td>
</tr>
<tr>
<td>Monitoring and controlling a conference via the Web</td>
<td>Using the MCU-323 Web Interface</td>
</tr>
<tr>
<td>Solutions to problems you may encounter in using the MCU-323</td>
<td>Troubleshooting the MCU-323</td>
</tr>
<tr>
<td>Cable pin-out diagrams, safety information, technical specifications, and a list of terms used in this guide</td>
<td>Appendices and Glossary</td>
</tr>
</tbody>
</table>
Overview

This chapter provides an overview of the MCU-323, its functionality, features, and physical description.

- Introduction
- MCU-323 Functionality
- MCU-323 Topologies
- Summary of MCU-323 Features
- Summary of Built-in Gateway Features
- Physical Description of the MCU-323
Introduction

The concept of videoconferencing is older than the advent of computers. The desire to add a video dimension to telephone calls was discussed as early as the 1920's. Multimedia conferencing over packet-based networks is the newest frontier of videoconferencing, adding the dimension of data collaboration to audio and video. The latest developments increase the efficient use of bandwidth and reduce the cost of both ownership and the use of videoconferencing equipment. Using common terminal equipment, anyone can carry on a videoconference with multiple participants, supported by an easy to use Multipoint Conferencing Unit (MCU) that runs unattended.

The RADVision MCU-323 system is a complete multimedia multipoint conferencing solution that includes a Multipoint Conferencing Unit and a Gatekeeper integrated into one box. The MCU-323 provides multipoint conference call services at low cost and high performance levels. Based on the RADVision H.323 Stack, which is widely used in many other H.323 compliant products, the MCU-323 is fully H.323 compliant and provides a high degree of interoperability with other conferencing systems and components. The MCU-323 offers a scalable solution at a low entry price. Utilizing distributed topologies that significantly reduce the overall bandwidth and CPU use per connection, the MCU-323 also reduces the dependence on costly telephone and ISDN lines.

Figure 1-1 – Typical Multipoint Conference Layout
MCU-323 Functionality

The MCU-323 enables voice only and multimedia conference calls between H.323 entities and non-H.323 entities. Non H.323 devices such as voice telephones and videoconferencing endpoints can connect to a conference via a gateway or a VIU-323 device.

The MCU-323 supports LAN and WAN terminals that can send and receive video streams, as well as those that only receive video streams. This means that terminals without a video camera or video capturing capabilities can participate in a conference as “voice only” participants while benefiting from seeing the other participants.

Immediate Conference Setup

In the past, the process of setting up and coordinating a multipoint videoconference was complicated and lengthy. The conference had to be planned well in advance, conference time was reserved at a service provider well in advance and all participants were notified of a specific date and time and conference identification code. A skilled technician was required to help set up the equipment and make sure the conference ran smoothly.

Today, the MCU-323 allows users to spontaneously initiate multipoint conferences. It runs unattended —there is no need to configure conferences in advance. A participant simply dials a number and the MCU-323 automatically sets up the conference. Anyone else who dials that number can join the conference at any time. The MCU-323 permits users to "invite" others to join the conference just as some telephones allow users to set up their own conference calls without the assistance of an operator.

Web Interface

The MCU-323 web interface allows you to control and monitor a conference through a web browser page displaying the participants names, phone numbers, and terminal types. Once the conference has been started, the participants decide upon a chairman to lead the conference. Anyone can view the web page for the conference by simply entering the IP address and conference ID (password) for the conference. The appointed chairman can obtain Chair Control of the conference at the click of a button. Chair Control allows the chairman to Lock the conference on a single participant, such as a lecturer giving a presentation. The chairman can also Disconnect participant terminals using the Chair Control. This for example, is useful in conserving bandwidth when a participant has left the conference without disconnecting their terminal.
Voice–activated Video Switching

The MCU-323 performs automatic switching of the video image viewed at each terminal according to the voice level of each participant. Whoever is speaking the loudest is the participant that is viewed. An adjustable minimum time interval for voice activation defines the minimum time interval before video images are switched. Normally, all the participants see the active speaker on their screen. The active speaker sees the previous active speaker on his screen, or himself (configurable). If the conference chairman locks the image to one participant, video switching is suspended and all conference participants see the participant that has been locked.

Continuous Presence

Continuous Presence allows you to view a number of participants in one screen simultaneously. The MCU-323 provides a Continuous Presence screen that is composed of four quadrants of equal size, each displaying the video image of a different participant. The upper left-or lower right hand quadrant (configurable) contains a voice–activated image that updates as attention shifts from one speaker to another. The remaining three quadrants contain the images of three other participants in the order that they join the conference on a "first come first serve" basis. Once all four quadrants are filled, only the loudest participant in the conference can replace the voice–activated quadrant. If the loudest speaker is already present in one of the remaining three quadrants, no switching occurs and the voice–activated quadrant remains as before. If one of the other three quadrants is vacated by disconnecting from the conference, that quadrant is filled by the next participant in line in the order of joining the conference.

The Continuous Presence image is formed by unifying (up to) four video images into a single picture. This is achieved by the MCU-323 unifying four QCIF signals and sending the resulting CIF signal to each participant of the conference. Because of this signal mixing, the outgoing bandwidth from the MCU-323 is four times that of the incoming bandwidth. This factor should be considered when setting up and allocating network resources for a conference using Continuous Presence. A Continuous Presence conference is set up by dialing a dedicated service that is defined for Continuous Presence. When a conference is set up across a Gateway or VIU–323 connection, participants at the remote end can only receive a single picture image, the voice–activated image of the active speaker. The incoming image from a Gateway or VIU–323 connected participant can be mixed in the Continuous Presence screen in the same manner as a participant on the LAN.

Chair Control Locking of the video image (via the MCU-323 web interface) can be used to suspend the voice–activated video switching. When locked, the voice activated picture quadrant remains the same, and video switching is suspended. Additional participants can enter the CP screen only if one of the quadrants is vacated by disconnection from the conference. In cascaded conferences, the Locking feature behaves differently for Master and Slave units, see Cascaded Conferences in this chapter.
Data Collaboration Using T.120

Data collaboration over the videoconference connection enhances the conference by providing the tools for sharing binary data instantaneously. Diagrams, graphic presentations, and slide lectures can be viewed simultaneously by participants of a videoconference. In addition, private text chats or whiteboard exchanges as well as rapid file transfers can be carried out while the videoconference proceeds. Limited support for data sharing without the use of an external T.120 Server can be activated using the MCU–323 web interface for endpoints that support data collaboration using NetMeeting.

Data sharing is facilitated by an external, Windows NT based RADVision T.120 Data Collaboration Server (DCS). The DCS controls the data sharing channels between terminals. It supports data sharing in multiple MCU–323 units simultaneously while remaining transparent to the conference participant.
Audio Mixing

The MCU-323 performs audio mixing on the incoming audio streams, and distributes an adjusted audio stream to the conference participants (removing the self– audio stream of each participant). The audio level adjustment is performed by an AGC (Automatic Gain Control) algorithm. The supported audio codings are: G.711 A Law and μ Law, G.723.1 and G.729 A/B. A mix of these audio codings in the same conference is also supported.

Audio Transcoding

Audio transcoding is the conversion of one audio transmission format into another using various algorithms to achieve different audio quality levels at reduced bandwidth levels. This can be used to accommodate endpoints that can only process specific audio formats, and to free up bandwidth on the LAN.

The MCU-323 provides audio transcoding for the G.723.1 (at bandwidth of 5.3 or 6.3 Kbps) and G.729 A/B (at bandwidth of 8 Kbps) codecs. The MCU-323 can be configured to prioritize the transcoding, giving preference to a particular codec that is requested in a defined conference service. The transcoding capacity depends on the number of optional transcoder modules installed in the MCU-323 and is available in configurations of 0, 16, or 24 supported ports. The MCU-323 can support conferences that combine transcoding methods such as G.723.1 and G.711 or G.729 and G.711.
MCU-323 Topologies

The MCU-323 operates in a centralized topology with terminals working opposite an MCU-323 unit, as opposed to connecting directly to each other. To facilitate better CPU and bandwidth utilization, you can arrange the MCU-323 in a distributed or cluster configuration. To increase the total number of participants in a conference, you can cascade two or more individual conferences. A description of the two configurations follows.

Distributed MCU-323s

The MCU-323 supports a distributed architecture of one controlling unit and up to four dedicated MCU-323s, significantly increasing the number of simultaneous calls that are possible. A single MCU-323, configured as a Distributed MCU-323 functions as the MC (Multipoint Controller) and includes a Dedicated MP section in the same unit, controlling up to three other MCU-323s configured as a Dedicated MP. Each Dedicated MP can act as a Multipoint Processor for a number of individual conferences. This cluster of MC and associated MPs are registered with a Gatekeeper as a single MCU-323 device. This means that routers and gateways on the network are not overloaded by all the media streams of a conference at once.

In a typical scenario, four MCU-323 units can each support multiple conferences with up to 15 participants per MCU-323, and one of the four units performs all control and management functions. You define Conferencing Services in the Distributed MCU-323, and Dedicated MP units are defined in the Distributed MCU-323 as linked MPs.

Figure 1-3 – Distributed MCU-323s
Cascaded Conferences

The MCU-323 allows you to join two or more conferences managed by separate MCU-323s to make one larger conference with many more participants. This is called **cascading**. Cascading creates a distributed environment that helps you reduce the drain on network resources. In addition, the processing resources required by the MCU-323 are distributed between the participating MCU-323s. Costly telephone line and ISDN line usage can be further reduced with the mediation of a Gateway.

Cascading occurs when one MCU-323, with "x" number of participants already in a conference, invites another MCU-323 with an active conference of "y" participants, into the conference. The two conferences effectively become one larger conference. The bandwidth being used across the cascaded link is only that of one audio/video stream between the two MCU-323s, instead of each participant adding the bandwidth of a direct call connection with another participant. Each MCU-323 unit retains control of its individual conference resources and participants.

In a cascaded conference using Continuous Presence, one MCU-323 must be defined as a Master, and all other units in the conference are defined as Slaves (configured in the Service Settings screen of the Unit Configuration). The image viewed by all participants of the conference is a four picture composite processed by the Master MCU-323 unit. In a cascaded CP conference, the Chair Control Locking feature acts differently in the Master and Slave units. In the Master MCU–323, Locking suspends voice–activated video switching in the voice–activated quadrant, and the participants in all quadrants do not change unless they disconnect from the conference and are replaced by another participant. In a Slave unit, Locking selects a single participant connected to that Slave unit, and sends only that participant's image to the Master MCU–323. The Master unit adds that image to the mix according to the normal mixing rules for the CP conference.

**Note**

Before a Slave unit joins a cascaded conference, it performs just like a Master unit in all respects.

The number of conferences you can unite into one conference depends on the bandwidth available on the LAN. Connecting each MCU-323 unit to a separate network segment can improve the capacity and prevent videoconferencing congestion on a particular network segment.

**Example:**

An MCU-323 that optimally supports up to 15 participants in a 110 Kbps (video bit rate) videoconference can cascade two MCU-323s and increase the total number of participants to as much as 28 utilizing the same bandwidth per LAN segment.
Figure 1-4 – Typical conference over the LAN with one MCU-323. Four media streams are required, using four times the bandwidth.

Figure 1-5 – Cascaded conference minimizing the use of network bandwidth. The MCU-323 processing toll is distributed among participating MCU-323s.
Bandwidth Considerations

When all the conference participants are connected to a LAN, the available bandwidth is determined by the capacity of the video conferencing programs in use, the use of audio transcoding, and policies set by the system administrator. The system administrator can limit the available bandwidth through the Gatekeeper settings. For more information, see Configuring the Built–in Gatekeeper.

When one or more of the conference participants is not on the LAN, and is connected to the conference via a Gateway, the available bandwidth is determined by factors such as the Gateway connection and audio transcoding capabilities.

Most videoconferencing terminals support varying bandwidths (video bit rates) and frame rates. To prevent videoconferencing terminals that support lower video bit and frame rates from receiving unsuitable quality video, you should set the service parameters according to the lowest video bit rates and frame rates supported. You can also set a Dynamic Bandwidth service, in which the MCU-323 adapts the bandwidth to the videoconferencing terminal with the lowest bandwidth capacity. See Defining Conferencing Services in Configuring the Unit for configuration information.
Summary of MCU-323 Features

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Coding</td>
<td>G.711 A/µ Law, G.723.1, G.729 A/B.</td>
</tr>
<tr>
<td>Video Coding</td>
<td>H.261 CIF and QCIF, H.263 CIF and QCIF.</td>
</tr>
<tr>
<td>LAN</td>
<td>10/100BASE-T Ethernet LAN UTP connection.</td>
</tr>
<tr>
<td>Bandwidth Support</td>
<td>- Supports dynamic bandwidth adjustment during a conference.</td>
</tr>
<tr>
<td></td>
<td>- Supports 768 Kbps high quality and 1.5 Mbps super-quality video sessions.</td>
</tr>
<tr>
<td>Audio Conferences</td>
<td>- Supports voice-only conferences.</td>
</tr>
<tr>
<td></td>
<td>- Includes audio mixing and voice–activated video switching.</td>
</tr>
<tr>
<td>Number Of Conference Participants</td>
<td>According to the conference type:</td>
</tr>
<tr>
<td></td>
<td>- 24 participants in a 64 Kbps voice only conference.</td>
</tr>
<tr>
<td></td>
<td>- 15 participants in a 110 Kbps multimedia conference.</td>
</tr>
<tr>
<td></td>
<td>- 9 participants in a 384 Kbps multimedia conference.</td>
</tr>
<tr>
<td></td>
<td>- 5 participants in a 768 Kbps multimedia conference.</td>
</tr>
<tr>
<td></td>
<td>- 3 participants in a 1.5 Mbps multimedia conference.</td>
</tr>
<tr>
<td>Video Modes</td>
<td>Voice–activated video switching plus configurable video switching modes:</td>
</tr>
<tr>
<td></td>
<td>- The speaker sees himself.</td>
</tr>
<tr>
<td></td>
<td>- The speaker sees the previous speaker.</td>
</tr>
<tr>
<td></td>
<td>- Lock onto one participant using Chair Control.</td>
</tr>
<tr>
<td>Continuous Presence</td>
<td>Allows you to view 4 conference participants simultaneously on the same screen by mixing 4 QCIF channels into one CIF stream.</td>
</tr>
<tr>
<td>Cascading</td>
<td>Supports merging several separate conferences to create very large conferences.</td>
</tr>
</tbody>
</table>
### Summary of MCU-323 Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Distributed Topology</strong></td>
<td>Distribution of up to 4 units to increase the number of concurrent conferences and the number of total available calls.</td>
</tr>
<tr>
<td><strong>Operational Advantages</strong></td>
<td>- Allows parties to view and/or listen without actively participating in a conference. &lt;br&gt; - Allows the linking of services to specific MPs. &lt;br&gt; - Operates without user intervention. No per-conference configuration is necessary.</td>
</tr>
<tr>
<td><strong>Web Monitoring and Control</strong></td>
<td>- Online monitoring and control of the conference using a web interface. &lt;br&gt; - Allows users to invite others to join the conference.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>- Password protection per conference to ensure privacy. &lt;br&gt; - Each unit is protected by a user configurable password.</td>
</tr>
<tr>
<td><strong>T.120 Sessions</strong></td>
<td>Enables T.120 data sharing sessions.</td>
</tr>
<tr>
<td><strong>Gatekeeper</strong></td>
<td>Built-in Gatekeeper functionality.</td>
</tr>
<tr>
<td><strong>Configuration</strong></td>
<td>Simple user-friendly configuration and setup. Configuration via the LAN port.</td>
</tr>
<tr>
<td><strong>Upgrades</strong></td>
<td>Supports field software upgrades.</td>
</tr>
</tbody>
</table>
### Summary of Built-in Gatekeeper Features

<table>
<thead>
<tr>
<th><strong>Address Translation</strong></th>
<th>Translates endpoint phone numbers or names (endpoint aliases) into IP addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admission</strong></td>
<td>Controls the terminal’s LAN and MCU-323 usage by controlling the following parameters:</td>
</tr>
<tr>
<td></td>
<td>- Bandwidth used by H.323 session in a zone.</td>
</tr>
<tr>
<td></td>
<td>- Bandwidth used by a single H.323 endpoint.</td>
</tr>
<tr>
<td></td>
<td>- The number of calls in a zone.</td>
</tr>
<tr>
<td></td>
<td>- The specific type of calls and other services a specific user can make or use.</td>
</tr>
<tr>
<td></td>
<td>- Defines maximum distance, multicast distance, neighbor distance and default distance.</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>Supports up to 100 endpoint registrations and 30 concurrent calls.</td>
</tr>
<tr>
<td><strong>Additional Call Services</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- <strong>Line Hunting</strong> – Provides call processing to locate an available Gateway for a user requesting a specific type of outside line.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Group Hunting</strong> – Allows single phone number or name description for a group of terminals.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Call Forwarding</strong> – Allows terminals to forward their calls to another terminal or Gateway.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Zone Management</strong> – Defines terminals that are part of a zone and their service privileges. Plug-and-play operation (factory set defaults) is possible.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Multiple Zone Operation</strong> – Allows a large network to be segmented into multiple zones, providing easy interconnection between the zones. Definition of zone prefixes is possible.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Call Routing</strong> – When informed of the network physical structure, provides optimal routing of calls to MCU-323s and other network services.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Proxy Support</strong> – Supports secured routing using the Cisco H.323 Proxy.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Multicast Gatekeeper Discovery</strong> – supports receiving multicast gatekeeper discovery messages.</td>
</tr>
</tbody>
</table>
Physical Description of the MCU-323

Front Panel

The front panel contains indicator LEDs and a Serial Port connector, as shown in Figure 1-6. The LED functions are described in the tables below. The asynchronous RS-232 serial port connects either to a terminal or to a modem.

![MCU-323 Front Panel](image)

*Figure 1-6 – MCU-323 Front Panel*

The four **Loaded** LEDs, at the center of the front panel, indicate the unit’s CPU load as outlined in the table below:

<table>
<thead>
<tr>
<th>LED State</th>
<th>CPU load range</th>
</tr>
</thead>
<tbody>
<tr>
<td>One flashing LED</td>
<td>Load in range 0-20%</td>
</tr>
<tr>
<td>One illuminated LED</td>
<td>Load in range 20-40%</td>
</tr>
<tr>
<td>Two illuminated LEDs</td>
<td>Load in range 40-60%</td>
</tr>
<tr>
<td>Three illuminated LEDs</td>
<td>Load in range 60-80%</td>
</tr>
<tr>
<td>Four illuminated LEDs</td>
<td>Load in range 80-100%</td>
</tr>
</tbody>
</table>

The remaining LEDs provide the following indications:

<table>
<thead>
<tr>
<th>LED</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN/Link</td>
<td>LAN activity and videoconferencing session activity on the LAN.</td>
</tr>
<tr>
<td>Function</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>Test</td>
<td>Test being performed at boot stage.</td>
</tr>
<tr>
<td>Power</td>
<td>Power ON when lit.</td>
</tr>
</tbody>
</table>
Rear Panel

The rear panel contains a LAN module port, the AC Power connector, and Power ON/OFF switch. The LAN port is a 10/100 Mbps 10/100Base-T IEEE 802.3 Ethernet connection.

*Figure 1-7 – MCU-323 Rear Panel*
Installing the MCU-323

To install the MCU-323 you need to:

☐ Prepare the site for installation
☐ Make cable connections to the MCU-323
☐ Mount the MCU-323 in a 19-inch rack
☐ Install the configuration software
Prepare the Site

- Before installing the MCU-323 unit, prepare the following
  - LAN port or hub to connect to the MCU-323.
  - All necessary cables.
  - A grounded AC power outlet.
  - Clearance of at least 10 cm (4 inches) behind the unit for interface cable connections.
  - Environmental conditions consisting of an operating temperature between 0°C and 40°C (32°F-104°F) and relative humidity between 15% and 85%, non-condensing.

Make Cable Connections

The following describes connecting the power and the LAN connection to the MCU-323. Refer to Overview for an illustration of the MCU-323 rear panel and its cable connections.

Connect the Power

The MCU-323 receives AC power through a standard power cable with a grounded three-prong plug. The wiring scheme is as follows:
- Brown lead Live (phase)
- Blue lead Neutral
- Green/yellow lead Earth ground

To connect power to the MCU-323

1. If your power cable was supplied without a plug, connect your local standard grounded power plug according to the wiring scheme above.
2. Connect the molded IEC socket of the power cable to the MCU-323 power connector at the right side of the rear panel.
3. Verify that the power On switch is in the Off (0) position.
4. Connect the three-prong power plug of the power cable to a grounded AC outlet.
Warning
Before connecting the MCU-323 to the power line, make sure the power source voltage matches the requirements of the unit, as marked below the power connector. Verify that the protective earth terminals of the MCU-323 are connected to a properly grounded power source. For additional important grounding information, see Safety Considerations.

Connect to the LAN

The MCU-323 supports a 10/100Base-T RJ-45 connection. The MCU-323 connects to a LAN segment via a direct connection to a hub.

LAN cables are not provided with the MCU-323. For proper performance, the LAN connection cable should not be longer than 15 meters. For pin–out information, see Cable Connectors. The LAN cable you use depends on the connection.

<table>
<thead>
<tr>
<th>To connect to</th>
<th>You need</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 10/100Base-T hub</td>
<td>A straight through Ethernet cable with RJ-45 connectors</td>
</tr>
</tbody>
</table>

➢ To connect to the LAN

- Connect the appropriate LAN cable to the LAN port at the rear of the MCU-323, and connect the other end of the cable to your local network connection or hub.
Mount the MCU-323 in a 19-inch Rack

You can install the MCU-323 in a standard 19-inch rack. Two mounting brackets are included in the package.

Figure 2-1 – Attaching Rack Mounting Brackets

➢ To rack-mount the MCU-323

1. Disconnect all cables, including the power cables, from the unit while installing the MCU-323 in the rack.

2. Each bracket has two screws and two flat washers to attach to the sides of the MCU-323. Pass the screws through the washers and brackets, inserting them into the screw holes on the sides of the unit.

3. Fasten the brackets to the side rails of the rack with four screws, two on each side. These screws are not included with the MCU-323.
Install the RADVision OnLAN Tools

The installation CD ROM included with your MCU-323 installs the OnLAN Configure 323 application, the Software Upload Utility, and product documentation.

To install the OnLAN Tools configuration software for the first time

1. Insert the supplied MCU-323 CD-ROM in your CD drive.

2. The RADVision OnLAN Tools Setup window displays. If it does not display automatically, access the CD ROM using Windows Explorer and invoke the Setup.exe file.

3. Select the MCU-323 in the Product Selection screen. Continue to follow the Setup program on-screen instructions.

4. When prompted to select the Setup Type, select one of the following:
   - Typical for a complete installation of all the OnLAN utilities.
   - Compact for the OnLAN Configure 323 only.
   - Custom to select the OnLAN utilities you wish to include.

The installation procedure creates the following directories and folders:

- A Start menu Program folder named RADVision OnLAN Tools, containing shortcuts to the OnLAN Configure 323 application, the Software Upload Utility, and product documentation.
- A directory named C:\Program Files\RADVision\RADVision OnLAN Tools.

Note
The directories described are the default installation directory settings. You can customize these settings during the installation procedure.
Preparing for Configuration

You configure the MCU-323 using the OnLAN Configure 323 application. Configuration includes:

- Invoking the OnLAN Configure 323 application
- Selecting an MCU-323 device to configure
- Entering a New IP Address for a New MCU-323
- Providing a password
- Selecting a configuration source
- Selecting the Unit Type
Invoking the OnLAN Configure 323 Application

➢ To initiate the OnLAN Configure 323 Application

1. From the Start | Programs menu, select the RADVision OnLAN Tools folder and click OnLAN Configure 323. The application displays a background screen, followed by the Select Unit screen, see Figure 3-1.

2. The OnLAN Configure 323 detects available devices on the local network segment, and displays them according to IP address and Unit Type in the Unit IP area of the Select Unit screen.

Figure 3-1 – Select Unit screen
Selecting an MCU-323 for Configuration

The first step in configuration is selecting an MCU-323 device on the LAN that you want to configure. When configuring more than one new unit, install and configure only one device at a time.

Unit IP (text box/list box) — Displays the unit IP address and type of all detected devices on the LAN.

Detect (button) — Click this button to restart the detection of devices on the local network segment.

Remote Configuration — The remote configuration option is reserved for future use.

➢ To select the OnLAN unit you want to configure

1. In the Select Unit screen, select the OnLAN device you want from the Unit IP list box.
2. Click Next. The Enter Password screen is displayed.
3. Enter the password for the unit and click Next. The Configuration Source screen is displayed.
   Your next steps are to determine the Unit Type, and configure either the built-in Gatekeeper or the MCU-323.

Entering a New IP Address for a New MCU-323

If there are no other RADVision units on the LAN, the first time you configure the MCU-323 the Unit IP text box and list box both appear empty. This is because new RADVision units have a default IP address not suited to your local network IP scheme. For the configuration software to detect a new unit, you must assign an IP address according to the IP addressing scheme of the network segment it is attached to.

You can change the IP address of a new unit from the Select Unit screen. Before you change the IP address of a new unit make sure that:

- The terminal running the configuration software resides on the same LAN segment as the new unit, and the terminal IP address matches the IP address of the network segment it is on.
- The new MCU-323 is the only new RADVision unit on the network. Turn off all other new RADVision units that don’t appear in the Select Unit screen before you proceed.
To change the IP address of a new MCU-323

1. Type the IP address you want to assign in the Unit IP text box. The LAN configuration station broadcasts the new IP address. The MCU-323 changes its IP address to the broadcast IP, and restarts with its new IP address and the Enter Password screen is displayed.

2. If you selected a unit from the Unit IP list, click Next to display the Enter Password screen.

Passwords

Once you select a unit to configure you must type in a password to access the Configuration Source screen and proceed with configuration.

New MCU-323 units leave the factory without a password. When configuring for the first time, leave this text box empty. The password can have a maximum of 16 characters and is case sensitive. The Key parameter is reserved for future use.

![Enter Password screen]

To proceed to the Configuration Source screen

1. Enter the password for the MCU-323 unit you wish to access. For first time configuration on a new unit, leave the password entry blank.

2. Click Next to proceed. The Configuration Source screen is displayed.
Preparing for Configuration

Changing the MCU-323 Password

![Change Password screen](image)

To change the unit configuration password

1. From the **Configuration Source** screen, click Change Password. The **Change Password** screen is displayed.

2. In the **Old Password** text box, type your current password. If this is the default password, leave this text box empty and click Tab.

3. In the **New Password** text box, type the new password.

4. In the **Confirm New Password** text box, type the new password again for verification.

5. Click **OK** to confirm. The **Configuration Source** screen is displayed again.

If you forget your password, contact RADVision Technical Support at HWsupport@tlv.radvision.com or OnLANsupport@radvision.com.
Selecting a Configuration Source

In the Configuration Source screen, you define the function of the MCU-323 or Unit Type, and enter the Unit Setup, Gatekeeper Setup, or Change Password dialogs used to configure the unit.

![Configuration Source screen](image)

**Figure 3-4 – Configuration Source screen**

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Proceed to ...</th>
<th>Using the ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the built-in Gatekeeper</td>
<td>Configure the Gatekeeper Setup <strong>first</strong></td>
<td>Gatekeeper Setup button</td>
</tr>
<tr>
<td>Use the MCU section only</td>
<td>Disable the built-in Gatekeeper and define a default (external) Gatekeeper as described below</td>
<td>Procedure outlined below, followed by the Unit Setup button</td>
</tr>
</tbody>
</table>
Preparing for Configuration

Note
To operate the unit as MCU-323 only you need to:

- Disable the built-in Gatekeeper, see *Disabling the Built-in Gatekeeper* in *Configuring the Built-in Gatekeeper* for instructions.
- Define an external gatekeeper as the default gatekeeper. See *Defining a Default Gatekeeper and Router in Configuring the Unit* for instructions.

The following parameters and options are available in the **Configuration Source** screen:

**Unit Type** (list box) — A drop-down list box that allows you to select the function mode for the MCU-323. The options are: **MCU**, **MCU Distributed**, and **MP Dedicated**.

**HW Version** — Displays the unit’s hardware version.

**SW Version** — Displays the first two digits of the unit software version. The ellipsis button displays a screen containing the full software version and related information.

**Change Password** (button) — Displays the *Change Password* screen. See *Changing the MCU-323 Password*.

**Source** (list box) — Displays the available stored configuration files for the MCU-323.

**Configure Gatekeeper** (button) — Displays the *Gatekeeper Setup* screen for configuring the built-in Gatekeeper of the unit.

**Unit Setup** (button) — Displays the *Unit Setup* screen for configuring the MCU-323 section of the unit.
Selecting the Unit Type and What You Want to Configure

➢ To set the unit function type

1. In the Configuration Source screen, select one of the function types displayed in the Unit Type drop down list:
   - MCU (Single Station MCU–323)
   - MCU Distributed (Distributed MCU–323)
   - MP Dedicated (Dedicated MP)

2. From the Source drop down list, select the configuration source file. If this is a first time configuration, select Current.

3. Click Unit Setup to access the multipoint conferencing unit configuration. Proceed to the chapter Configuring the Unit, and refer to the section corresponding to the Unit Type you selected for specific configuration instructions.
   OR
   Click Gatekeeper Setup to access the built-in Gatekeeper configuration. Proceed to the chapter Configuring the Built-in Gatekeeper for configuration instructions.
Configuring the Built–in Gatekeeper

You configure the Built–in Gatekeeper by accessing the Application Parameters screen and selecting one of the following configuration modules:

- Services Definition
- Zone Definition
- Neighbor Gatekeepers
- Network Topology
- Network Control

If you are working with an external gatekeeper or in the Distributed MCU-323 or Dedicated MP modes, skip this section and proceed to the chapter Configuring the Unit.
Accessing the Gatekeeper Configuration

➢ To begin Gatekeeper Setup

1. In the Configuration Source screen click Gatekeeper Setup. The Gatekeeper Application Parameters screen is displayed.

2. The Application Parameters screen contains five configuration modules. Use the table below as a guide to selecting the module you want to configure first.

3. After you complete setting an option, you will return to the Application Parameters screen.

4. Select another Gatekeeper option to configure, or click Exit to leave the Gatekeeper configuration and return to the Configuration Source screen.

The table below provides you with a guide to the configuration options.

![Application Parameters screen]

*Figure 4-1 – Application Parameters screen*
Configuring the Built-in Gatekeeper

<table>
<thead>
<tr>
<th>To...</th>
<th>Click the button...</th>
<th>For instructions refer to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Prefixes for available services</td>
<td>Services Definition</td>
<td>Services Definition</td>
</tr>
<tr>
<td>Define endpoints for the Gatekeeper zone</td>
<td>Zone Definition</td>
<td>Zone Definition</td>
</tr>
<tr>
<td>Define Neighbor Gatekeepers</td>
<td>Neighbor Gatekeepers</td>
<td>Neighbor Gatekeepers</td>
</tr>
<tr>
<td>Define Islands for routing purposes</td>
<td>Network Topology</td>
<td>Network Topology</td>
</tr>
<tr>
<td>Turn Gatekeeper On/Off, restore defaults, allow aliases, enable Gatekeeper call routing, set dynamic IP, set distance definitions</td>
<td>Network Control</td>
<td>Network Control</td>
</tr>
</tbody>
</table>

**Services Definition**

The Gatekeeper offers call services that enhance the normal call process by adding functions such as automatic call forwarding and/or routing. To do this, an added address tag or **Prefix** must be assigned for each service. A service is automatically accessed when the **Prefix** is added to the phone number dialed for a conference call.

**Forward Prefix** — You can define a prefix for the **Forward** service. When a terminal wishes to notify the Gatekeeper to forward its calls, it requests the **Forward** service using this prefix together with the new destination endpoint. Subsequently, when the Gatekeeper receives a call for that terminal, it transfers the call to the new endpoint until the terminal deactivates the **Forward** service request.

**Exit Zone** — When you define a prefix for the **Exit Zone** service, you need to dial that prefix to reach an endpoint in another zone. This is useful in restricting unauthorized users from making calls to other zones. When this service is defined, the Gatekeeper only completes calls to other zones if the **Exit Zone** prefix is present in the dialed address string.

**Zone Prefixes 1 and 2** — As the built-in Gatekeeper supports multiple zone environments, this service lets you define one or two **Prefixes** for each zone of the Gatekeeper. **Zone Prefixes** are similar to telephone area codes. If an endpoint in a zone dials a **Zone Prefix** before its number, and the Gatekeeper cannot resolve it in its zone, the Gatekeeper attempts to locate and route the call to the appropriate zone of the neighboring gatekeeper. On receiving the call, the built-in Gatekeeper strips off the **Zone Prefix** and applies a destination location mechanism to route the call to its final destination.
Even if two endpoints in two zones have an identical number, there is no ambiguity in telling them apart since the Zone Prefix preceding the number determines exactly which endpoint is being called.

When no Zone Prefixes are defined, the following call requests are accepted:

- Call requests to a service defined in the zone and allowed as Public.
- Calls to Online terminals in the zone.
- Calls to terminals marked as Forwarded in the zone.

*Figure 4-2 – Gatekeeper Services Definition Table screen*
To define a Forward Prefix, Zone Prefix or Exit Zone prefix for the Gatekeeper

1. In the Application Parameters screen click the Services Definition button. The Gatekeeper Services Definition Table is displayed.

2. Select the built-in service you want to define (Forward, Zone Prefix 1, Zone prefix 2 or Exit Zone), and click Edit. The Services Definition screen is displayed.

3. In the Prefix field enter the prefix for this service. The prefix can be up to 31 characters long. Valid characters are 0 through 9, pound (#), asterisk (*), and comma (,).

4. Specify the availability of the service. See the table below for service accessibility options.

5. Notify users that this service has been defined and is available.
Service Access Control

In the basic default configuration, all services are available to all endpoints by defining them both as Public and Default. This allows all endpoints to access the network services. You can restrict access to and distinguish between services by changing the service status to either Public or Default. The table below outlines your options for service access control.

<table>
<thead>
<tr>
<th>If you want to allow access to</th>
<th>Set the service to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only predefined endpoints inside the zone and all endpoints in other zones.</td>
<td>Public</td>
</tr>
<tr>
<td>All endpoints inside the zone.</td>
<td>Default</td>
</tr>
<tr>
<td>All endpoints.</td>
<td>Public and Default</td>
</tr>
</tbody>
</table>

Single Number Access to a Group of Terminals

To allow single number access to a group of terminals, you have to define these terminals as service providers.

➢ To define a terminal as a service provider you have to

1. Define the service in the Gatekeeper Services Definition Table.
2. Define the service prefix for the terminals in the group as an additional phone number.

➢ To define the service for the Gatekeeper

1. From the Gatekeeper Services Definition Table screen, click Add. The Services Definition screen is displayed.
2. In the Description text box, type a description for this service.
3. In the Prefix text box, type a prefix. Remember that prefixes can be up to 31 characters long and valid characters are 0 through 9 and pound (#), asterisk (*) and comma (,). It is advisable to set prefixes that do not begin with the same sub-strings as your terminal phone numbers, or else include one of ‘#’, ‘*’, ‘,’.
4. Check the Public and Default check boxes.
5. Click Ok. This service is added to the Services Definition Table.
Configuring the Built–in Gatekeeper

### Note
The prefixes you set in the **Service Definition Table** of the MCU-323 should match those set in the **Service Definition Table** of the Gatekeeper. See **Services Definition**.

- **To define the service prefix as an additional phone number**
  - If the terminal does not support the RAS protocol and has to be predefined, follow the steps in *Adding a New Endpoint* to redefine the endpoint or in *Editing Endpoint Settings* if the terminal is already predefined. Add the service prefix to the Phone Number text box.
  - If the terminal supports dynamic registration, you can either add the service to its configuration file or redefine it as you would a terminal that does not support the RAS protocol.

### Editing the Gatekeeper Default Services

You can edit the default services from the **Service Definition Table** screen.

- **To edit the default services**
  1. From the **Services Definition Table**, select the service you want to edit and click **Edit**. The **Services Definition** screen is displayed.
  2. In the **Services Definition** screen, make the required changes and click **Ok**.

### Deleting and Adding Gatekeeper Services

You are allowed to delete all services except for the default Gatekeeper services.

- **To delete a service from the Gatekeeper Services Definition Table**
  1. From the **Services Definition Table**, select the service you want to delete and click **Delete**.
  2. Click **Ok** or **Apply** for the configuration software to upload the change to the Gatekeeper.

- **To add a service to the Services Definition Table**
  1. From the **Services Definition Table** screen, click **Add**. The **Services Definition** screen is displayed.
  2. In the **Services Definition** screen, type a description and a prefix and set the access control **Default** and **Public** flags. Click **Ok**.

4-6
Saving the Service Definitions to a File

You can save the services you define in the Services Definition Table to a file. Services Definition Table data files are saved with an ‘*.srv’ file extension.

To save the Gatekeeper services to a file

1. From the Services Definition Table screen, click Save. The Save As dialog box is displayed.
2. From the Folders list box, select the folder in which you want to save this file. By default, this is the same directory in which you installed the configuration software.
3. In the File name text box enter a file name. *.srv is the default file extension for service files. Click Ok.

Note
You can save to files the data collected in any of the Gatekeeper Setup screens. The data from each screen is saved to a file with a different file extension indicating the type of parameter that was saved. For example, *.srv for Services, *.zon for Zone settings, *.nbr for Neighbor Gatekeeper parameters, etc.
Zone Definition

An H.323 Zone is a logical collection of terminals, gateways, and multiple point control units managed by a single gatekeeper. You can predefine the endpoints in a Zone using the Zone Definition options.

Zone Access Control

The RADVision Gatekeeper can operate in one of two modes: Open Zone and Strict Zone, giving you the choice to control endpoint access to the zone.

In an Open Zone mode, the gatekeeper accepts registration from all endpoints for which this gatekeeper is defined as the default gatekeeper. This mode allows “plug-and-play” endpoint additions to the network, but does not give you full access control over the zone.

To configure the Gatekeeper to operate in Open Zone mode

1. In the Application Parameters screen, click Network Control. The Network Control screen is displayed.
2. Make sure the Everyone can register option is selected. Click Ok to confirm.

In a Strict Zone mode the gatekeeper only accepts registration from predefined endpoints. This mode does not allow “plug-and-play” endpoint additions to the network, as you have to predefine any endpoints you want to add. Operating in a Strict Zone mode gives you full access control over the zone.

Note
For information on network control parameters, see Network Control.

To configure the Gatekeeper to operate in a Strict Zone mode

1. In the Application Parameters screen click Network Control. The Network Control screen is displayed.
2. Clear the Everyone can Register option. Click Ok.
3. Predefine all endpoints for which you want to allow registration to the Gatekeeper. For details, see Adding a New Endpoint.
In addition to controlling endpoint access to a zone, predefining endpoints with the Gatekeeper is necessary when registering endpoints that do not support dynamic registration. Only endpoints that support the RAS protocol can dynamically register with the Gatekeeper. Some endpoints may not support the RAS protocol and must be predefined with the Gatekeeper.

In both the strict zone and open zone modes, endpoint registration can be static or dynamic. Although the strict zone mode of operation only accepts registration from predefined endpoints they can also register dynamically.

The Zone Definition Table displays both predefined endpoints and online endpoints that are not predefined. The Zone Definition Table allows you to:

- Add predefined endpoints.
- Edit predefined and online endpoint properties.
- View predefined and online endpoint properties.
- Delete an endpoint.
- Save settings and load previously saved settings.

While the Zone Definition Table screen is open, endpoints cannot register dynamically with the Gatekeeper. To allow new registrations, exit the Zone Definition Table as soon as you complete configuring the Zones.
Configuring the Built-in Gatekeeper

- To display the Zone Definition Table
  - In the Application Parameters screen click Zone Definition. The Zone Definition Table is displayed.

![Zone Definition Table](image)

**Figure 4-4 – Zone Definition table**

The following parameters and settings are displayed in the Zone Definition Table:

- **Number of Entries** — Displays the number of endpoints defined in the current zone. When you add or delete an endpoint, this counter updates automatically (read only).

- **Max Entries** — Displays the maximum number of endpoints that can be registered with the current Gatekeeper. Currently the maximum number is 100 (read only).

- **Unit Type** — The type of unit that is registered with the Gatekeeper.

- **Terminal ID** — The endpoint identities on the IP network. Together with the endpoint phone numbers, they are the endpoint aliases.

- **IP Address** — The IP address of this endpoint.

- **Phone Num.** — The phone number of this endpoint on the IP network. An endpoint may have more than one phone number assigned to it.
**Status** — Indicates the designated status of the endpoint. The status of the endpoint can be one or more of the following:

- **predef** — The endpoint has been predefined. All predefined endpoints can make calls. To receive calls predefined endpoints that do not support the RAS protocol also have to be defined as Online Always, and predefined endpoints that support the RAS protocol have to be online.

- **online** — The endpoint is currently dynamically registered with the Gatekeeper. When a predefined endpoint is online (dynamic registration) its status is online & predef.

- **always** — The predefined endpoint is defined as Online Always. Predefined endpoints that do not support the RAS protocol and cannot dynamically register with the Gatekeeper have to be defined as Online Always to be able to receive calls. The status of such an endpoint is always & predef.
Adding a New Endpoint

To add a new endpoint to the Zone Definition Table

- From the Zone Definition Table screen, click Add. The Predefined Properties screen is displayed:

![Predefined Properties screen](image)

**Figure 4-5 – Predefined Properties screen**

The Predefined Properties screen allows you to define the registration properties for an endpoint. The following are the available parameters and settings:

**Predefined** – If you are editing a predefined endpoint this box is automatically selected.

**Online** – If you are editing a predefined endpoint that has dynamically registered with the Gatekeeper, this box is automatically selected.
Zone Definition

**Unit Type** – The type of unit you are defining. Unit types include: **Terminal**, **Gateway**, **MCU** and **Undefined**. The Gatekeeper allows dynamic registration of a predefined endpoint only when it corresponds to the **Unit Type** you set. If you are not sure what type of endpoint you are predefining, choose **Undefined**.

**Max. Distance** – The logical distance outside this zone that the Gatekeeper allows this endpoint to call. To inactivate, set to 0. For details on setting the distance parameters, see **Distance Settings**.

**Registration IP** – This is the address through which the endpoint receives Registration Admission Status (RAS) messages from the Gatekeeper. This field must be filled.

**Port** – This is the port number for this H.323 endpoint. The IP address together with the port number form the socket that is the communication link between the endpoint and the Gatekeeper. If this is the only endpoint running on the terminal you can leave the port number set to zero. If two or more endpoints are running on the same terminal, you must enter a different number for each port.

**Terminal IDs and Phone Numbers** – These are the aliases you assign to the endpoint. You can enter up to five different IDs and five different Phone Numbers. Aliases should be unique for endpoints in a zone, unless **Zone Prefixes** are defined. For details on setting **Zone Prefixes**, see **Services Definition**. Additional phone numbers can be identical.

**Allowed Services** – Displays the **Allowed Services** screen, where you can define endpoint access to services defined for the Gatekeeper.

---

**Defining the Properties of a New Endpoint**

1. **To define properties for a new endpoint**
   1. In the **Predefined Properties** screen, select the type of endpoint you are adding from the Unit Type drop down list.
   2. Enter the **Max. Distance** if you want to set distance limitations (between 0 and 255) in a multiple zone environment for this endpoint.
   3. If the endpoint you are defining cannot register dynamically with the Gatekeeper, select the **Online Always** check box.
   4. Enter the IP address of the endpoint in the **Registration IP** field.
   5. Enter the port number of the endpoint in the **Port** field if necessary.
   6. Enter the IDs and phone numbers you want to assign to this endpoint in the corresponding fields.

   If the endpoint supports dynamic registration, you have to enable the Gatekeeper to add the predefined properties to the registration data. Otherwise, no calls are forwarded to the
predefined aliases. This is done by selecting the **Alias Assignment** check box in the Gatekeeper **Network Control** screen. See **Alias Assignment in Network Control**.

You can set the **Alias Assignment** parameter when you finish predefining all endpoints. See **Alias Assignment**.

**Specifying Allowed Services**

You can define which of the services defined for the Gatekeeper this endpoint can use. By default, a new endpoint is allowed to use all services defined for the Gatekeeper.

![Allowed Services](image)

**Figure 4-6 – Allowed Services screen**

- **To define Allowed Services for an endpoint**
  1. From the **Predefined Properties** screen, click **Allowed Services**. The **Allowed Services** screen is displayed.
  2. Select the service you want or do not want this endpoint to use and click **Enable/Disable** to enable or disable that service.
3. Click Ok to confirm and return to the Predefined Properties screen. You have finished predefining this endpoint. Predefine other endpoints or exit the Zone Definition Table by clicking Ok.

Note
When the Zone Definition Table screen is open, endpoints cannot register dynamically with the Gatekeeper. To allow new registrations, exit the Zone Definition Table screen as soon as you complete the settings.

Predefining Endpoints in a Dynamic IP Environment
In a dynamic IP mode the endpoint does not have a fixed IP address, and the Gatekeeper identifies the endpoint according to its aliases. To work in a dynamic IP environment you have to check the Dynamic IP Environment check box in the Network Control screen. Even if a dynamic IP environment does not govern your network, you can benefit from this feature and allow users to migrate between workstations. Since the Gatekeeper identifies the endpoint by alias and not IP address, users can switch workstations without worrying about not receiving their calls. See Network Control for details about working in a dynamic IP environment.

➢ To predefine an endpoint in a dynamic IP environment

1. In the Application Parameters screen, click Network Control. The Network Control screen is displayed.

2. Check the Dynamic IP Environment check box. Click Ok.

3. In the Application Parameters screen, click Zone Definition. The Zone Definition Table screen is displayed.

4. Click Add. The Predefined Properties screen is displayed. Follow the steps as for Defining the Properties of a New Endpoint with the following exceptions:

- You can enter any number in the IP Registration field.
- Define at least one unique terminal ID or phone number.

Note
If this endpoint can dynamically register with the Gatekeeper, at least one of the aliases you define should correspond to one of the online aliases. Otherwise, the Gatekeeper cannot match the predefined properties to the endpoint.
Editing Endpoint Settings

The **Edit** button allows you to:

- **Edit** the properties of a predefined endpoint.
- **Add** predefined properties to an online endpoint.
- View the properties of predefined and online endpoints.

➢ **To edit or view the properties of a predefined endpoint**

1. From the **Zone Definition Table**, select the predefined endpoint you want to edit and click **Edit**. The **Predefined Properties** screen is displayed.
2. Make the necessary changes/additions and click **Ok**.

➢ **To view the properties of an online endpoint**

- From the **Zone Definition Table**, select the online endpoint whose properties you want to view, and click **Edit**. The **Online Properties** screen displays the endpoint registration data.
The following parameters and settings are displayed in the **Online Properties** screen:

**Registration IP and Port** — This is the IP address with which the endpoint registered to the Gatekeeper. Together with the Port, it forms the socket through which the endpoint receives RAS messages from the Gatekeeper.

**Call Signaling IP and Port** — These are the sockets through which the endpoint expects to get call signaling messages from the Gatekeeper.

**Terminal IDs and Phone Numbers** — These are the IDs and phone numbers that identify the endpoint on the network.

**Forward** — Displays the forwarding information if the endpoint is using the Forward service to forward calls to another endpoint or terminal on the WAN. The following information is displayed:
- **Always** — The type of forwarding service. In this version only Always is available.
- **Phone Num.** — The destination phone number.
- **2nd** — The second destination phone number when forwarding 2B calls through the Gateway to a terminal on the WAN.
- **Terminal ID** — The destination ID.

**Supported Services** — Displays the **Supported Services** screen (See *Figure 4-8*). This read-only screen displays the description and prefix of services provided by the endpoint to other endpoints.

**Make Predefined/Predefined Parameters** – Displays the **Predefined Properties** screen (as discussed in *Adding a New Endpoint*) allowing you to predefine properties for the online endpoint.

![Supported Services screen](image)

*Figure 4-8 – Supported Services screen for a Gateway*
Adding Predefined Properties to an Online Endpoint

➢ To add predefined properties to an online endpoint

1. Click Make Predefined. The Predefined Properties screen is displayed (see Figure 4-5) including the online registration data of the endpoint.

2. Make the necessary additions to the Predefined Properties fields. Refer to Adding a New Endpoint for a description of the available parameters.

3. Click Allowed Services (in the Predefined Properties screen) if you want to enable or disable any services for this endpoint. Refer to Specifying Allowed Services for procedures and parameter definitions.

4. Click Ok to confirm the changes. Return to the Zone Definition Table. Click Ok to exit the Zone Definition Table.

5. From the Application Parameters screen click Network Control. The Network Control screen is displayed.

6. In the Network Control screen, make sure the Alias Assignment box is selected. The next time this endpoint registers dynamically with the Gatekeeper, the predefined properties you added will be displayed in the Online Properties screen and you can place calls to these phone numbers and IDs.

Deleting an Endpoint

You can delete endpoints from the Zone Definition Table. Deleted endpoints cannot make or receive calls unless they re-register with the Gatekeeper. You may want to delete endpoints from the Zone Definition Table in the following cases:

- You want to unregister an endpoint that cannot dynamically register with the Gatekeeper, such as NetMeeting.

- You want to unregister an endpoint that disconnected from the network in a disorderly manner after registration, and still appears in the Zone Definition Table.

➢ To delete an endpoint from the Zone Definition Table

• Select the endpoint you want to delete, click Delete. The endpoint is deleted from the Zone Definition Table and is unregistered from the Gatekeeper.

Note
If you want to re-register a deleted endpoint that supports dynamic registration, you have to close the Zone Definition Table screen first.
Saving or Loading Settings of the Zone Definition Table

You can save the settings you define in the Zone Definition Table to a file. This is useful to prevent all Gatekeeper data being lost when the Gatekeeper is unexpectedly shut off. Zone Definition Table data files are saved with an ‘*.nbr’ file extension.

➢ To save the data defined in the Zone Definition Table to a file

1. From the Zone Definition Table screen, click Save. The Save As dialog box is displayed.
2. From the Folders list box select the folder in which you want to save this file. By default this is the same directory in which you installed the configuration software.
3. In the File name field enter a file name. *.zon is the default file extension for the Zone Definition Table. Click Ok to confirm.

You can load data files to the Zone Definition Table. These are files that you have previously saved, and include properties you predefined for endpoints.

➢ To load a data file to the Zone Definition Table

1. From the Zone Definition Table screen, click Load. The Open dialog box is displayed.
2. From the File name list box select the file you want to load and click Ok. The file is loaded to the Zone Definition Table.
Neighbor Gatekeepers

For gatekeepers to direct calls to and from endpoints in other zones they have to be able to communicate with the gatekeepers in the other zones. The RADVision Gatekeeper can communicate with other gatekeepers if you define these gatekeepers as Neighbors.

The Neighbor Gatekeepers option in the Gatekeeper Setup allows you to specify the IP addresses of gatekeepers in other zones. You need to build a table that defines all neighboring gatekeepers that the current Gatekeeper can access through IP Unicast. When a call is directed to another zone, the Gatekeeper uses Neighbor Gatekeepers definitions to resolve the destination IP address.

**Note**
It is important to define all other known gatekeepers in the network as Neighbors to allow calls from the current gatekeeper zone to reach their zones.
To display the Neighbor Gatekeepers Table

- In the Application Parameters screen click Neighbor Gatekeepers. The Neighbor Gatekeepers Table is displayed.

![Neighbor Gatekeepers Table screen](image)

The Neighbor Gatekeepers Table screen displays the following parameters and settings:

**Number of Entries** — Displays the number of neighbors defined for the Gatekeeper. When you add or delete a neighbor, this counter updates automatically.

**Max Entries** — Displays the maximum number of neighbors that can be registered with the current Gatekeeper. Currently, the maximum number is 50.

**Description** — This is the description of the Neighbor Gatekeeper. To enable Proxy support, the word "proxy" must be entered as the description, see Gatekeeper Proxy Support for more information.

**Neighbor IP** — The IP address of this Neighbor Gatekeeper. This field is mandatory.

**Port** — The port number of this Neighbor Gatekeeper.
Prefix — The prefix required, when it has been defined, to call an endpoint in a neighboring gatekeeper zone (see Services Definition).

Distance — A designation between 0 and 255 representing the logical distance from the current Gatekeeper to the neighbor gatekeeper. For details on defining Distance parameters see Distance Settings.

The buttons in the Neighbor Gatekeepers Table screen allow you to Add a new neighbor definition, Edit or Delete a neighbor definition, Save and Load setting files.

Adding a New Neighbor Gatekeeper

To add a new Neighbor Gatekeeper to the Neighbor Gatekeepers Table

1. From the Neighbor Gatekeepers Table screen, click Add. The Neighbor GK Parameters screen is displayed.
2. In the Neighbor IP field enter the IP address of the Neighbor Gatekeeper.
3. In the Neighbor Port text box, specify the RAS port of the Neighbor Gatekeeper. The default port for the built-in Gatekeeper is 1719.

Figure 4-10 – Neighbor GK Parameters screen
4. In the Neighbor Prefix text box, enter the Zone Prefix if one is defined for this Neighbor Gatekeeper. For details on defining Zone Prefixes, see Services.

5. In the Distance field enter the logical distance (between 0 and 255) between the gatekeeper you are defining and the current gatekeeper. This value is compared to the Max.Distance or Default Distance parameters of endpoints to determine whether they can route calls to this zone. Setting this parameter is optional.

6. In the Description field enter an identifying description for the Neighbor Gatekeeper. To enable Proxy support you must enter the word "proxy" as the description.

7. Click Ok to add this gatekeeper to the Neighbor Gatekeepers Table.

Editing Neighbor Gatekeeper Settings

➢ To edit the parameters of a Neighbor Gatekeeper

1. Select the Neighbor Gatekeeper you want to edit and click Edit. The Neighbor GK Parameters screen is displayed.

2. Make the changes, and then click Ok to confirm and return to the Neighbor Gatekeepers Table screen.

Deleting a Neighbor Gatekeeper

➢ To delete a gatekeeper from the Neighbor Gatekeepers Table

- Select the Neighbor Gatekeeper you want to delete and click Delete. The selected gatekeeper is deleted from the Neighbor Gatekeepers Table and the current Gatekeeper will not be able to route calls to endpoints in that zone.

Saving and Loading Neighbor Gatekeepers Table Settings

You can save the data you define in the Neighbor Gatekeepers Table to a file. This is useful to prevent all Gatekeeper data from being lost when the Gatekeeper is unexpectedly shut off. Neighbor Gatekeepers Table data files are saved with an "*.nbr" file extension.

➢ To save Neighbor Gatekeepers Table settings to a file

1. From the Neighbor Gatekeepers Table screen, click Save. The Save As dialog box is displayed.
2. From the **Folders** list box select the folder in which you want to save this file. By default, this is the same directory in which you installed the configuration software.

3. In the **File name** field enter a file name. "*.nbr" is the default file extension for the **Zone Definition Table**. Click **Ok** to confirm.

   You can load data files to the **Neighbor Gatekeepers Table**. These are files that you have previously saved, and include properties you predefined for endpoints.

   ➢ **To load a data file to the Neighbor Gatekeepers Table**

      1. From the **Neighbor Gatekeepers Table** screen, click **Load**. The **Open** dialog box is displayed.

      2. From the **File name** list box select the file you want to load and click **Ok**. The file is loaded to the **Neighbor Gatekeepers Table**.
Network Topology

The Network Topology screen allows you to define clusters of IP subnets for the Gatekeeper that are characterized by homogenous and fast videoconferencing LAN connectivity. These IP clusters are called Islands, and they enable the built-in Gatekeeper to direct calls through the best routes, avoiding slow connections or bottlenecks. If you use an Island scheme, the built-in Gatekeeper routes service calls first to the gateway or endpoints that provide the service and belong to the same Island, and then to other Islands. This ensures that the call is directed over the fastest available channel.

You define Islands for the Gatekeeper by grouping defined subnets under the same Island Code. Each Island must consist of at least one subnet.

The Network Topology Table allows you to define, view, edit and delete Islands for the Gatekeeper. You can also save the Island definitions to a file.
To display the Network Topology Table

- In the Gatekeeper Application Parameters screen, click Network Topology. The Network Topology Table is displayed.

![Figure 4-11 – Network Topology Table screen]

The following parameters and settings are displayed in the Network Topology Table:

**Number of Entries** — Displays the number of Islands defined for the Gatekeeper. When you add or delete an Island, this counter updates automatically (read only).

**Max Entries** — Displays the maximum number of islands that can be defined for the current Gatekeeper. Currently the maximum number is 50 (read only).

**Description** — A description of the subnet.

**Subnet IP** — The IP address of this subnet.

**Subnet Mask** — The IP mask that you can apply to an IP address to test if it belongs to this subnet.

**Island Code** — The identifying code for all subnets belonging to one Island. Values are between 0 and 255.
Adding a New Subnet Address

![Subnet Parameters screen]

To add a new subnet address to the Network Topology Table

1. From the Network Topology Table screen, click Add. The Subnet Parameters screen is displayed.
2. In the Subnet IP field enter the IP address of this subnet.
3. In the Subnet Mask field enter the IP mask for this subnet.
4. In the Island Code field enter the identifying code of the Island that this subnet belongs to (values between 0 and 255).
5. In the Description field enter a description for this subnet.
Editing Subnet Setting

You can view and edit subnet settings.

➢ To edit the subnet settings
1. Select the subnet you want to edit and click Edit. The Subnet Parameters screen is displayed.
2. Make the changes and then click Ok to confirm and return to the Network Topology Table.

Deleting a Subnet Setting

➢ To delete a subnet setting from the Network Topology Table
• Select the subnet you want to delete and click Delete. The selected subnet setting is deleted from the Network Topology Table.

Saving or Loading Network Topology Table Settings

You can save the settings you define in the Network Topology Table to a file. Network Topology Table data files are saved with a ‘*.tpl’ file extension.

➢ To save the settings defined in the Network Topology Table to a file
1. From the Network Topology Table screen, click Save. The Save As dialog box is displayed.
2. From the Folders list box select the folder in which you want to save this file. By default this is the same directory in which you installed the configuration software.
3. In the File name field enter a file name. ”*.tpl” is the default file extension for the Network Topology Table. Click Ok to confirm.

You can load data files to the Network Topology Table. These are files that you have previously saved, and include properties you predefined for endpoints.

➢ To load a data file to the Network Topology Table
1. From the Network Topology Table screen, click Load. The Open dialog box is displayed.
2. From the File name list box select the file you want to load and click Ok. The file is loaded to the Network Topology Table.

Network Control

The Network Control screen allows you to configure additional parameters such as disabling the built-in Gatekeeper, characterizing endpoint registration, call management and bandwidth control. The Network Control option also displays details concerning ongoing calls, online endpoints and H.323 bandwidth usage.

➢ To display the Network Control Table

- In the Application Parameters screen click Network Control. The Network Control screen is displayed.

![Network Control Screen](image)

*Figure 4-13 – Network Control screen*
The **Network Control** screen contains the following areas, as described below:

- **Read only parameters**
- **Registration policy options**
- **Built-in Gatekeeper settings**
- **Network Resources used by H.323 traffic**
- **Miscellaneous Network Control settings**

The **Network Control** screen displays the following read only parameters:

**Ongoing Calls** — Displays the number of currently ongoing calls in the zone.

**Online Endpoints** — Displays the number of endpoints currently registered with the Gatekeeper.

**Current Bandwidth Usage** — Displays the bandwidth being used by H.323 calls in the zone.

The following are the configurable registration policy settings:

**Everyone Can Register** — Determines whether endpoints not defined in the Zone Definition Table can register with the Gatekeeper. When selected, all endpoints can register with the Gatekeeper. See **Zone Definition** for details on defining zones.

**Alias Assignment** — Set this option for the Gatekeeper to assign predefined aliases to the endpoint. Otherwise, you can only place calls to the aliases declared in the registration request and not to the predefined aliases. You can, however, place calls to aliases of a predefined endpoint that is defined as **Online Always**. See **Adding a New Endpoint** for details on predefining endpoints.

**Call Indirect** — Set this option to force all calls to be routed by the Gatekeeper. Indirect call mode provides call control functions as well as routing information. Calls requesting services are routed through the Gatekeeper regardless of this parameter. When disabled, calls are routed directly or via a Proxy. See **Gatekeeper Proxy Support** for more information.

**Dynamic IP Environment** — You can set the Gatekeeper to work in a dynamic IP environment. In a dynamic IP environment, terminals get different IP addresses at each start up. Because the terminal IP is not fixed, the Gatekeeper cannot identify the terminal by its IP address, and therefore uses terminal aliases for identification.

If your network is not governed by DHCP, you can use the dynamic IP environment support to allow user migration between workstations without the need to forward calls. When this option is set, the Gatekeeper allows H.323 endpoints that have registered with an IP address to re-register using a different IP address but having the same terminal IDs and phone numbers. Calls to an endpoint with a changed IP address are routed to the last registered IP address. See **Predefining Endpoints in a Dynamic IP Environment** for details.
The following are the configurable built–in Gatekeeper Settings:

**GK On** — This option allows you to enable or disable the built–in Gatekeeper. If you want to work with an external gatekeeper, clear this check box. If you are working with the built–in Gatekeeper, clearing this check box will disconnect all calls and unregister all terminals. The **Accept Registration/Unregister All** and the **Accept Calls/Disconnect All** buttons allow you to close down the Gatekeeper function in an orderly manner.

**Accept Registration/Unregister All** — The **Accept Registration** option is normally selected to allow endpoint registration to the Gatekeeper. If you want to close down the Gatekeeper, you can clear this option to prevent new dynamic registrations from endpoints. The **Unregister All** button unregisters all endpoints that remain registered.

**Accept Calls/Disconnect All** — The **Accept Calls** option is normally selected to enable the Gatekeeper to receive calls. If you want to close down the Gatekeeper, you can clear this option to prevent the Gatekeeper from accepting new calls. The **Disconnect All** button disconnects all calls that remain connected.

**Use Proxy for Unknown Zones** — This option forces routing of incoming traffic from zones of unknown gatekeepers through the Proxy. For more information on the Proxy, see Supporting the H.323 Proxy.

**Unregistration Timeout** — This is the maximum length of time (in hours) that an endpoint can remain inactive before its dynamic registration expires.

The following parameters allow you to control the network resources used by H.323 traffic:

**Max. Number of Calls** — The maximum number of simultaneous calls allowed in a zone. The Gatekeeper can support up to 30 simultaneous calls. The default is 25. The Gatekeeper will reject a new call if the number of ongoing calls reaches the value set for this parameter.

**Max. Total Bandwidth** — This parameter determines the total amount of bandwidth that can be supported by the Gatekeeper at any given time.

**Max. Bandwidth per Terminal** — The maximum bandwidth use allowed per terminal. This parameter applies to terminals only, and not to other endpoints such as gateways or MCU-323s.

The following are miscellaneous Network Control settings:

**GK Identifier** — This is the name of the local Gatekeeper. Terminals identify the Gatekeeper by this name during the discovery process. The Gatekeeper only responds to discovery requests that contain either its identifier or no identifier. The default name is RVGK.

**Discovery Multicast** — Use this to discover the gatekeeper using multicasting by entering the IP address and port of the multicast channel (defaults are displayed).

**Advanced Settings** — This button displays the Advanced Settings screen that consists of three parameters, listed below and shown in Figure 4-14.
- **Default Distance** — This is a designation (between 0 and 255) determining the logical distance that the Gatekeeper is allowed to route out of zone call requests from dynamically registered endpoints. The Default Distance is compared with the Neighbor Distance of the destination endpoint zone. Only if it is the same as or greater than the Neighbor Distance, is the call completed. For more information, see *Distance Settings*.

- **Multicast Distance** — This is a designation (between 0 and 255) determining the logical distance outside the zone that the Gatekeeper can route a call using multicast. For more information, see *Distance Settings*.

- **Unresponsive Timeout** — Determines how long the Gatekeeper waits for an endpoint to respond following a Gatekeeper status inquiry. The Gatekeeper makes four status inquiry attempts before deciding that the endpoint is no longer available. Once the Unresponsive Timeout interval passes without a response, the Gatekeeper unregisters the endpoint from Online status, and the endpoint is unable to receive calls.

**Factory Defaults** — This button resets the Gatekeeper parameters to the factory configuration. It deletes configuration changes you made including settings concerning endpoints, neighbors, topology and services. It also disconnects all calls and resets the MCU-323. Use with care!

![Advanced Settings screen](image)

*Figure 4-14 – Advanced Settings screen*
Disabling the Built–in Gatekeeper

The built–in Gatekeeper is enabled by default. If you decide to work with an external gatekeeper, you must disable the built–in Gatekeeper for this MCU-323.

➢ To disable the Built–in Gatekeeper

1. From the Network Control screen, clear the Accept Registration and Accept Calls check boxes. The Gatekeeper will not accept any dynamic registrations or call requests. Use the Ongoing Calls and Online Endpoints counters to monitor the number of calls and registered endpoints.

2. If the Ongoing Calls and Online Endpoints counters do not drop to 0, click the Unregister All and Disconnect All buttons to unregister any remaining endpoints and disconnect any ongoing calls.

3. Clear the GK On check box. You are prompted to confirm this action. You will lose all Gatekeeper configuration settings that you have not saved to a file. When you confirm, the built–in Gatekeeper is inactivated.

Note
Endpoints may remain online if they are disconnected from the network in a disorderly manner. In this case, Online Endpoints and Ongoing Calls will continue showing activity. The same occurs if such an endpoint registered forwarding information. In this case, disable the Gatekeeper by clearing the GK On parameter.

Alias Assignment

If the endpoint supports dynamic registration, you have to enable the Gatekeeper to add the registration data to the predefined properties. Otherwise, no calls are forwarded to the predefined aliases.

➢ To enable the Gatekeeper to add endpoint registration data to predefined properties

- In the Network Control screen, select the Alias Assignment check box and click Ok. You can now make a call to predefined aliases of dynamically registered endpoints.
Distance Settings

Distance settings give you control over endpoint dialing options between zones. Distance settings are arbitrary numbers that are chosen by you to designate a "logical distance" that defines the access rights between zones for different endpoints in relation to an origin point such as a particular gateway. There are four parameters for distance settings, which are interconnected but are accessed from different configuration screens:

- **Neighbor Distance** — Access this parameter from the Neighbor Gatekeepers screen.
- **Max. Distance** — Access this parameter from the Zone Definition screen.
- **Default Distance** — Access this parameter from the Network Control screen.
- **Multicast Distance** — Access this parameter from the Network Control screen.

The following are descriptions of the Distance settings parameters:

**Neighbor Distance** — Determines the logical distance between zones. When you define neighbor gatekeepers, you can define a logical distance between them. When you set a value for this parameter, you also have to set the Max. Distance and Default Distance parameters for endpoints in this zone to be able to dial to endpoints in the neighbor gatekeeper zone.

**Max. Distance** — Determines how far outside the zone this endpoint can make a call. For example, if an endpoint Max. Distance is set to 50 and it makes a call request to a zone that you have defined as a neighbor gatekeeper with a Neighbor Distance of 100, the call is rejected.

**Default Distance** — This is the equivalent of the Max. Distance parameter for online endpoints that do not have predefined properties.

**Multicast Distance** — This is a logical distance determining how far outside the zone the gatekeeper can route a call using multicast.

To set distance settings for a zone

1. From the Application Parameters screen, click Neighbor Gatekeepers. The Neighbor Gatekeepers Table is displayed.
2. Click Add to define a new neighbor gatekeeper, or click Edit to edit one already defined. The Neighbor GK Parameters screen is displayed. See Adding a New Neighbor Gatekeeper.
3. In the Neighbor Distance field enter a number between 0 and 255. Click Ok to confirm.
4. From the Application Parameters screen, click Zone Definition. The Zone Definition Table is displayed.
5. Click **Add** to define a new endpoint, or click **Edit** to edit an existing one. The **Predefined Properties** screen is displayed. If the endpoint is online and you want to set predefined properties for it, from the **Online Properties** screen that is displayed click **Make Predefined** to access the **Predefined Properties** screen. See **Adding a New Endpoint**.

6. In the **Max. Distance** field enter a number between 0 and 255. The number you enter will depend on whether you want to allow this endpoint to make call requests to the zone for which you defined a **Neighbor Distance**. Click **Ok** to confirm. Repeat steps 7 and 8 for all predefined endpoints and online endpoints with predefined properties.

7. From the **Application Parameters** screen click **Network Control**. The **Network Control** screen is displayed.

8. Click **Advanced Settings**. The **Advanced Settings** screen is displayed. (see Figure 4-14). In the **Default Distance** text box, enter a number between 0 and 255. This number depends on which zones you want to allow dynamically registered endpoints to make call requests to. For example, if you set it to 50, all dynamically registered endpoints can make calls to the zone for which you defined a distance of 50 or greater.

9. Click **Ok** to confirm.

### Saving or Loading Network Control Settings

You can save the **Network Control** settings to a file. This is useful to prevent all Gatekeeper data from being lost when the Gatekeeper is unexpectedly shut off. **Network Control** settings files are saved with an **'*ctr'** file extension.

- **To save the Network Control Settings to a file**
  1. From the **Network Control** screen, click **Save**. The **Save As** dialog box is displayed.
  2. From the **Folders** list box select the folder in which you want to save this file. By default this is the same directory in which you installed the configuration software.
  3. In the **File name** field enter a file name. '*ctr' is the default file extension for the Network Control settings. Click **Ok** to confirm.

- **To load a data file to the Network Control settings**
  1. From the **Network Control** screen, click **Load**. The **Open** dialog box is displayed.
  2. From the **File name** list box select the file you want to load and click **Ok**. The file is loaded to the **Network Control** settings.
Supporting the H.323 Proxy

This chapter describes how to configure the MCU-323 to support the Cisco H.323 Proxy. It covers the following topics:

- The H.323 Proxy
- Proxy Facilitated Call Flow
- Configuring Proxy support
The H.323 Proxy

The Cisco H.323 Proxy is a device that acts like a gateway and relays H.323 data between H.323 zones. A Proxy registers with a Gatekeeper, thereby becoming part of that Gatekeeper's zone. The Proxy isolates endpoints of different zones by concealing their addresses. The only addresses that are revealed are those of the Gatekeeper and Proxy. During call setup, the Gatekeepers of each zone obtain address information from each other. The Proxies use the address information from the Gatekeepers to route the call between zones. In this way, endpoints in different zones cannot see each other directly. They only see each other's Proxy address.

The Proxy and Gatekeeper can be configured to manage endpoint to endpoint security when the network firewall does not support Dynamic Access Control. In addition, the Proxy can manage Quality of Service (QoS) for gateways that don't support QoS.

The built-in Gatekeeper in RADVision devices such as the MCU-323 or the L2W–323P Gateway facilitates the use of the Cisco H.323 Proxy by enabling the Proxy to register with the Gatekeeper. The Gatekeeper routes H.323 signal traffic to or from another zone through the Proxy.
Proxy Facilitated Call Flow

The call flow described below is a typical example of how the Proxy is used to process a call.

Figure 5-1 – Obtaining Address Information via GK

The call flow steps below correspond to the numbering in Figure 5-1 and Figure 5-2:

1. Endpoint 1 in Zone 1 requests permission from Gatekeeper 1 to call Endpoint 2, located in Zone 2.
2. Gatekeeper 1 identifies Gatekeeper 2 as the Gatekeeper for Endpoint 2, and asks for the Endpoint 2 address.
3. Gatekeeper 2 in Zone 2 replies to Gatekeeper 1 with the address of Proxy 2, thus hiding the address of Endpoint 2 from Zone 1.
4. Gatekeeper 1 passes on the Proxy 1 address to Endpoint 1.
5. Endpoint 1 calls Proxy 1.
6. Proxy 1 asks Gatekeeper 1 for the address of Endpoint 2.
7. Gatekeeper 1 instructs Proxy 1 to call Proxy 2.
8. Proxy 1 calls Proxy 2.
9. Proxy 2 asks Gatekeeper 2 for the address of Endpoint 2.
10. Gatekeeper 2 replies with the address for Endpoint 2.
11. Proxy 2 completes the call to Endpoint 2.
Configuring the Built-in Gatekeeper for Proxy Support

To activate Proxy support, the Proxy must register with the RADVision built-in Gatekeeper. To enable Proxy registration with the Gatekeeper, you must:

- Set the built-in Gatekeeper to **Direct Mode**.
- Define the **Neighbor Gatekeeper** IP address, port number, and prefix number.
- Define the Proxy in the **Neighbor GK Parameters** screen of the built-in Gatekeeper.

When setting up Proxy support, consider the following:

- Only one Proxy in a zone can be the active Proxy. If more than one Proxy registers with the Gatekeeper, only the first registered Proxy will be the active Proxy. If the active Proxy unregisters, any Proxy that replaces it must re-register to become the active Proxy.
- If the proxy is registered with the Gatekeeper but not defined in the Neighbor GK Parameters Description text box, the Proxy will not be active in the zone and calls will not be routed through it.
- If the Proxy has been configured properly but is not registered successfully with the Gatekeeper, calls to and from a Proxy configured neighbor gatekeeper will be rejected.
- When Use Proxy for Unknown Zones is enabled, the Gatekeeper forces routing of incoming calls from Gatekeepers that are not listed in the Neighbor Gatekeeper Table. If a Proxy is not available, calls will be rejected, according to the rules described above.
- While the Zone Definition Table of the configuration application is open, a Proxy that has already been registered is still acknowledged by the Gatekeeper through the "keep alive" mechanism.
- The Gatekeeper sees each Proxy call as two calls. You should consider this when allocating call resources.
- The Gatekeeper supports 30 calls at a time.
To set the Gatekeeper to Direct Call mode

1. In the Application Parameters screen of the Gatekeeper setup, click Network Control. The Network Control screen is displayed.
2. In the Network Control screen, uncheck the Call Indirect check box.

To set the Gatekeeper to force routing of calls from unknown gatekeepers through the Proxy

- In the Network Control screen, check the Use Proxy for Unknown Zones checkbox.
To define a Neighbor Gatekeeper for proxy support

1. In the Neighbor Gatekeeper Table, click Add. The Neighbor GK Parameters screen is displayed.

2. Enter the IP address and port number (default is 1719) of the neighbor gatekeeper in the Neighbor IP and Neighbor Port text boxes.

3. Enter the prefix for the neighbor gatekeeper in the Neighbor Prefix text box. If you want the Gatekeeper to perform e-mail address resolution, you must enter the domain of the destination e-mail address instead of the numeric prefix, using the form: "@domain".

4. Enter the word "proxy" in the Description text box. Entering the value "proxy" activates the Gatekeeper Proxy support for that neighbor gatekeeper. The word "proxy" can be upper or lower case, and must not have any leading spaces before it.

5. Repeat this procedure for each Neighbor Gatekeeper you want to define for Proxy support.
Configuring the Unit

You configure the unit by:

- Selecting the Unit Type:
  - Single Station MCU-323, Distributed MCU-323, or Dedicated MP
- Accessing Unit Setup from the Configuration Source screen
- Configuring the Unit settings according to the Unit Type selected
Selecting the Unit Type and What You Want to Configure

To set the unit function type

1. In the Configuration Source screen, select one of the following function types displayed in the Unit Type drop down list:
   - MCU (single station MCU–323)
   - MCU Distributed (distributed MCU–323)
   - MP Dedicated (dedicated MP)

2. From the Source drop down list, select the configuration source file. If this is a first time configuration, select Current.

3. Click Unit Setup to proceed with configuration. Refer to the section corresponding to the Unit Type you selected for further configuration instructions.

Note
When configuring a unit to function as an MCU-323 with a built-in Gatekeeper, the Gatekeeper must be configured prior to the MCU-323. Refer to Configuring the Built-in Gatekeeper for instructions.

<table>
<thead>
<tr>
<th>To configure the unit as a ...</th>
<th>Proceed to ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Station MCU-323</td>
<td>Configuring a Single Station MCU-323</td>
</tr>
<tr>
<td>Distributed MCU-323</td>
<td>Configuring a Distributed MCU-323</td>
</tr>
<tr>
<td>Dedicated MP</td>
<td>Configuring a Dedicated MP</td>
</tr>
</tbody>
</table>

The table below outlines the configuration screens contained in Unit Setup for each of the function types, and points to where each screen is described.
<table>
<thead>
<tr>
<th>Configuration Screens</th>
<th>Single Station MCU-323</th>
<th>Distributed MCU-323</th>
<th>Dedicated MP</th>
<th>Described in sections:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Identification/ Time and Date</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Configuring a Single Station MCU-323, Configuring a Distributed MCU-323, and Configuring a Dedicated MP</td>
</tr>
<tr>
<td>MP Definition Table/ MP Settings</td>
<td>–</td>
<td>√</td>
<td>–</td>
<td>Configuring a Distributed MCU-323</td>
</tr>
<tr>
<td>Services Definition Table/ Service Settings</td>
<td>√</td>
<td>√</td>
<td>–</td>
<td>Configuring a Single Station MCU-323 and Configuring a Distributed MCU-323</td>
</tr>
<tr>
<td>Miscellaneous Settings</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Configuring a Single Station MCU-323, Configuring a Distributed MCU-323, and Configuring a Dedicated MP</td>
</tr>
<tr>
<td>Advanced</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Appendix C, Advanced Commands of the MCU-323</td>
</tr>
<tr>
<td>LAN Port Settings</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Configuring a Single Station MCU-323, Configuring a Distributed MCU-323, and Configuring a Dedicated MP</td>
</tr>
<tr>
<td>Save Setup</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>Saving the Unit Setup</td>
</tr>
</tbody>
</table>
Configuring a Single Station MCU-323

Identification Information

The Unit Identifications screen displays basic identification information for the MCU-323. All parameters except for Location are read-only. The system administrator can use the Location parameter for mapping the unit on a network.

![Unit Identifications screen](image)

*Figure 6-1 – Unit Identifications screen*

The following are the available ID Information parameters:

- **Unit’s Name** — Displays the unit’s logical name.
- **Location** (text box) — Type a description of the unit physical location in the provided text box.
- **Contact** — Displays the name and/or number of the person to contact for assistance.
Configuring the Unit

Description — Displays a description of the unit.

Date/Time (button) — Displays the Date/Time Settings screen for adjusting the call time.

Date/Time Settings

The Date/Time Settings screen displays the local time and date, and allows you to set the time and date displayed for a remote unit according to the Time Difference you enter.

Local Date/Time (read only) — States current time and date at your site in US time format.

Time Difference — Allows you to enter a time interval between the local unit and a remote site in 1/2 hour units, for a maximum difference of plus or minus 23.5 hours.

Remote Date/Time — Displays the current time and date at a remote site, according to the Time Difference entered.

Figure 6-2 – Date/Time Settings
Defining Conferencing Services

The most important aspect of MCU-323 configuration is the definition of Conferencing Services. You define these services in the Services Definition Table. Services are the mechanism that defines the qualities and capabilities of a conference. According to the prefix dialed when establishing a conference, you can request a high quality, super quality, continuous presence or other type of conference. You can use the predefined default services provided, or define services by adding or editing them in the Services Definition Table of the MCU–323.

<table>
<thead>
<tr>
<th>Description</th>
<th>Prefix</th>
<th>Frame Rate</th>
<th>Video Bit Rate [Kbps]</th>
<th>Num of Parties</th>
<th>Picture Format</th>
<th>Video Format</th>
<th>T120</th>
<th>Transcending Priority</th>
<th>Silence Suppr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Quality</td>
<td>60</td>
<td>7.5</td>
<td>110</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>Med Quality</td>
<td>61</td>
<td>7.5</td>
<td>320</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>High Quality</td>
<td>62</td>
<td>30</td>
<td>320</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>Super Quality</td>
<td>53</td>
<td>30</td>
<td>700</td>
<td>3</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>Full Room</td>
<td>64</td>
<td>30</td>
<td>110</td>
<td>15</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>Dynamic Rate</td>
<td>65</td>
<td>7.5</td>
<td>~</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>Cont. Presence</td>
<td>66</td>
<td>15</td>
<td>110/440</td>
<td>10</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 only</td>
<td>No</td>
</tr>
<tr>
<td>Data Share</td>
<td>67</td>
<td>30</td>
<td>320</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>Yes</td>
<td>G.711 only</td>
<td>No</td>
</tr>
</tbody>
</table>

When you access the Services Definition Table for the first time, a set of predefined default services are displayed, as outlined in Table 6-1. You can add, edit, or delete settings in the Services Definition Table and save the settings to a file as described in Adding, Editing, or Deleting Conferencing Services. Following is a description of each parameter displayed in the Services Definition Table.

Number of Entries — A counter that displays the number of services currently defined in the Services Definition Table.

Max Entries — Displays the total number of services you can define per MCU-323.
Configuring the Unit

**Entry** — Entry number in the **Service Definition Table**.

**Description** — A text description of the service.

**Prefix** — The prefix required to gain access to this conference type.

**Frame Rate** — The maximum frame rate suggested for this service.

**Video Bit Rate** — The maximum video bit rate suggested for the conference (in Kbps).

**Number of Parties** — The maximum number of participants allowed for a conference type.

**Picture Format** — The picture signal format that is used in this conference type.

**Video Format** — The video encoding method used.

**T120** — Indicates support for T.120 data sharing across the connection using an External T.120 Server.

**Transcoder Priority** — displays the transcoder priority setting.

**Silence Suppression** — Indicates support for Silence Suppression.

*Table 6-1 – Default Services for the MCU–323*

<table>
<thead>
<tr>
<th>Description</th>
<th>Prefix</th>
<th>Frame Rate</th>
<th>Video Rate</th>
<th>Participants</th>
<th>CIF/QCIF</th>
<th>Vid Format</th>
<th>T.120</th>
<th>X-coding</th>
<th>Silence Supp.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Quality</td>
<td>60</td>
<td>7.5</td>
<td>110</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>Med Quality</td>
<td>61</td>
<td>7.5</td>
<td>320</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>High Quality</td>
<td>62</td>
<td>30</td>
<td>320</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>Super Quality</td>
<td>63</td>
<td>30</td>
<td>700</td>
<td>3</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>Full Room</td>
<td>64</td>
<td>30</td>
<td>110</td>
<td>15</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>Dynamic Rate</td>
<td>65</td>
<td>7.5</td>
<td>~</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>Continuous Pr</td>
<td>66</td>
<td>15</td>
<td>110/440</td>
<td>10</td>
<td>CIF</td>
<td>H.261</td>
<td>No</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
<tr>
<td>Data Share</td>
<td>67</td>
<td>30</td>
<td>320</td>
<td>5</td>
<td>CIF</td>
<td>H.261</td>
<td>Yes</td>
<td>G.711 Only</td>
<td>No</td>
</tr>
</tbody>
</table>
The **Service Settings** screen allows you to define new services or change the settings of existing services. Following is a description of the parameters of the **Service Settings** screen.

**Entry** — Entry number in the **Service Definition Table**.

**Description** — A text description of the service; a maximum of 31 characters can be entered.

**Prefix** — The prefix required to gain access to this conference type; the prefix can be up to 31 characters. Valid characters are 0 through 9 and ‘#’, ‘*’. It is important for this prefix to be identical to the prefix previously defined in the Service Definition table of the Gatekeeper (see **Configuring the Built-in Gatekeeper**).

**Number of Parties** — The maximum number of participants (from 2 to 24) allowed for a conference type. This parameter depends on the video bit rate as illustrated by the tables below.

---

**Figure 6-4 – Service Settings screen with Continuous Presence enabled**

<table>
<thead>
<tr>
<th>Entry</th>
<th>Description</th>
<th>Prefix</th>
<th>Video Format</th>
<th>Video Bit Rate (Kbps)</th>
<th>Frame Rate</th>
<th>Picture Format</th>
<th>Transcoding Priority</th>
<th>MP Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>No Description</td>
<td>50</td>
<td></td>
<td>640</td>
<td>110</td>
<td>CIF</td>
<td>G.711 (64Kbps) First - G.723.1 (64Kbps) Second</td>
<td>172.020.027.051.0</td>
</tr>
</tbody>
</table>
Table 6-2 – Participants per Video Bit Rate

<table>
<thead>
<tr>
<th>Video Bit Rate (Kbps)</th>
<th>Maximum Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (voice only)</td>
<td>24</td>
</tr>
<tr>
<td>110</td>
<td>15</td>
</tr>
<tr>
<td>320</td>
<td>9</td>
</tr>
<tr>
<td>720</td>
<td>5</td>
</tr>
<tr>
<td>800</td>
<td>4</td>
</tr>
<tr>
<td>1500</td>
<td>3</td>
</tr>
<tr>
<td>~ (dynamic)</td>
<td>3-9</td>
</tr>
</tbody>
</table>

Table 6-3 – Participants per Video Bit Rate under Continuous Presence

<table>
<thead>
<tr>
<th>Video Bit Rate (Kbps)</th>
<th>Maximum CP participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>12</td>
</tr>
<tr>
<td>110</td>
<td>10</td>
</tr>
<tr>
<td>220</td>
<td>6</td>
</tr>
<tr>
<td>300</td>
<td>5</td>
</tr>
<tr>
<td>320</td>
<td>4</td>
</tr>
</tbody>
</table>

**Video Bit Rate** — The maximum video bit rate suggested for the conference (in Kbps). This is not the total bandwidth, as it does not include the bandwidth needed for the audio data transfer (normally 64 Kbps). Valid values are from 0 to 1500, or ~ (tilde).

When you set the video bit rate to ~, the MCU-323 dynamically adjusts the bandwidth according to the terminal with the lowest capability and ensures that other terminals do not exceed this bandwidth. The default upper limit suggested for such a service is 320 Kbps. When a dynamic rate conference begins, the MCU-323 allocates 320 Kbps for the conference, even if terminals that join the conference do not use all the bandwidth. The default upper limit video bit rate for a dynamic service can be changed using the **Advanced Commands**, see **Advanced Commands of the MCU-323** for more information.

When Continuous Presence is enabled, the Video Bit Rate field displays two values, the "In" bit rate and the "Out" bit rate in Kbps, with a maximum allowable "In" bit rate of 320 Kbps.
Note
To define a service for a voice only conference, set the video bit rate to 0.

Once a full capacity conference has started, no other conference is allowed to begin until the current conference is closed. This applies even when not all the participants are connected to the conference. Bandwidth is reserved for the participants that have not yet joined the conference.

**Video Format** — The video encoding method used. This can be set to **H.261** or **H.263** in the *Service Settings* screen.

**T120 Enabled** — Enables support for T.120 data sharing across the connection using an External T.120 Server, **YES** (enabled) or **NO** (disabled). When this feature is enabled, the Data Share button of the MCU-323 web interface is not available, see *Using the Web Interface* in see Using the MCU-323.

**Frame Rate** — The maximum frame rate suggested for this service. The supported values range from 7.5 frames per second (fps) to 30 fps. This parameter adjusts for the trade–off between picture resolution and motion smoothness.

**Silence Suppression** — Enables support for Silence Suppression (**Yes** or **No**), available when Transcoding Priority is set to G.723.1 or G.729.

**Picture Format** — The picture signal format that is used in this conference type. This can be set to **CIF** or **QCIF** in the *Service Settings* screen.

**Transcoder Priority** — Sets the order of priorities for audio transcoding to be performed. The available options are:
- G.711 (transcoder disabled)
- G.711 (64 Kbps) First – G.723.1 (6.4 Kbps) Second
- G.723.1 (6.4 Kbps) First – G.711 (64 Kbps) Second
- G.711 (64 Kbps) First – G.729 (8 Kbps) Second
- G.729 (8 Kbps) First – G.711 (64 Kbps) Second

**MP Link** — A drop down list of the available Dedicated MP units to which you want to link a service. This means that the Distributed MCU-323 grants routing priority to this MP when processing a call request for this service. This field is activated only when the unit type is set as MCU-323 Distributed. See
Linking a Conferencing Service to an MP.

Continuous Presence — Enables the simultaneous display of up to four conference participants on the same screen. The following settings are available in the Continuous Presence list box:

- **Disable** – Select this to disable Continuous Presence.
- **Master** – Select this to enable Continuous Presence if this unit is the Master for the conference.
- **Slave** – Select this to enable Continuous Presence for all secondary units in the conference.

Continuous Presence operates by mixing 4 QCIF channels into one CIF stream. Continuous Presence operates with the H.261 video format only. Up to 12 parties can participate in a Continuous Presence conference (see Table 6-3 in the description for Number of Parties). Terminals that are connected via Gateways or the VIU–323, can participate in a Continuous Presence conference, but only view a single picture containing the active speaker.

Adding, Editing, or Deleting Conferencing Services

The Services Definition Table allows you to add new services, and to edit or delete existing services.

- **To add a service to the Services Definition Table**
  1. In the Services Definition Table, click Add. The Service Settings screen is displayed.
  2. Enter the required settings, following the explanations provided for each parameter.
  3. Click Ok in the to add this service to the Services Definition table.

- **To edit a service**
  1. Select the line in the table representing the service you want to edit and click Edit. The Service Settings screen is displayed for that service.
  2. Make the necessary changes, and click Ok to confirm.

- **To delete a service**
  - Select the entry in the table for the service you want to delete, and click Delete. The selected service is deleted from the Services Definition Table.
Defining a Default Gatekeeper and Router

The **Miscellaneous Settings** screen allows you to define a gatekeeper and a default router for the MCU-323, and gives you access to the **Advanced** screen.

![Miscellaneous Settings screen](image)

The following parameters and settings are displayed in the Miscellaneous Settings screen:

**Default Gatekeeper IP** — Enter the IP address of the Gatekeeper with which you want the MCU-323 to register. If you are using the built-in Gatekeeper, the IP address in this field is the same as for the MCU-323 unit. If you disable the built-in Gatekeeper, you must define an alternative gatekeeper IP address for the MCU-323.

**Default Gatekeeper Port** — The port through which the MCU-323 communicates with the gatekeeper.

**Default Router IP** — The default router IP address for the network segment to which the MCU-323 is connected.

**T120 Server IP** — The IP address of the external T120 server.

**T120 Server Port** — The port number for the external T120 server.

**External T120 Server** — Enables or disables support for the external T120 Server. The number of calls supported by the T120 server depends on the type of license provided.
Configuring the Unit

**Number of Installed Transcoders** — A read only parameter indicating the number of hardware based ports available in this unit for G.723.1 or G.729A/B transcoding.

**Advanced** — Displays the Advanced screen. To use the Advanced Commands, see Advanced Commands of the MCU-323.

➢ To define a default gatekeeper and router
  - Enter the IP addresses in the Miscellaneous Settings screen as required, and click Next to proceed. The LAN Port Settings screen is displayed.

**LAN Port Settings**

![LAN Port Settings](image)

*Figure 6-6 – LAN Port Settings*

The LAN Port Settings screen defines the LAN port. The following are the available parameters:

- **Port Number** — Displays the port number.
- **Enabled** — Check this check box to enable the LAN port.
- **Port Type** — Displays the type of LAN connection.
- **MAC Addr** — Displays the Media Access Control address of this unit.
**IP Address** — The IP address of the LAN port.

**IP Mask** — The IP mask defines the portion of the IP address that is used for sub-network definitions.

**Description** — A text description of the LAN port settings.

To define the LAN settings

1. In the LAN Port Settings screen, enter the **IP Address** and **IP Mask** and check the **Enabled** check box.

2. Click **Next** to display the **LAN Parameters** screen.

3. If the settings displayed are correct, click **Yes** or **Finish** to proceed to the **Save Setup** screen, see *Saving the Unit Setup*. Otherwise, click **No** in the **LAN Parameters** screen to return to the **LAN Port Settings** screen and modify the settings.

The **LAN Parameters** screen displays a summary of the LAN port settings. The Status column indicates that the port is **enabled** or **disabled**. An asterisk (*) indicates that the port parameters were edited using the **LAN Port Settings** screen.

![LAN Parameters](image)

*Figure 6-7 – LAN Parameters*
Configuring a Distributed MCU-323

When configured as a Distributed MCU-323, the MCU-323 can transfer calls to additional MCU-323 units configured as Dedicated MPs. The Distributed MCU-323 and units defined as Dedicated MP function together as one MCU-323. This increases the total number of calls and conferences that can take place simultaneously. A Distributed MCU-323 cannot run the built-in Gatekeeper, and an external gatekeeper must be used to administer the H.323 network.

Most of the configuration of a Distributed MCU-323 is identical to that of a Single Station MCU-323. You will also have to:

- Create a list of associated MPs for the Distributed MCU-323 using the MP Definition Table.
- Link a service to a particular MP, giving it priority over other MPs when a call request for this service reaches the Distributed MCU-323.

Identification Information

The Unit Identifications screen displays basic identification information for the MCU-323. All parameters except for Location are read-only. The system administrator can use the Location parameter for mapping the unit on a network. The following are the available Identification Information parameters. See Figure 6-1 for an example of the screen:

Unit’s Name — Displays the unit’s logical name.

Location (text box) — Type a description of the unit physical location in the provided text box.

Contact — Displays the name and/or number of the person to contact for assistance.

Description — Displays a description of the unit.

Date/Time (button) — Displays the Date/Time Settings screen for adjusting the call time.

Date/Time Settings

Refer to Figure 6-2 for an example of the Date/Time Settings screen.

The Date/Time Settings screen displays the local time and date, and allows you to set the time and date displayed for a remote unit located in a different international time-zone, according to the Time Difference you enter.

Local Date/Time (read only) — States current time and date at your site in US time format.

Time Difference — Allows you to enter a time interval between the local unit and a remote endpoint in 1/2 hour units, for a maximum difference of plus or minus 23.5 hours.
Remote Date/Time — Displays the current time and date at a remote endpoint that is located in a different international time-zone. This is set according to the Time Difference entered.

**Defining MPs for the Distributed MCU-323**

The MP Definition Table allows you to define the Dedicated MPs controlled by the Distributed MCU-323.

![MP Definition Table](image)

*Figure 6-8 – MP Definition Table*

**Number of Entries** — A counter that displays the number of MPs currently defined in the MP Definition Table.

**Max Entries** — Displays the total number of MPs you can define for each Distributed MCU-323.

**Entry** — Entry number in the MP Definition Table. When an MP Link address has been selected, the Distributed MCU-323 forwards calls first to the MP defined as entry number 1 and continues down the list of MPs in sequential order. When MP Link is defined as "None", calls are forwarded according to the Transcoding Priority specified in a service. See...
Linking a Conferencing Service to an MP.

**Description** — A description of the MP in free text; limited to a maximum of 31 characters.

**IP Address** — The IP address of the MP. For optimal functionality of the Distributed MCU-323, make sure each MP is connected on a separate LAN segment.

**Status (Enable/Disable)** — Allows you to enable or disable the availability of an MP. Select this check box to enable the MP. When disabled, the Distributed MCU-323 does not use this MP to process video and audio channels.

### Adding an MP Entry

![Figure 6-9 – MP Settings screen](image)

To add an MP entry to the MP Definition Table

1. If you have already defined several MPs, and want to add a new MP entry to the middle of the list, select the MP entry after which you want to add the new MP and click **Add**. The **MP Settings** screen is displayed.

2. Enter the **IP address** and a description, and check the **Status** check box to **Enable** the MP.

3. Click **Ok**. The new MP entry is added to the **MP Definition** after the previously selected entry.
Editing MP Entries

➢ To edit an MP entry

1. In the MP Definition Table, select the MP entry you want to edit, and click Edit. The MP Settings screen is displayed for that MP.

2. Make the necessary changes, and click Ok to confirm.

➢ To delete an MP entry

- Select the MP entry you want to delete, and click Delete. The selected MP entry is deleted from the MP Definition Table.

Defining Conferencing Services for the Distributed MCU-323

The Services Definition Table screen for the Distributed MCU-323 is the same as for the Single Station MCU-323 except for the MP Link parameter. For a description of the common parameters and how to define a service, see Defining Conferencing Services.
Linking a Conferencing Service to an MP

The MP Link parameter allows you to link a service to a particular MP. This means that the Distributed MCU-323 grants routing priority to this MP when processing a call request for this service. This is beneficial when the MPs are located at remote sites as well as locally. By linking specific services to one of the local MPs, you can direct a local call request directly to that MP, saving time and network resources. When MP Link is defined as "None", or when the requested linked MP has no more ports available, the Distributed MCU-323 gives routing priority to an MP according to the Transcoding Priority that is set for this service. If no transcoder is present, routing priority is determined by the order of the MP entry on the list.

Example:

Your Distributed MCU-323 is located in New York and you have defined MPs located in New York (local) and in Tokyo (remote). When a call request originating in New York reaches the Distributed MCU-323, it selects the first available MP on its list to process the audio and video channels, according to the order in which the MPs were defined. This could mean that the Tokyo MP processes the video and audio streams of this call, resulting in an unnecessary use of network resources. By associating call requests originating in New York to the local MP, you ensure that a local call is processed locally, provided this MP is free to accept the call request.
To link a service to a particular MP

1. From the Services Definition Table, click Add or select an existing service and click Edit. The Service Settings screen is displayed.

2. From the MP Link drop down list, select the MP to which you want to link this service.

3. Click Ok to confirm. The IP of the linked MP appears in the MP Link field of the service entry in the Services Definition Table.
Defining a Default Gatekeeper and Router for a Distributed MCU-323

The Miscellaneous Settings screen allows you to define a default gatekeeper and a default router for the MCU-323, and gives you access to the Advanced screen.

The following parameters and settings are displayed in the Miscellaneous Settings screen (see Figure 6-5):

- **Default Gatekeeper IP** — Enter the IP address of the gatekeeper with which you want the MCU-323 to register. If you are using the built-in Gatekeeper, the IP address in this field is the same as for the MCU-323 unit. If you disable the built-in Gatekeeper, you must define another gatekeeper IP address for the MCU-323.

- **Default Gatekeeper Port** — Displays the port through which the MCU-323 communicates with the gatekeeper.

- **Default Router IP** — Enter the default router IP address for the network segment to which the MCU-323 is connected.

- **T.120 Server IP** — The IP address of the external T.120 server.

- **T.120 Server Port** — The port number for the external T.120 server.

- **External T.120 Server** — Enables or disables support for the external T.120 Server.

- **Number of Installed Transcoders** — A read only parameter indicating the number of hardware based ports available for G.723.1 or G.729A/B transcoding in the current unit.

- **Advanced (button)** — Displays the Advanced screen. To use the Advanced Commands, see Advanced Commands of the MCU-323.

To define a default gatekeeper and router

- Enter the IP addresses in the Miscellaneous Settings screen as required, and click Next to proceed. The LAN Port Settings screen is displayed.
LAN Port Settings for a Distributed MCU-323

The **LAN Port Settings** screen defines the LAN port (see *Figure 6-6*). The following are the available parameters:

- **Port Number** — Displays the port number.
- **Enabled** — Check this check box to enable the LAN port.
- **Port Type** — Displays the type of LAN connection.
- **MAC Addr** — Displays the Media Access Control address of this unit.
- **IP Address** — The IP address of the LAN port.
- **IP Mask** — The IP mask defines the portion of the IP address that is used for sub-network definitions.
- **Description** — A text description of the LAN port settings.

To define the LAN settings

1. In the **LAN Port Settings** screen, enter the **IP Address** and **IP Mask** and check the **Enabled** check box.
2. Click **Next** to display the **LAN Parameters** screen.
3. If the settings displayed are correct, click **Yes** or **Finish** to proceed to the **Save Setup** screen, see *Saving the Unit Setup*. Otherwise, click **No** in the **LAN Parameters** screen to return to the **LAN Port Settings** screen and modify the settings.

The **LAN Parameters** screen displays a summary of the LAN port settings (see *Figure 6-7*). The **Status** column indicates that the port is **enabled** or **disabled**. An asterisk (*) indicates that the port parameters were edited using the **LAN Port Settings** screen.
Configuring a Dedicated MP

For the Distributed MCU-323 and its MPs to function properly, you must also configure the MCU-323 units defined in the MP Definition Table to function as Dedicated MP units.

Note
For better bandwidth utilization in the Distributed MCU-323 and its associated MPs, it is recommended that you connect each MP on a separate LAN segment.

Identification Information

The Unit Identifications screen displays basic identification information for the MCU-323. All parameters except for Location are read-only. The system administrator can use the Location parameter for mapping the unit on a network.

The following are the available Identification Information parameters. See Figure 6-1 for an example of the screen:

- **Unit’s Name** — Displays the unit’s logical name.
- **Location** (text box) — Type a description of the unit physical location in the provided text box.
- **Contact** — Displays the name and/or number of the person to contact for assistance.
- **Description** — Displays a description of the unit.
- **Date/Time** (button) — Displays the Date/Time Settings screen for adjusting the call time.

Date/Time Settings

Refer to Figure 6-2 for an example of the Date/Time Settings screen.

The Date/Time Settings screen displays the local time and date, and allows you to set the time and date displayed for a remote unit according to the Time Difference you enter.

- **Local Date/Time** (read only) — States current time and date at your site in US time format.
- **Time Difference** — Allows you to enter a time interval between the local unit and a remote site in 1/2-hour units, for a maximum difference of plus or minus 23.5 hours.
- **Remote Date/Time** — Displays the current time and date at a remote site, according to the Time Difference entered.
Defining a Default Router for a Dedicated MP

The Miscellaneous Settings screen allows you to define a Default Router IP Address for the MP, and gives you access to the Advanced Commands screen.

![Miscellaneous Settings screen for a Dedicated MP](image)

**Figure 6-12 – Miscellaneous Settings screen for a Dedicated MP**

**Default Router IP** — Sets the default router IP address for the network segment to which the MCU-323 is connected.

**Number of Installed Transcoders** — A read only parameter indicating the number of hardware based ports available for G.723.1 or G.729A/B transcoding in the current unit.

**Advanced** (button) — Displays the Advanced screen. For information on using the advanced commands, see Advanced Commands of the MCU-323.

➢ **To define a Default Router**

- Enter the Default Router IP address, and click Next to proceed. The LAN Port Settings screen is displayed.

LAN Port Settings for a Dedicated MP

The LAN Port Settings screen defines the LAN port (see Figure 6-6). The following are the available parameters:

**Port Number** — Displays the port number.

**Enabled** — Check this check box to enable the LAN port.

**Port Type** — Displays the type of LAN connection.
MAC Addr — Displays the Media Access Control address of this unit.

IP Address — The IP address of the LAN port.

IP Mask — The IP mask defines the portion of the IP address that is used for sub-network definitions.

Description — A text description of the LAN port settings.

To define the LAN settings

1. In the LAN Port Settings screen, enter the IP Address and IP Mask and check the Enabled check box.

2. Click Next to display the LAN Parameters screen.

3. If the settings displayed are correct, click Yes or Finish to proceed to the Save Setup screen, see Saving the Unit Setup. Otherwise, click No in the LAN Parameters screen to return to the LAN Port Settings screen and modify the settings.

The LAN Parameters screen displays a summary of the LAN port settings (see Figure 6-7). The Status column indicates that the port is enabled or disabled. An asterisk (*) indicates that the port parameters were edited using the LAN Port Settings screen.
Saving the Unit Setup

After completing and confirming the Unit Setup parameters, the Save Setup screen is displayed. Use this screen to confirm changes to the Unit Setup and save the settings as configuration files on your local hard disk.

![Figure 6-13 – Save Setup for MCU-323 Parameters]

➢ To save the Unit Setup settings to a file

1. In the Save As box, type the name of the file you want to create or save settings to an existing file. You cannot save settings to the Plug & Play file.

2. Click Yes to save the file. The Confirm screen is displayed.

3. Click Yes to upload the new configuration settings to the unit, or No to exit without uploading the file.
Figure 6-14 – Confirm

This screen uploads the new configuration to the MCU-323. These parameters become the Current settings the next time you access Unit Setup.
File Extensions for Saved Configuration Files

Unit Setup configuration settings are saved to your local hard disk in the RVCFG directory as a file named rvc3_00*.ini, where the asterisk (*) is the sequence number of the configuration file. The name you assign in the Save As: text box appears only in the Source text box of the Configuration Source screen.

The default configuration file (RV323_xx.ini, xx being the software version number) located in the RVCFG directory, lists all new configuration files that have been created as: Entry_n= file name. Note that the configuration file names (Plug & Play, Current, etc.) do not have a file extension.

For example:

[SETUP_DIRECTORY]
FileExist=1
Entries=3
;don't delete this line
Entry_1=Plug & Play
Entry_2= mcu_Setup
Entry_3= mcu_setup 2

Where "Entries=3" Indicates the number of configuration entries available, and "Entry_2= mcu_Setup" is the configuration file name, as entered in the Save As: box shown in Figure 6-13.
Using the MCU-323

This chapter provides examples of setting up conferences and managing the conference through a web interface. Topics discussed are:

- Organizing a conference
- Joining a Conference
- Inviting a Participant Into a Conference
- Creating a Cascaded Conference
- Using the MCU-323 Web Interface
- Starting the Web Interface
- Monitoring a Conference from the Web Interface
- Opening a Data Collaboration Session
- Inviting Participants from the Web Interface
- Taking Chair Control of a Conference
- Disconnecting a Participant
- Locking the Conference to View One Participant
Organizing a Conference

1. Choose a conferencing service type, see *Configuring the Unit* for more information.

2. Devise a unique **conference ID** (password) as follows:
   
   `<Service type prefix>++<Unique ID>`
   
   For example, 605793,
   
   where 60 is the conferencing service type prefix, and 5793 is the unique ID.

3. Notify all conference participants of the **conference ID** and when the conference will be held. If some users join the conference via gateways, they also need to know a gateway ISDN phone number.

   For a list of existing services and details on defining MCU-323 conferencing services see *Defining Conferencing Services* in *Configuring the Unit*.

Joining a Conference

➢ To join the conference

1. On the LAN, dial the **conference ID**. VIU users dial the same way as LAN participants.

2. On ISDN, dial a gateway ISDN phone number. Follow IVR instructions and enter the **conference ID**.

Inviting a Participant Into a Conference

You can invite a terminal into a conference by dialing the conference prefix and ID, the "**" symbol, followed by the number of that terminal. You can also enter the same number sequence using the web interface, see *Inviting Participants from the Web Interface*.

Examples:

In all examples, the conference ID is **601234**.

A. To initiate a conference and invite a terminal with phone number **9999** dial: **601234****9999**.

B. Terminal **1111** and **2222** are in a conference. You wish to invite terminal **9999** to join. **1111** must disconnect and then re-connect, and then dial: **601234****9999**.

   Now **1111**, **2222**, and **9999** are in the conference together.
C. To invite more than one terminal into the conference dial:
   \[601234**2222**9999**8888.\]
   The number of terminals you can invite at a time depends on the total number of
   parties allowed for this conference, and on the maximum number of characters
   allowed in the dialing field of the videoconferencing program.

D. To invite someone via a gateway which can be reached from the LAN by dialing
   80, dial:
   \[601234**80123456.\]
   Where 80 is the prefix for outgoing calls from the gateway and 123456 is the
   ISDN phone number of the invited person.

Creating a Cascaded Conference

You can merge two or more conferences managed by individual MCU-323s to create one
larger conference with many participants. This can be done using the dialer as described
below, or via the web interface, as described in Inviting Participants from the Web
Interface. For a discussion of Cascading, see Overview at the beginning of this user guide.

The following conditions must be met for a cascaded conference to take place:

- The individual conferences must have the same or similar video parameters.
- When using Continuous Presence in a cascaded conference, only one MCU-323 in the
  entire extended conference can be defined as a Master, and all other units must be
  configured as Slave.
- The MCU-323s participating in the cascaded conference must register with the same
  gatekeeper or neighboring gatekeepers.
- The prefixes of the conference services provided by the MCU-323s must be unique.
- Cascaded conferences should be planned carefully to avoid loops. For example, unit A
  invites unit B, unit B invites unit C, and unit C invites unit A resulting in a loop.
- When more than two MCU-323s are participating in a cascaded conference, it is
  recommended that all MCU-323s join the same conference in a star topology.
  Otherwise, terminals connected to the cascaded conference via another conference cause
  a delay in the reception and transmission of the audio and video streams.

\textbf{Note}

T.120 data collaboration is not supported across a cascaded connection.
➢ To invite an MCU-323 to join a cascaded conference

- From the terminal dialing interface, enter the local conference ID, the invite sign ‘**’, and the conference ID of the MCU-323 you are inviting.

**Example:**

To initiate a conference and invite an MCU-323 whose conference ID is 74, dial:

641**741.

Where 641 is the conference ID for the first MCU-323, "**" is the invite sign, and 741 is the conference ID for the invited MCU-323.

Terminals dialing into a cascaded conference can invite participants to join the cascaded conference.

**Example:**

To initiate a conference, invite an MCU-323 whose conference ID is 741 and invite a terminal to join the 741 conference, dial:

641**741**5578.

Where 641 is the conference ID for the first MCU-323, "**" is the invite sign, 741 is the conference ID for the invited MCU-323 and 5578 is the invited terminal phone number. Terminal 5578 joins the 641 conference.

The inviting terminal and terminal 5578 are part of a cascaded conference.
Using the Web Interface

The MCU-323 online web interface for monitoring and control allows you to:

- View information about conference participants.
- Invite new participants into the conference.
- Open a Data Collaboration (T.120) session with other participants. The Data Share button of the web interface is only available when the External T.120 Server settings are disabled (see Defining Conferencing Services for information on disabling the External T.120 Server support).
- Obtain Chair Control over the conference, this exclusively allows you to: disconnect participants from the conference or lock the conference video broadcast on one participant so that all participants see only the locked participant.

Web Interface Requirements

To use the web interface of the MCU-323 you require the following:

- An Internet browser: Netscape Navigator version 3.0 or later, or Microsoft Internet Explorer version 3.0 or later.

To open a data collaboration session via the web interface you require:

- Data Collaboration software compliant with Microsoft NetMeeting.
- Microsoft Internet Explorer.

Starting the Web Interface

1. Launch your browser.
2. Type in the URL or IP address of the MCU-323 unit you want to monitor/control.
3. The opening web page displays in your browser.
4. Type the conference ID as set up by the conference organizer.

5. Click Ok to continue. The Participants Table page displays.

**Monitoring a Conference from the Web Interface**

The Participants Table page is divided into two frames: a left frame and a main frame. The left frame includes the function buttons and the main frame displays a list of conference participants, their phone numbers, terminal types and IP addresses, as they appear in the MCU-323.
Function Buttons

Data Share — Opens a data collaboration session with the selected participant. It only appears when you select a participant that supports data collaboration and when External T.120 Server support is disabled (see Defining Conferencing Services for information on disabling the External T.120 Server support).

Invite — Allows you to invite one or more participant into the conference.

Refresh — Updates the main screen to reflect changes that take place in the conference.

Chair Control — Grants chair control. The chair has additional functions not available to other participants or monitoring parties. These include the ability to disconnect participants and lock the conference video broadcast on a particular participant. Once Chair Control is granted, no one else can take control until it is released.

Invite (text box) — Allows you to enter a telephone number for inviting participants into a conference. The text box only appears once the Invite button has been clicked.

Participants Table

Selection Radio Button — A selection button precedes each entry line. The selection button allows you to select a participant and access the functions you can perform on the participant.
**Participant** — Displays the participant’s H.323 alias as defined in the terminal. When you invite a participant via the Web Interface, the Last Name defined in the User Information of the terminal is displayed. A (***) next to participants indicates that they were invited into the conference using the Web Interface. If the MCU-323 cannot identify a participant’s name, “Unknown” is displayed instead.

**Phone Number** — Displays the participant’s phone number. If the MCU-323 cannot identify a participant’s phone number, “Unknown” is displayed. For participants dialing from the WAN through a Gateway, the Gateway phone number is displayed.

**Type** — Displays the type of conferencing software the participant is using. Also indicates support for Microsoft NetMeeting when applicable.

**IP** — The IP address of the participant. If the participant is connected to the conference via a Gateway, the Gateway IP address appears instead.
Opening a Data Collaboration Session

If a participant’s Type column indicates that their terminal supports Microsoft NetMeeting, you can initiate a data collaboration session with it. Depending on the participant’s terminal type, NetMeeting may have to be activated before data collaboration can take place.

As new participants join a data collaboration session, participants who have already joined will be able to view and share data with them.

**Note**
The Data Share feature of the web interface is only enabled if the External T.120 Server support is disabled. See *Defining Conferencing Services* for information on disabling the External T.120 Server support. For data collaboration using External T.120 Server support, follow the instructions provided with your terminal video equipment or video application.

![Image of MCU-323 interface](image.png)

*Figure 7-3 – Opening a data collaboration session with another terminal*

➢ To open a data collaboration session

1. Select the participant with whom you want to open a data collaboration session. The Data Share button appears in the left frame.

2. Click Data Share. The NetMeeting board opens and you can use it to communicate.
3. Repeat steps 1 and 2 for all participants who have NetMeeting compliant terminals, and who you wish to include in the Data Collaboration session.

**Inviting Participants from the Web Interface**

The **Invite** function allows you to invite new participants into a conference. You can also invite other MCU-323s into a conference to create a cascaded conference. For more information, see **Overview**.

![Figure 7-4 – Inviting a new participant from the web interface](image)

To invite a new participant from the Web Interface

1. In the left frame click **Invite**. The **Invite** text box for entering the phone number is displayed at the bottom of the left frame.

2. In the **Invite** text box type the phone number of the party you want to invite. If the invited party is on the WAN, type the gateway prefix for outgoing calls, followed by the invited party’s ISDN number. If inviting more than one participant, dial the invite sign (***) before each terminal phone number. The **Invite** text box can accept up to 200 characters.
3. Click **Ok** to confirm. The invited party is added to the participants in the main screen, and (***) appears beside the participant’s name. Click **Refresh** to update the screen more quickly.

➢ To create a cascaded conference via the Web Interface

1. In the left frame click **Invite**. The **Invite** text box appears at the bottom of the left frame.

2. In the **Invite** text box type the conference ID of the MCU-323 conference you want to add to a cascade. If the remote MCU-323 connects via gateways, type the gateway prefix for outgoing calls, the ISDN number of the remote gateway, and the conference ID.

3. Click **Ok** to confirm. The cascaded MCU-323 is added to the participants in the conference.

4. Click **Refresh**. The MCU-323 appears in the main screen with the invite sign (***) next to it. Participants in the invited MCU-323 conference are now part of the cascaded conference.

5. To view the participants in one of the cascaded conferences, open a new web interface page using the IP address and conference ID of the MCU-323 controlling that conference.

**Note**
You cannot invite a terminal into a conference managed by another MCU-323 from this Web Interface, even when the MCU-323s are cascaded.
Taking Chair Control of a Conference

The Chair Control function lets you control a videoconference, to disconnect participants from the conference, or lock the video broadcast on a particular participant. You can function as an outside conference chairman, and do not have to be a conference participant to obtain Chair Control via the Web Interface. Chair Control is obtained on a ‘first come, first served’ basis. Once Chair Control is granted, no one else can obtain it until it is released.

You can monitor a cascaded conference through the individual Web Interface for the MCU-323 controlling each independent conference. The functions provided by the Web Interface do not affect the cascaded conference, only the individual conference corresponding to the particular web page opened. It is advisable to designate the same Chairman for all the individual conferences of a cascaded conference.

➢ To obtain Chair Control

• In the left frame, click Chair Control. ‘Chair control granted’ displays in the status bar (if it has not already been granted to another participant).

If you are participating in the conference from the same PC as you are using to open the Web Interface, your own entry line in the web page is displayed in bold. The Chair Control button is replaced by a Chair Release button, and the RADVision logo on the left frame flashes occasionally.
The management functions available to the Chairman include **Disconnect** and **Lock/Unlock**. To access these functions you must first select a participant from the Participants Table.

**Disconnect** — Disconnects the selected participant from the conference.

**Lock/Unlock** — Allows you to lock the conference video broadcast on one participant so that all participants see this participant only.

- If you close your browser without releasing **Chair Control**, the MCU-323 automatically releases it after a period of three minutes. Once released, **Chair Control** is available upon request.

- If a participant tries to obtain **Chair Control** when it is already granted to someone else, the ‘Chairman not granted’ message is displayed in the status bar.
Disconnecting a Participant

The Disconnect feature is used to disconnect a participant from a conference. It can also be used to break up a cascaded conference into its component conferences. This is done by disconnecting the MCU-323s participating in the conference.

A typical scenario for disconnecting a participant is having invited someone to join your conference without knowing whether the person is actually at the terminal. If the invited person’s terminal is set to respond automatically, it connects to the conference even when no one is present. Disconnecting the unattended terminal conserves telephone or ISDN resources, and frees a channel for another participant to use.

![Figure 7-6 – Disconnecting a participant from the conference](image)

➢ To disconnect a participant

1. Select the participant you want to disconnect. Click Disconnect. A confirmation message appears at the bottom of the left frame.

2. Click Ok to confirm. The selected participant is disconnected from the conference and the main frame is updated.
Locking the Conference to View One Participant

The **Lock** function allows you to lock the conference video broadcast on a participant so that all others see the locked participant. The locked participant sees the last participant to speak. A typical locking scenario is distance learning, where one of the conference participants is a teacher or tutor doing most of the talking. Locking the conference video broadcast ensures that students see only the teacher. The teacher on the other hand, can see a student asking a question, i.e. the last participant to speak.

![Figure 7-7 – Locking the conference video broadcast on a participant](image-url)
To lock the conference on one participant

- Select the participant on which you want to lock the conference. Click **Lock/Unlock**. The selected participant’s entry is highlighted with a different color.

To unlock the participant

- Select the locked participant and click **Lock/Unlock**.

To lock a cascaded conference on one participant

1. From the Web Interface, select the participant on which you want to lock the conference. Click **Lock/Unlock**. The selected participant’s entry is highlighted with a different color.

2. From the Web Interface of the other MCU-323s participating in the cascaded conference, select and lock the MCU-323 that manages the conference of the locked participant. All the participants of the cascaded conference will see the locked participant.

**Note**

- If you try to lock the video broadcast on a participant that does not have a video camera or video capturing capabilities, locking does not take place and the following message is displayed in the status bar: “This participant does not send any video.”

- In a conference using Continuous Presence, locking the image on a participant disables voice-activated video switching. In a cascaded Continuous Presence conference, locking disables voice-activated video switching in the Master unit, and locks the image in a Slave unit to a selected participant. For a full description of Continuous Presence, refer to **Overview**.
Using the T.120 Server

This chapter describes the configuration of the MCU–323 to use the RADVision Data Collaboration Server. It includes:

- Overview
- Configuration Checklist
- Tips and Considerations
Overview

RADVision support for T.120 data sharing is facilitated by an independent, external T.120 Data Collaboration Server (RADVision DCS–100). Installed on a Windows NT Server, the DCS–100 relieves the MCU-323 of the resource strain in processing T.120 data sharing requests. In addition, the DCS–100 allows the MCU-323 to control access for the data sharing application, while remaining transparent to the participants of a conference at their terminals.

![Connection Setup Process for T.120 Data Collaboration Server](image)

1. A terminal requests the opening of a data sharing session with another terminal in an active videoconference.
2. The MCU-323 relays the request to the DCS, notifying the server of the MCU-323 capabilities and notifying the terminal of the DCS IP address at the same time.
3. The DCS initiates the opening of data sharing channels between the terminals.
4. The terminals are connected in a data sharing session.
Configuration Checklist

For the MCU–323 to work properly with the DCS–100, ensure that the following has been configured:

1. In the Miscellaneous Settings screen of the Unit Setup:
   - Check the External T120 Server checkbox.
   - Enter the T120 Server IP address.
   - Enter the T120 Server Port number.

2. In the Service Settings screen of each service you want to support T.120, check the T120 Enabled checkbox.
3. Ensure that the DCS–100 registration license installed supports the number of participants you want to connect.

**Tips and Considerations**

- In a cascaded conference, T.120 communication is not supported across the cascaded link. However, participants connected to the same MCU-323 unit can carry on a data collaboration session.

- At present, the Cisco H.323 Proxy does not support T.120 activation. A possible workaround is to configure the Proxy for "T.120 Bypass". This causes the T.120 signal to be routed normally instead of through the firewall. Unless a firewall supports dynamic port allocation, it cannot accept the bypass T.120 call.
This chapter provides a list of Advanced Commands for the MCU–323 and instructs you in their use.

- Overview
- Using the Advanced Commands
Overview

**Advanced Commands** are text-based commands used for the enhanced control of the MCU-323, regardless of the **Unit Type** configured. Advanced Commands let you change certain settings in realtime, such as setting the video-switching mode. They also allow you to monitor information such as CPU usage in the MCU-323.

The **Advanced Command** syntax consists of a word or sequence of words with no spaces, followed by an optional “:” (colon) and a parameter. When you do not enter a parameter, most of the Advanced Commands display the current setting for the MCU-323. Advanced Commands are not case sensitive.

Example:

“NotifyLevel:10”, means set the print debug information level to 10.

Using the Advanced Commands

![Figure 9-1 – Advanced Commands screen](image)

---

9-1
To use an Advanced command

1. Access the Advanced screen using the Advanced button in the Miscellaneous Parameters screen.

2. Enter a command from the list below into the Command text box.

3. Click Send.

The command you entered is relayed to the MCU-323. The MCU-323 acts upon this command and sends a response to verify that a valid command was entered. The response is displayed in the Response field of the Advanced screen. When you send an invalid command, an “Unknown Command” response is displayed.

The following is a description of the available Advanced Commands:

<table>
<thead>
<tr>
<th>Command Name and Description</th>
<th>Parameter Range</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CpUseDisp:XXX</strong></td>
<td>No parameter — Displays the current CPU usage load. None — No CPU usage information is displayed. Rare — Rarely displays CPU usage information. Often — Displays CPU usage often. Differ — Displays CPU usage information only if the usage changes by more than 1%.</td>
</tr>
<tr>
<td>Displays or sets the frequency of the CPU usage load displays.</td>
<td></td>
</tr>
<tr>
<td><strong>DynamBitrateDflt: &lt;rate&gt;</strong></td>
<td>Enter the required rate in kilobits–per–second from 64 Kbps up to 1500. The default value is 320 Kbps.</td>
</tr>
<tr>
<td>Sets the default maximum dynamic bit rate.</td>
<td></td>
</tr>
<tr>
<td>Command Name and Description</td>
<td>Parameter Range</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>NotifyLevel:XX</strong></td>
<td>10 to 35 – it is not recommended to exceed a NotifyLevel of 25, as this may overload the system with a very large debug message output.</td>
</tr>
<tr>
<td><strong>Register:XXX</strong></td>
<td>No parameter — Displays the IP address of the Gatekeeper to which the MCU-323 is registered. IP address of a Gatekeeper — The MCU-323 registers with this Gatekeeper. You do not have to type the whole IP address. When the Gatekeeper is on the same network segment as the MCU-323, the host portion of the IP address is enough.</td>
</tr>
<tr>
<td><strong>SetPaletteNum:X</strong></td>
<td>No parameters — Displays the number of the current color scheme option. 0-2 — Changes the color scheme according to the option you specify.</td>
</tr>
</tbody>
</table>

Changes the type and number of debug messages that are generated.

Displays the IP address of the Gatekeeper the MCU-323 is registered with or registers the MCU-323 with another Gatekeeper.

*Note: Before you register the MCU-323 with another Gatekeeper you must unregister it from its current Gatekeeper.*
Using the Advanced Commands of the MCU-323

<table>
<thead>
<tr>
<th>Command Name and Description</th>
<th>Parameter Range</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SpeakSlet_fast</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>Selects fast video switching mode. This mode is useful when fast and interactive video switching is required. This is the default mode for the MCU-323.</td>
<td></td>
</tr>
<tr>
<td><strong>SpeakSlet_slow</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>Selects slow video switching mode. This mode is useful when background noise causes a high level of false video switching sequences. This mode will decrease the number of false switching events causing the switch to be less sensitive.</td>
<td></td>
</tr>
<tr>
<td><strong>Unregister</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>Unregisters the MCU-323 from the Gatekeeper. You can then register the MCU-323 with another Gatekeeper.</td>
<td></td>
</tr>
<tr>
<td><strong>VdoCPmatrix: x</strong></td>
<td>1 – upper left quadrant (default)</td>
</tr>
<tr>
<td>Configures the position of the voice-activated quadrant in the Continuous Presence screen.</td>
<td>2 – lower right quadrant</td>
</tr>
<tr>
<td><strong>VdoSWMode:XXXXX</strong></td>
<td><strong>No Parameter</strong> — Displays the current video switching mode. <strong>ALLC1</strong> — All participants see the participant that is talking the loudest, and the participant talking the loudest sees himself/herself. <strong>CUCME</strong> — All participants see the participant that is talking the loudest and the participant currently talking sees the previous participant that spoke.</td>
</tr>
<tr>
<td>Displays or sets the video switching mode for the MCU-323. The default mode is CUCME.</td>
<td></td>
</tr>
</tbody>
</table>

Additional advanced commands may be available for different versions of the MCU-323. Contact RADVision Technical Support at HWsupport@tlv.radvision.com or OnLANsupport@radvision.com for additional information.
Troubleshooting the MCU-323

In this chapter:

☐ LED Indications
☐ Initial Setup Problems
☐ Operation Tips
LED Indications

**The Power LED does not light**
This indicates that the MCU-323 is not properly connected to the power source. Make sure the power cable is firmly connected to the MCU-323 and to the power outlet.

**The Link LED of a connected LAN port does not light**
This indicates that the LAN port is not connected to the network segment. Make sure that the connections are secure, that you are using the correct Ethernet cable and connector, and that the devices at both ends of the Link are powered-up.

Initial Setup Problems

- When entering an MCU-323 IP address manually, the address must have a full three digit component for each part of the IP address (for example, 192.003.045.012).
- Check the password — passwords for the MCU-323 are case sensitive.

Console Port Access Problems

You can access the MCU-323 through the console port for local configuration and diagnostics.

- **Access problems from a local terminal connected to the MCU-323 console port**
  - Make sure the MCU-323 is connected to the terminal using a crossed RS-232 cable.
  - Check that the connections are secure at both ends.
  - Verify communication with the terminal.

- **To verify the communication between the MCU-323 and a terminal**
  1. Run the terminal emulation application (e.g. HyperTerminal). The command prompt is displayed.
  2. Verify that the communication settings for the terminal are as follows: 9600 Baud rate, 8 data bits, no parity, 1 stop bit, no Flow Control.
  3. Check to see that the crossed cable is properly connected at both ends.
  4. Click **Enter**. The command prompt (cursor) moves down to the next line to indicate that the connection is active.
5. Restart the MCU-323. A log of the startup events is displayed on screen.

6. If nothing is displayed, a failure in the serial controller and/or the cable is indicated. Alternately, a problem in the PC may be indicated, and/or the Com port you selected may not be the correct one. Contact the local RADVision distributor or RADVision Customer Support department for further help.

**Operation Tips**

- When a new call fails — check the **Zone Definition Table** to see what endpoints are registered in that zone.

- To avoid confusion when LAN endpoint phone numbers begin with the same numeric string as service prefixes. You can modify the prefixes in the Gatekeeper and MCU-323 **Services Definition Table** so that they are unique within the zone.

- The MCU reserves bandwidth for the total number of participants in this conference even if not all the expected participants join the conference. To prevent this waste of bandwidth and MCU-323 resources, we recommend you set an average number of participants, for example four.

- Each entry line in the **Services Definition Table** represents a different type of conference call using a particular service. Several conferences using the same service can take place at the same time. A **unique password** should be added to the conference prefix to distinguish it from other conferences.

- When using data collaboration applications, check to see if the MCU-323 is enabled for simple T.120 support, or an external T.120 server. If the external T.120 server is enabled, you must ensure that the T120 server IP address and port are configured.

- When the **Zone Definition Table** of the Gatekeeper configuration is open, the Gatekeeper cannot receive new registrations.

- When using the H.323 Proxy in a conference take into consideration that the Proxy uses two calls to the Gatekeeper for each call being set up. This can limit the number of concurrent calls that are supported.
Safety Considerations
Safety Considerations

To avoid getting an electric shock, and to avoid damaging the MCU-323, servicing the MCU-323 should be performed by qualified technical personnel only.

Grounding

Before connecting the MCU-323 to the power line, the unit’s protective earth terminals must be connected to the protective conductor of the power cord. The power plug should only be inserted into a power outlet that has a protective earth contact. Do not use an extension cord that does not have a protective conductor (ground). The MCU-323 can become dangerous if you interrupt any of the protective (grounding) conductors or disconnect any of the protective earth terminals.

High Voltage

Disconnect the MCU-323 from the power line before removing the cover. Avoid any adjustment, maintenance, or repair of the opened unit under voltage. These actions should only be carried out by a skilled person who is aware of the dangers involved. Capacitors inside the instrument may still be charged, even if the unit has been disconnected from the power source. Wrist strap use is mandatory.
Cable Connectors
RS-232 9-pin Serial Port

The following table describes the various pins of the RS-232 9-pin Serial Port:

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
<th>I/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>RXD</td>
<td>Input</td>
</tr>
<tr>
<td>3</td>
<td>TXD</td>
<td>Output</td>
</tr>
<tr>
<td>4</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>GND</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>NC</td>
<td></td>
</tr>
</tbody>
</table>

Null Modem Cable

![Null Modem Cable Diagram]

Figure B-1 – Null modem cable connectors
RJ-45 8-pin LAN Port

The following table describes the various pins of the RJ-45 LAN Port:

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
<th>I/O</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TXD+</td>
<td>Output</td>
</tr>
<tr>
<td>2</td>
<td>TXD+</td>
<td>Output</td>
</tr>
<tr>
<td>3</td>
<td>RXD+</td>
<td>Input</td>
</tr>
<tr>
<td>4</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>RXD-</td>
<td>Input</td>
</tr>
<tr>
<td>7</td>
<td>NC</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>NC</td>
<td></td>
</tr>
</tbody>
</table>
Uploading Files to the MCU-323
Using the Software Upload Utility

The MCU-323 stores the operating software in its onboard Flash memory. Use the **Software Upload Utility** to upload flash files to the MCU-323 and update or upgrade the software modules.

**Note**
The Software Upload Utility serves other RADVision OnLAN units as well. You only need to install it once on your local PC for all OnLAN units.

➢ To run the OnLAN Software Upload Utility do one of the following

- From the Start | Programs menu, point to **RADVision OnLAN Tools** and select **Software Upload Utility**.

**OR**

- Run Windows Explorer, point to the flash file (*.fls) you want to upload and double-click it.

The Software Upload Utility window is displayed.
Figure C-1 – Software Upload Utility screen
Uploading Flash Files to the MCU-323

To upload a file to the MCU-323

1. In the **IP:** text box type the IP address of the MCU-323 to which you want to upload the file.

2. Enter your User Name and Password in the text boxes provided.

3. From the list of files, locate and select the file you wish to upload. If the file you wish to upload is not displayed, use the **Look in:** drop-down list box to browse for the desired file.

4. Click **Upload.** A confirmation box is displayed.

5. Click **Yes** to confirm the upload process.

The connection attempt window displays connection progress. If the connection attempt is not successful, an abort message is displayed.

When the configuration terminal connects to the unit, a status window shows the uploading progress and confirms the name of the file destination and its IP address.

After a file is successfully uploaded to the MCU-323, the message “Upload Process Complete” is displayed.
Technical Specifications
Interfaces

LAN: 10/100BASE-T Ethernet LAN UTP connection.

LED Indicators

- Power
- Test
- Function
- LAN/Link

Dimensions

- Height: 4.3 cm (1U or 1.75 in.)
- Width: 43.2 cm (17.0 in.)
- Weight: 2.5 Kg (5.5 lbs.)
- The unit is rack mountable in a standard 19-inch rack

Power Supply

- 100-240 VAC auto sense, 50/60 Hz

Environment

- Operating Temperature: 0-40°C (32-104°F)
- Humidity: 15%-85% non-condensing

Certifications:

- UL 1950/CSA 950, Verified to EN 60950
- FCC Part 15
- EN 55022, EN 50082-1
- CE S09550.02
Glossary

10Base-T

The IEEE 802.3 standard for Ethernet local area network system at rates of up to 10 Mbps.

10/100Base-T

Combines support for 10 Mbps Ethernet, and 100 Mbps Fast Ethernet (IEEE 802.3u)

1B Call

A voice or video call that uses only one B channel of an ISDN line.

2B call

A video call that uses 2B channels of an ISDN line.

Aliases

Alternative identification strings for an IP address.

B channel

Bearer Channel. In ISDN communications, a B channel transmits data or voice at 64Kbps or 56Kbps.

Bandwidth

The data transfer capacity of a channel measured in bits per second. The bandwidth of Ethernet is 10Mbps.

BRI

Basic Rate Interface to an ISDN network. A BRI line has two 64Kbps B channels that transmit the data and one 16Kbps D channel that is used for call setup and control signaling.

Broadcast

In packet switched networks, the data is sent to all users connected to the network or network segment.

Cascade

Multiple conferences that are connected together into a larger aggregated conference. This is done by inviting additional MCU-323s into an existing conference.

Channel bonding

Increasing the bandwidth of a call by aggregating two or more channels of an ISDN line.
Glossary

CIF

Common Intermediate Format – A standard video format used in videoconferencing. CIF is defined by a screen resolution of 352 x 288 pixels.

Circuit-switched

The temporary connection of two or more communications channels. Users have full use of the circuit until the connection is terminated. ISDN is a circuit switched network.

Console port

The serial port on the Gateway that connects to a terminal or to a modem. This port is used for local monitoring, diagnostics and remote configuration.

Continuous Presence

Continuous Presence allows you to view other conference participants on the same screen at the same time as the active speaker. The RADVision MCU-323 achieves this by combining four QCIF images into one CIF image.

Dedicated MCU-323

The Dedicated MCU-323 is an MCU-323 device defined as an MP and controlled by a Distributed MCU-323.

Distributed MCU-323

A Distributed MCU-323 is an MCU-323 device defined as an MC, controlling up to four MP's, including the MP section housed in the same box as the Distributed MCU-323 unit.

DTMF

Dual Tone Multi-Frequency signals are the type of audio signals used in telephony for tone dialing.

Endpoint

An H.323 terminal, gateway or Multipoint Controller Unit (MCU). An endpoint can call or be called and it can generate or end information streams.

G.711

An ITU standard for speech codecs that provides toll quality audio at 64 Kbps using the PCM method and either µ-law or A-law.

G.723.1

An ITU standard for speech codecs that provides good quality audio at 5.3 or 6.3 Kbps using the MP–MLQ (6.3 Kbps) and ACELP (5.3 Kbps) methods.

G.728

An ITU standard for speech codecs that provides near toll quality audio at 16 Kbps, using the LD-CELP method.
G.729 A/B
An ITU standard for speech codecs that provides near toll quality audio at 8 Kbps using the CS–ACELP method. G.729 Annex A is a reduced complexity codec and G.729 Annex B supports silence suppression and comfort-noise generation.

Gatekeeper
The gatekeeper is an H.323 entity that provides address resolution, access control and other services to endpoints on an H.323 network.

Gateway hunting
The Gatekeeper’s ability to search for an available Gateway. When the Gatekeeper receives a call request prefixed by a service supported by several Gateways, the Gatekeeper forwards the call to the first available Gateway supporting the requested service.

Group hunting
The Gatekeeper’s ability to search for an available terminal within a definition group of terminals. Terminals can be defined as definition groups by registering with the Gatekeeper as service providers.

H.320
The ITU standard for videoconferencing over digital networks such as ISDN.

H.323
The ITU standard for videoconferencing over packet switched networks such as LANs and the Internet.

IMUX
Inverse Multiplexor is a device that divides a high-speed transmission into several low-speed transmissions and vice versa. It is used to transmit LAN and videoconferencing traffic over lower-speed digital channels.

IP address
The unique address of a computer attached to a TCP/IP network. IP addresses are 32 bit long where each octet is represented in decimal and is separated by dots.

IP network
A network that uses the TCP/IP protocol.

ISDN
Integrated Services Digital Network. ISDN is an entirely digital telephone network that allows both data and voice communication over the same line. ISDN replaces the old analog local loop and operates at significantly faster speeds than the traditional telephone service.
ITU–T
International Telecommunications Union is an international organization with 150 member countries founded in 1865 and headquartered in Geneva. The ITU–T is the Telecommunication Standardization Sector of the ITU, developing standards for interconnecting Telecommunication equipment across networks.

IVR
Interactive Voice Response is a two-stage incoming call routing method supported by the Gateway. It enables Direct Inward Dialing to a LAN terminal even when the ISDN lines do not have multiple numbers allowing direct dialing to an endpoint.

Kbps
Kilo Bits Per Second. One thousand bits per second. Used to define data transfer bit–rates.

L2W-323P Gateway
Translates between H.323 and H.320 protocols allowing the exchange of voice, video and data between H.323 based conferencing endpoints on IP networks and H.320 compliant endpoints on circuit switched ISDN networks as well as Voice over IP (VoIP).

LAN
Local Area Network. A network of connected computers covering a small geographic area such as a building or a campus.

LED
Light Emitting Diode. A display technology that uses a semiconductor diode that emits light when charged. The Gateway’s LEDs indicate both correct and problematic operation.

Logical port
A number that combined with the IP address provides a unique transport address for a device or application.

Mbps
Mega Bits Per Second. One million bits per second. Used to define data transfer bit–rates.

MC
Multipoint Controller – a unit that performs control functions for a multipoint videoconference.

MCU–323
Multipoint Conferencing Unit – a RADVision device that performs the tasks of an MC and an MP, and has a built–in Gatekeeper unit.
MP
Multipoint Processor – a unit that performs the call processing tasks for a multipoint videoconference.

Multicast
In packet-switched networks, the data is sent to multiple users connected to the network or network segment. Multicast is a one-to-many transmission similar to broadcasting, except that multicasting implies sending to a list of specific users, whereas broadcasting implies sending to everybody.

Neighbor Gatekeeper
The gatekeeper of a neighboring zone.

Packet-switched
Networks that break up a message into smaller packets before switching the packets to their required destination. Each packet contains a destination address so all packets in a single message do not have to travel by the same path. The destination computer reassembles the packets back into their proper sequence.

PBX
Private Branch Exchange. A private telephone switching system in an organization that interconnects telephone extensions to each other and to the public telephone network.

PPP
Point-to-Point Protocol. A data link protocol that provides dial-up access over point-to-point links. It can run on any full-duplex link from POTS to ISDN to high-speed lines (T1, T3, etc.).

Prefix
Part of the dialing sequence used to define a service.

PRI
Primary Rate Interface to an ISDN network. In the U.S. a PRI line provides 23B channels and one 64Kbps D channel (23B+D), that is equivalent to a T1 line and in Europe, a PRI line provides 30B channels and 1D channel (30B+D), equivalent to an E1 line.

PSTN
Public Switched Telephone Network. The worldwide telephone network.

QCIF
Quarter Common Intermediate Format – A standard video format used in videoconferencing. QCIF is defined as one quarter the screen resolution of CIF, or 176 x 144 pixels.
Glossary

RAS
Registration Admission Status protocol. The communication protocol used to convey registration, admission and status messages between H.323 endpoints and the Gatekeeper.

Restricted Bandwidth
Bandwidth rates that use seven bit encoding as opposed to eight bit encoding. Restricted rates are multiples of 56 Kbps, compared to standard rates that are multiples of 64 Kbps.

RJ-45

Room system
H.320 based legacy videoconferencing stations. They are called room systems because they are usually large monitors with a wide-angle camera and served groups of people who meet in a room and conference with other similar groups at remote locations.

Silence Suppression
Silence information within the audio stream can consume LAN bandwidth and burden MCU voice processing. Using compression techniques, Silence Suppression can greatly reduce the wasted bandwidth in a multipoint conference and on congested networks.

Socket
Unique transport address for an application or device formed by the IP address and port number.

Subnet
A portion of an IP network defined by a subnet mask. Devices on the same subnet have the same subnet mask.

T.120
Data sharing protocol for multipoint data communication in a multimedia conferencing environment. T.120 enables white board collaborations, file transfers, graphic presentations and application sharing between participants in a conference.

TCS4
A Direct Inward Dialing routing method for H.320 calls supported by the Gateway.

Unicast
In packet-switched networks, the data is sent to one user.

UTP
Untwisted Shielded Pair.
V.35

V.35 is a high-speed RS-232 interface that enables the Gateway to make high bandwidth calls. When a V.35 module is installed in the Gateway, the Gateway connects to an IMUX, Modem or Terminal Adapter to provide rates of up to 384Kbps.

VIU-323

RADVision’s Video Interface Unit is a self-contained terminal adapter that connects H.320 Room Systems to IP networks without disrupting the current H.320 capabilities of the Room System.

VoIP

Voice over IP is the ability to make telephone calls over IP based data networks with suitable quality of service.

WAN

Wide Area Network. A communications network over a wide geographic area.

Zone

In H.323 networks, a collection of terminals, gateways and MCUs managed by a single gatekeeper. A zone must include at least one terminal and may include several LAN segments connected by routers.
Index

A

Advanced commands
listed • 9-2
overview • 9-1
using • 9-1
Alias Assignment
defined • 4-33
setting • 4-36
Allowed Services
Allowed Services screen • 4-14
defining for an endpoint • 4-14
Audio transcoding
overview • 1-5
supported options • 6-9
transcoding priority • 6-9

B

Bandwidth
considerations • 1-9
maximum bandwidth per terminal • 4-34
maximum supported • 4-34
Built–in Gatekeeper • See also Gatekeeper
disabling • 4-35
Proxy support • 5-4
summary of features • 1-12

C

Cables
connecting • 2-1
LAN connection • 2-2
power • 2-1
Calls
disconnecting • 4-33
maximum number allowed • 4-34
Cascaded conference
creating • 7-2
overview • 1-7
Conferencing services
adding • 6-10
default • 6-6
defining • 6-5, 6-17
deleting • 6-10
editing • 6-10
linking • 6-18
Conferencing topology
overview • 1-6
Configuration files
file extensions • 6-27
saved • 6-27
Configuration software • See OnLAN Tools
Console port
access problems • 10-1
Continuous presence
configuring • 6-10
overview • 1-3

D

Data collaboration
opening a session • 7-8
overview • 1-4
Data Collaboration Server • See RADVision DCS–100
Date and time settings • See OnLAN Configure
Dedicated MP • See also MP
configuring • 6-22
LAN port settings • 6-23
overview • 1-6
DHCP • See Dynamic IP Environment
Discovery Multicast • 4-34

Index–1
Distance
  Default Distance · 4-34, 4-36
  Max. Distance · 4-13, 4-36
  Multicast Distance · 4-34, 4-36
  Neighbor Distance · 4-24, 4-36
Distributed MCU-323
  conferencing services · 6-17
  configuring · 6-14
  defining MPs · 6-15
  LAN port settings · 6-21
  overview · 1-6
Distributed topology
  overview · 1-6
Dynamic IP Environment
  defined · 4-33
  endpoint definition · 4-15

E
Endpoint
  distance parameters · 4-13, 4-34
  editing Predefined Properties · 4-16
  predefining properties · 4-12
  status · 4-11
  Supported Services · 4-18
  viewing Online Properties · 4-17

F
File extensions
  configuration files · 6-27

G
Gatekeeper
  defining default gatekeeper · 6-11, 6-20
  disabling the built-in Gatekeeper · 4-35
  in Network Control screen · 4-33
  Indirect Call · 4-33
  summary of features · 1-12
  working with more than one · 4-22
  Zone configuration · 4-8
Gatekeeper Configuration
  Supported Services screen · 4-18
  GK Identifier · 4-34

H
H.323 Proxy
  call flow description · 5-2
  configuring support for · 5-4
  overview · 5-1

I
Identification information · 6-3, 6-14, 6-22
IP address
  assigning IP address to MCU–323 · 3-2
  Neighbor Gatekeeper IP address · 4-23
  subnet IP · 4-28
Islands
  defined · 4-27
  Island Code · 4-28

L
LAN
  connecting to · 2-2
LAN port settings
  dedicated MP · 6-23
  Distributed MCU–323 · 6-21
  Single Station MCU–323 · 6-12
LED indicators
  troubleshooting · 10-1
Load
  loading Neighbor Gatekeeper settings · 4-26
  loading settings to the Zone Definition Table · 4-21
Locking · See Web interface

Index–2
MCU-323
- assigning IP address · 3-2
- conferencing services · 6-17
- configuring Distributed MCU-323 · 6-14
- configuring Single Station MCU-323 · 6-3
- default gatekeeper · 6-20
- default router · 6-20
- define MPs for distributed MCU-323 · 6-15
- Distributed MCU-323 · 6-14
- front panel · 1-13
- installation · 2-1
- introduction to · 1-2
- LED indicators · 1-13
- operation tips · 10-2
- rack mounting · 2-3
- rear panel · 1-14
- selecting unit type · 6-1
- summary of features · 1-10
- Unit Type · 6-1
MCU–323
- Identification information · 6-3
MP
- adding an entry · 6-16
- conferencing service · 6-18
- configuring dedicated MP · 6-22
- define for distributed MCU-323 · 6-15
- editing an MP entry · 6-17
- linking conferencing service · 6-18
- MP definition table · 6-16
MP definition table
- adding an entry · 6-16
- editing an entry · 6-17
Multicast Distance · 4-34

N
Neighbor Gatekeeper
- defining for Proxy support · 5-6
Neighbor Gatekeepers
- defining · 4-24
- deleting · 4-25
- distance parameters · 4-24, 4-36
- editing settings · 4-25
- Neighbor GK Parameters screen · 4-24
Neighbor Gatekeepers Table
- loading settings · 4-26
- Neighbor Gatekeepers Table · 4-23
Neighbor Gatekeepers Table
- saving settings to a file · 4-25
Network Control
- Network Control screen · 4-31
- network resources · 4-34
- registration policy · 4-32
Network Control
- saving settings to a file · 4-38
Network Control settings
- Everyone can register · 4-8
Network resources · 4-34
Network Topology
- Islands · 4-27
- Network Topology Table · 4-28
Network Topology Table
- saving settings to a file · 4-30

O
OnLAN Configure
- assigning IP address · 3-2
- configuration source screen · 3-5
- date and time settings · 6-4, 6-14, 6-22
- LAN port settings · 6-12, 6-21, 6-23
- passwords · 3-3
- select unit screen · 3-1
- selecting an MCU-323 to configure · 3-1
- selecting unit type · 3-6
- services definition table · 6-5
- starting · 3-1
- unit identification information · 6-3
OnLAN Tools
- installing · 2-4
Online Always · 4-11

Index–3
Participants table · See Web interface
Password
  changing · 3-4
  enter password screen · 3-3
Port
  Neighbor Gatekeeper · 4-23

Rack mounting · 2-3
RADVision DCS
  operating tips · 8-3
RADVision DCS–100
  configuring MCU–323 for · 8-2
  overview · 8-1
Router
  defining default router · 6-11, 6-20, 6-23

Saving
  Neighbor Gatekeepers Table · 4-25
  Network Control settings · 4-38
  Network Topology Table · 4-30
  Unit Setup · 6-25
Services
  default conferencing services · 6-6
  defining for a terminal · 4-5
  defining in the Unit Configuration · 6-5
  prefix · 4-4
  supported by an endpoint · 4-18
Services definition table
  default values · 6-6
  description · 6-5
  editing or modifying · 6-10
Single Number Access to a group of terminals · 4-5
Single Station MCU-323
  configuring · 6-3
  LAN port settings · 6-12

Site preparation · 2-1
Software Upload Utility
  starting · C-1
  using · C-3
Subnet
  defining · 4-29
  deleting · 4-30
  editing · 4-30
  in definition of Islands · 4-27
  subnet mask · 4-28

T.120 Server
  configuring · 8-2
  operation tips · 8-3
  RADVision DCS–100 · 8-1
Topology
  overview · 1-6
Transcoding · See Audio transcoding
Transcoding priority
  available options · 6-9
  configuring · 6-9

Unicast · 4-22
Unit setup
  save settings to file · 6-25
Unit type
  selecting · 3-6
Uploading files to MCU-323 · C-3. See also Software Upload Utility
Use Proxy for unknown zones
  configuring · 5-5

Video bit rate
  participants per bit rate level · 6-8
Video switching
  voice activated, overview · 1-3
Videoconference
  cascaded, setting up · 7-2
  inviting participants · 7-1
  joining · 7-1
  monitoring · 7-5
  organizing · 7-1
Voice activated video switching
  overview · 1-3

W
Web interface
  description · 7-6
  disconnecting participants · 7-13
  inviting participants · 7-9
  locking video on participant · 7-14
  overview · 1-2
  participants table · 7-6
  requirements · 7-4

Z
Zone
  controlling access to · 4-8
  Open Zone mode · 4-8
  Strict Zone mode · 4-8
Zone Definition
  deleting endpoints from Zone Definition Table · 4-20
  saving settings to a file · 4-21
Zone Definition Table
  deleting endpoints from · 4-20
  described · 4-10
  loading settings to the Zone Definition Table · 4-21