



## NOTICE

© 2005 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.

This publication is RADVISION confidential. 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. All registered trademarks recognized.

For further information contact RADVISION or your local distributor or reseller.

The following third party products are included in this package subject to the terms of the specified vendors and are provided free of charge. These products are provided "as is" and RADVISION Ltd. and the third party vendors accept no warranty with respect to these products.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that the above copyright notices appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation.

1. Westhawk Java SNMP Stack, copyright © 2000, 2001, 2002 by [Westhawk Ltd.](#) Author, [Tim Panton](#).
2. Apache Tomcat, copyright © 1999-2001 by The Apache Software Foundation.
3. MySQL™, copyright © 1995-2003 by MySQL AB.  
If you require the MySQL source code files, please contact RADVISION customer support.
4. Java™ 2 Runtime Environment (J2RE), Standard Edition, Version 1.4.1\_x, copyright © 1995-2003 by Sun Microsystems, Inc.
5. This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at <http://oss.software.ibm.com/icu4j/>.

Video Management System (VMS) Network Manager , November 2005

Publication 2

<http://www.radvision.com>

# CONTENTS

---

## *About This Manual*

VMS Network Manager Features	vii
Feedback	ix

## **1** *VMS Network Manager Overview*

What's in this Chapter	1
About the VMS Network Manager	1
What the VMS Network Manager Provides	2

## **2** *Network Tree View*

What's in this Chapter	7
About the Network Tree View	8
Monitor Tab	12
Elements Tab	14
Alarms Tab	15
Events Tab	16
Conferences Tab	17
Calls Tab	19
Configure Tab	20
Logs Tab	25
Access Tab	26
Additional Network Tabs	28
Additional ECS Tabs	31
Additional Endpoints Tab	52

	Additional MCU Tabs	61
	Additional Gateway Tab	67
	Additional Cisco MCM Tabs	68
	Additional DCS Tab	79
<b>3</b>	<i>Network Table View</i>	
	What's in this Chapter	81
	About the Network Table View	81
<b>4</b>	<i>Network Map View</i>	
	What's in this Chapter	83
	About the Network Map View	83
<b>5</b>	<i>Alarms View</i>	
	What's in this Chapter	85
	Alarms Tab	85
	Events Tab	86
<b>6</b>	<i>Conferences and Calls View</i>	
	What's in this Chapter	89
	Calls Tab	90
	Conferences Tab	91
<b>7</b>	<i>Settings View</i>	
	What's in this Chapter	93
	Settings Interface	94
	Users Tab	95
	Alert Recipients Tab	97
	Traps Tab	100

	Alarms Tab	102
	Network Subsets Tab	103
	Logs Tab	105
	Element Logs Tab	106
	Element Access Tab	106
	Endpoint Management Tab	108
	Auto-detect Tab	114
	Cisco MCM Tab	116
<b>8</b>	<i>Finding and Managing Elements</i>	
	What's in this Chapter	119
	Performing Auto-detect	120
	Adding Elements Manually	122
	Creating Custom Views	126
<b>APPENDIX A</b>	<i>Configuration Utility</i>	129
	What's in this Appendix	129
	VMS Manager Server Configuration Utility	129
	Utility Tabs	130
<b>APPENDIX B</b>	<i>ECS Bandwidth Policies</i>	135
	What's in this Chapter	135
	Sample Topology with Subzones	135
	Subzone Rules	137
	Applying Rules	138
	Calculating Used Bandwidth	139
	Dedicated Rules	139
	Default Rules	140
	<i>Index</i>	141



# ABOUT THIS MANUAL

---

## VMS NETWORK MANAGER FEATURES

The Video Management System (VMS) Network Manager User Guide presents a practical guide to installing, configuring and using the Video Management System (VMS) Network Manager and describes the functionality of each feature of the interface.

This section lists the features of the Video Management System (VMS) Network Manager.

### NEW IN VERSION 2.3

Video Management System (VMS) Network Manager version 2.3 includes the following new features:

- Supports software upgrade and configuration update for the following additional Sony endpoints:
  - PCS-11
  - PCS-G70
  - PCS-TL50
  - PCS 1600/P (configuration update only)

### NEW IN VERSION 2.1

Video Management System (VMS) Network Manager version 2.1 includes the following new features:

- Supports software upgrade and configuration update for Sony PCS-1 endpoints.

## VMS Network Manager Features

- Supports endpoint management for commonly used endpoints including, automatic detection, central configuration and dialing from the managed endpoint.
- Supports Cisco MCM with extensive configuration options using the Video Management System (VMS) Network Manager interface including, Local and Remote Zones, Prefixes, bandwidth rules, debug flags and Telnet commands.
- Supports the Local user profile with configurable network subsets for restricting user read permissions and write permissions to specific zones and element types on the network.
- Supports network hierarchy management allowing central control by the Video Management System (VMS) Network Manager of network elements. Replaces the ENC functionality in RADVISION ECS elements.
- Supports network call monitoring with comprehensive details about point-to-point calls on the network and call disconnection.
- Supports the customization of alarm severity settings per user profile.
- Supports alarm e-mail notifications and sound notifications per user profiles.
- Supports offline element configuration.
- Supports drag and drop network hierarchy configuration with automatic IP addressing updates to the relevant element tables.

### EXISTING FEATURES

Video Management System (VMS) Network Manager includes the following features:

- Provides network status about elements, calls, endpoints, bandwidth usage, B-Channel usage and error status.
- Provides conference view showing the MCU controlling the conference, conference ID, conference type, video and bandwidth settings and the number of participants.
- Auto-detects RADVISION elements present on the network.

- Allows basic element configuration for network administrators to view and edit the most commonly used configuration parameters of various elements in the network, such as MCU elements, ECS elements and Gateways.
- Provides alarms and events displaying active alarms in any network elements and events that have taken place in the network.
- Provides full element manager and terminal manager connectivity.
- Provides centralized log management allowing management of both the network and element type levels, control of network log file size, the number of backups to maintain and the level of activity detail. Also includes logs for element types that do not maintain log files of their own, such as MCU elements and Gateways.
- Provides multiple network views such as, the Network Tree view displaying elements according to zone, the Network Table view displaying a single, unified list of all network elements, the Network Map view displaying elements and network status in a graphic, multi-layered format and custom views.

## FEEDBACK

The team at RADVISION constantly endeavor to provide accurate and informative documentation. However, if you have comments or suggestions regarding improvements to future publications, we would value your contribution.

Please reply to the following address and include a summary/headline of your comments:

[documentation@radvision.com](mailto:documentation@radvision.com)

We thank you for your contribution and wish you the best with your endeavors.



# 1

## VMS NETWORK MANAGER OVERVIEW

---

### WHAT'S IN THIS CHAPTER

This chapter introduces you to the following:

- [About the VMS Network Manager](#)
- [What the VMS Network Manager Provides](#)

### ABOUT THE VMS NETWORK MANAGER

The Video Management System (VMS) Network Manager is a simple-to-use network management system for RADVISION IP video conferencing networks.

Designed with the network administrator in mind, the Video Management System (VMS) Network Manager provides a unified interface for managing all the devices (**elements**) in your video conferencing network, including:

- RADVISION elements
  - MCU
  - ECS
  - Gateway
  - DCS
  - VPS
- Third party elements and endpoints:
  - Cisco MCM
  - Endpoints: Polycom, Tandberg, Aethra, Sony
  - Schedulers

## What the VMS Network Manager Provides

### SYSTEM REQUIREMENTS

The Video Management System (VMS) Network Manager must be installed on a dedicated standalone server running the Windows 2000 or Windows XP platform.

The Video Management System (VMS) Network Manager communicates with RADVISION elements using a variety of industry-standard protocols, such as SNMP, XML, Telnet and FTP.

---

**Note** Ports supporting these protocols must be available in each element in order to be managed by the Video Management System (VMS) Network Manager.

---

### WHAT THE VMS NETWORK MANAGER PROVIDES

The Video Management System (VMS) Network Manager is a fully compliant network management system that provides network-wide functionality for RADVISION elements.

### NETWORK STATUS

The Video Management System (VMS) Network Manager provides network administrators with the most critical network status information at a glance, including:

- Element information—Total number of elements, the number of faulty elements and the number of elements that are offline.
- Call information—Total number of calls in the network, the number of point-to-point calls and the number of conferences.
- Endpoint information.
- Bandwidth information—Inter-zone bandwidth usage.
- B-channel usage information.

All network status information is updated in real time by the Video Management System (VMS) Network Manager database.

### VIEWING CALLS AND CONFERENCES

The Video Management System (VMS) Network Manager provides network administrators with a view of all calls and conferences currently taking place over the network. With these view, administrators can quickly determine:

#### Calls

- Source and destination alias
- Source and destination gatekeeper
- Allocated resources

One click control allows the network administrator to view call details or to access the source or destination gatekeeper element manager per call. For more information about viewing calls with the Video Management System (VMS) Network Manager, see the [Conferences and Calls View](#) chapter.

### Conferences

- The MCU controlling the conference.
- Conference ID.
- Conference type.
- Video and bandwidth settings.
- Number of participants—including the current number, the number reserved and the number of local participants.

One click control allows the network administrator to link to the MCU Conference Control interface to assume full control of any conference in the list. For more information about viewing conferences with the Video Management System (VMS) Network Manager, see the [Conferences and Calls View](#) chapter.

## AUTO-DETECT

The Video Management System (VMS) Network Manager uses an automatic detection mechanism for discovering the RADVISION elements present on the network. This information is saved to the Video Management System (VMS) Network Manager database and is used to create the various network views available via the Video Management System (VMS) Network Manager interface. Auto-detect can be run at regular intervals and whenever the server is restarted. Auto-detect can also be manually initiated at any time. For more information, see [Multiple Network Views](#) on page 5

---

**Note** The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed. For more information, see the [Network Tree View](#) chapter.

---

## What the VMS Network Manager Provides

### BASIC ELEMENT CONFIGURATION

The Video Management System (VMS) Network Manager provides network administrators with the ability to view and edit the most commonly used configuration parameters of various elements in the network, such as MCU elements, ECS elements and Gateways.

### MCU CONFIGURATION

Using the Video Management System (VMS) Network Manager, network administrators can configure the following MCU parameters:

- IP address
- MCU type (such as MCU or MP Only)
- DCS parameters, if applicable

### ECS CONFIGURATION

Using the Video Management System (VMS) Network Manager, network administrators can configure the following ECS parameters:

- Dial plan version
- Registration and routing modes

### GATEWAY CONFIGURATION

Using the Video Management System (VMS) Network Manager, network administrators can configure the following Gateway parameters

- Gatekeeper IP address
- Location

### CISCO MCM CONFIGURATION

Using the Video Management System (VMS) Network Manager, network administrators can configure the following Cisco MCM parameters:

- GKTMP port
- LRQ hop count

---

**Note** For more information about configuring elements with the Video Management System (VMS) Network Manager, see the [Network Tree View](#) chapter.

---

### VIEWING ALARMS AND EVENTS

The Video Management System (VMS) Network Manager provides network administrators with a list of the alarms currently active in any of the elements in the network. The list is constantly updated by the system, ensuring that any problems are located without delay. One-click access from any alarm directly to the administration interface of the device ensures that problems can be investigated and dealt with immediately.

In addition, the Video Management System (VMS) Network Manager provides a list of all events that have taken place in the network. This list can be filtered by the network administrator, as required. For more information, see the [Alarms View](#) chapter.

### CONNECTING TO ELEMENT MANAGERS

The Video Management System (VMS) Network Manager provides one-click access to the administration interfaces (**element managers**) of all the elements in the network, regardless of type, without the need to log in individually to each element. This gives network administrators the ability to perform a full range of management and configuration procedures on individual elements. Links to element managers can be found throughout the Video Management System (VMS) Network Manager interface, including the Alarm and Event views, the Conferences view and the various network views.

### CONNECTING TO TERMINAL MANAGERS

In addition to providing one-click access to element managers, the Network Tree view of the Video Management System (VMS) Network Manager also provides one-click access to the web-based management systems of some common endpoints registered to the network.

### CENTRALIZED LOG MANAGEMENT

The Video Management System (VMS) Network Manager provides centralized log management at both the network and element type levels. Using the Settings View, network administrators can define the size of the network log file, as well as the number of backups to maintain and the level of activity detail to include in the log. In addition, the Video Management System (VMS) Network Manager can be used to keep logs for those elements types, such as MCU elements and Gateways, that do not maintain log files of their own.

### MULTIPLE NETWORK VIEWS

The Video Management System (VMS) Network Manager provides network administrators with multiple options for viewing the elements in the network, including a Network Tree view with elements arranged in a tree structure according to zone, a Network Table view that displays a single, unified list of all network elements, as well as a Network Map view that displays elements and network status information in a graphic, multi-layered format. For more information about the network views, see the [Network Tree View](#) chapter.

The Network Tree view features a default view based on the zones in the IP conferencing network. However, the Video Management System (VMS) Network Manager also enables network administrators to create custom views. By creating folders and placing elements into them, administrators can view the network in whatever arrangement works best, such as dividing the network according to location. The views created in the Network Tree view can also be displayed in graphic format in the Network Map view.

## What the VMS Network Manager Provides

For more information about creating custom views, see the [Finding and Managing Elements](#) chapter.

### **OFFLINE CONFIGURATION**

The Video Management System (VMS) Network Manager can hold configuration details for offline elements and apply settings as each element goes online. Both added elements and existing elements can be configured to allow offline configuration.

### **ENC FUNCTIONALITY**

The Video Management System (VMS) Network Manager replaces the ENC functionality supported in some versions of the RADVISION ECS and allows administrators to re-configure the ENC support settings globally so that all ECSs operate under the management of the Video Management System (VMS) Network Manager. Administrators can manage and configure gatekeeper network hierarchy parent, child and neighbor relationships. Administrators can select each element node to view the relevant tables for defining the IP addresses of related elements.

This functionality is supported by the drag and drop management feature for automatic re-configuration of parent and child settings and by the offline management capability of the Video Management System (VMS) Network Manager which allows pre-configuration of network hierarchy relationships.

### **NETWORK SUBSETS**

The Video Management System (VMS) Network Manager enables administrators to define subsets of the network and restrict users with specific profiles to control certain network areas. Administrators can configure the network subsets using criteria to include or exclude certain zones and element types.

### **CISCO MCM SUPPORT**

The Video Management System (VMS) Network Manager provides extensive monitoring, configuration and management capabilities of the Cisco MCM including local and remote zone setup, bandwidth policies, prefixes, logs, debugging and Telnet commands.

### **DRAG AND DROP MANAGEMENT**

The Video Management System (VMS) Network Manager provides Network Tree drag and drop functionality for convenient element hierarchy management. Element addressing details are automatically updated in the tables of related elements. This feature can be used during offline configuration.

### **MONITORING CALLS**

The Video Management System (VMS) Network Manager supports a comprehensive calls view detailing endpoint information, source and destination gatekeepers, bandwidth settings and call disconnection capabilities.

# 2

## NETWORK TREE VIEW

---

### WHAT'S IN THIS CHAPTER

This chapter provides a description of the network tree view available in the Video Management System (VMS) Network Manager, and includes the following:

- [About the Network Tree View](#)
- [Monitor Tab](#)
- [Elements Tab](#)
- [Alarms Tab](#)
- [Events Tab](#)
- [Calls Tab](#)
- [Configure Tab](#)
- [Logs Tab](#)
- [Access Tab](#)
- [Additional Network Tabs](#)
- [Additional ECS Tabs](#)
- [Additional Endpoints Tab](#)
- [Additional MCU Tabs](#)
- [Additional Gateway Tab](#)
- [Additional Cisco MCM Tabs](#)
- [Additional DCS Tab](#)

### ABOUT THE NETWORK TREE VIEW

The Network Tree view organizes the information about the IP conferencing network into one or more tabbed views, each of which lists the elements in the network in a tree structure (Figure 2-1). By default, the tree divides the elements by zones.

### MANAGING ZONES

The Network Tree displays the network according to zones which are defined by gatekeepers. There is a zone node in the tree for each gatekeeper in the network, or pair of gatekeepers where an alternate gatekeeper is used. Each zone includes a gatekeeper element with which the zone is defined and other elements such as MCUs and Gateways which are registered in that zone. An element can be **managed**, **unmanaged** or **inferred**. A zone is not an element that can be managed.

#### Elements

- **Managed**—The element exists in the Video Management System (VMS) Network Manager database and provides monitoring information and access to configuration settings.
- **Inferred**—The element does not exist in the Video Management System (VMS) Network Manager database but may appear as an inferred element because a managed element refers to that element.

For example, a gatekeeper is inferred when a managed element is registered to that gatekeeper zone, but the gatekeeper is not managed by the Video Management System (VMS) Network Manager.

- **Unmanaged**—The element exists in the Video Management System (VMS) Network Manager database but has no open communication channels with the Video Management System (VMS) Network Manager and provides no monitoring information or access to configuration settings.

An element may be unmanaged when the Video Management System (VMS) Network Manager license limitations have been exceeded or when the user manually sets the element as unmanaged.

## Zones

Gatekeeper zones can be managed in a hierarchical structure with parents, neighbors and children. This hierarchical structure is reflected in the Network Tree view and can be arranged using the Video Management System (VMS) Network Manager drag and drop capabilities or by configuring elements offline in place of the ECS Network Configurator (ENC).

A zone cannot be deleted manually from the tree but is automatically deleted in one of the following circumstances:

- A managed gatekeeper in the zone is deleted from the tree.
- The gatekeeper is inferred and the last remaining managed element in the zone is deleted from the tree.

## DRAG AND DROP MANAGEMENT

The drag and drop feature enables quick configuration of the network hierarchy and automatically reconfigures element relationships by automatically assigning and updating the appropriate details of the elements with which the managed element registers.

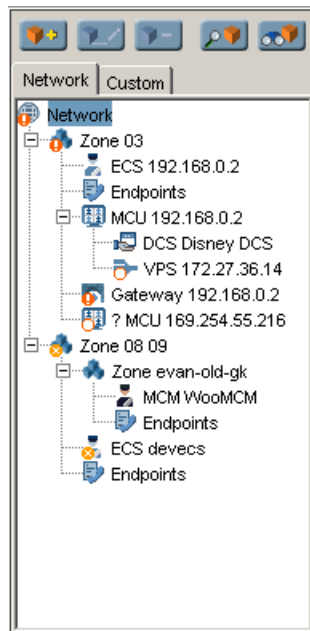
You can configure the following element relationships using the drag and drop feature:

- Gatekeeper Parent <> Child
- Gatekeeper <> MCU/Gateway
- MCU <> MP
- MCU <> DCS

Gatekeeper parent and child element tables are updated for each element in the relationship. MCU and Gateway elements are updated with the appropriate gatekeeper IP address. MP and DCS elements are updated with the relevant IP address and configuration details for registering with the MCU.

## NETWORK TREE INTERFACE

The Network Tree view enables you to select an element in the tree to display specific information, such as alarms, traps and services related to the element. In addition to the default view where elements are divided into zones, you can add custom views to organize the elements according to criteria you define, such as location or customer use. You can add folders to the custom views and organize the elements in these folders, as required. For more information, see the [Finding and Managing Elements](#) chapter.



**Figure 2-1** Network Tree

The Network Tree contains one default tab—the **Network** tab, which displays the network root, the zones into which the network is divided and the elements contained in each zone. The tree can be expanded and collapsed, as required. Each element type is represented by a different icon, and the current status of the element is superimposed on that icon.

## ELEMENT CONTROL

The Network Map view contains five buttons which allow you to perform the following:

- Add element
- Edit element
- Delete element
- Find element
- Auto-detect elements

For more information about these actions, see the [Finding and Managing Elements](#) chapter.

---

**Note** These buttons are also available in [Network Table View](#) and the [Network Map View](#).

---

You can perform auto-detect in the Network Tree view, which enables you to search the network for new or modified elements and add them to the Video Management System (VMS) Network Manager database.

When you select an element (or endpoint) in the tree, the main display area changes to display the relevant tabs. Some of the tabs are common to the different elements types, while others are unique to a particular element type. The main display area also contains the Network Tree buttons, which are described in the following section.

NETWORK TREE  
BUTTONS

Selected tabs in the Network Tree view also include the following buttons:

**Upload**

In all tabs where you can type information directly into a field, click **Upload** to update the information in the database.

**Refresh**

Click **Refresh** to download updated information from the database.

---

**Note** Click the pin icon at the top of any tab to enable information about two elements in the tree to be displayed simultaneously.

---

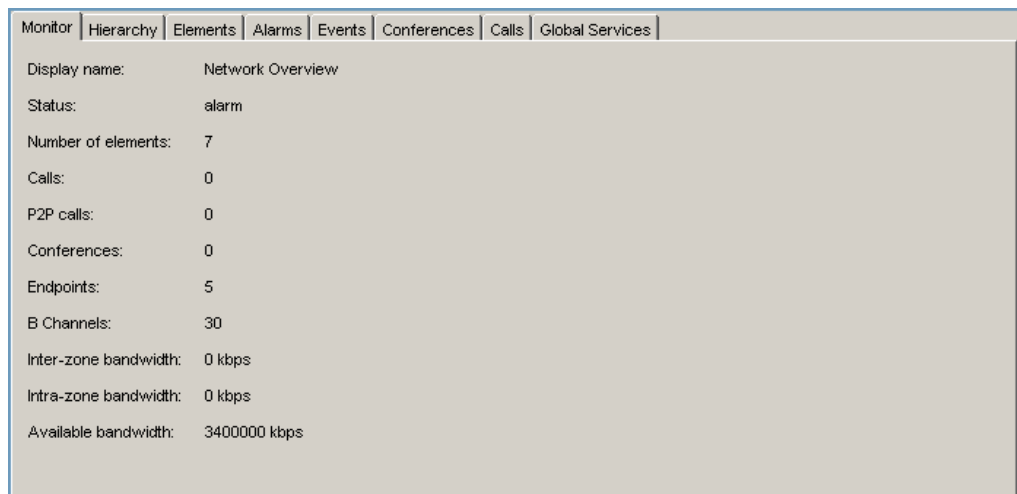
## Monitor Tab

### NETWORK TREE TABS

Selecting items in the Network Tree displays one or more tabs on the right-hand side of the main display area. Network Tree tabs provide a variety of information about the selected item, such as its current status and alarms, the services configured for the item, and any special access information. In addition, you can configure the most commonly used parameters of each element type.

### MONITOR TAB

The **Monitor** tab, which is the default tab displayed when an item is selected in the Network Tree view, displays general information about the item.



Monitor	Hierarchy	Elements	Alarms	Events	Conferences	Calls	Global Services
Display name:	Network Overview						
Status:	alarm						
Number of elements:	7						
Calls:	0						
P2P calls:	0						
Conferences:	0						
Endpoints:	5						
B Channels:	30						
Inter-zone bandwidth:	0 kbps						
Intra-zone bandwidth:	0 kbps						
Available bandwidth:	3400000 kbps						

**Figure 2-2** Network Tree—Monitor Tab

---

**Note** When the gatekeeper in a zone is unmanaged or inferred, the calls, bandwidth and registration information is displayed as zero.

---

The information displayed in the **Monitor** tab is dependent on the item selected in the tree.

At the network and zone level, the tab displays the following information:

- Display name—Name of the selected zone or element.
- Status.
- Number of elements.
- Calls.
- Point-to-point calls.
- Number of conferences.
- Number of endpoints registered in the network.
- Number of B channels.
- Bandwidth information—Inter-zone, intra-zone, available bandwidth.

---

**Note** Call and conference statistics for OnLan Gateways and OnLan MCUs are not included in summary details for selected elements.

---

At the element level, the **Monitor** tab displays the name of the element, the IP address, the version number and its current online status. In addition, the tab includes information relevant to the type of element selected. For example, when an MCU is selected in the tree, the **Monitor** tab includes the current alarm status, the current number of conferences, and so on.

---

**Note** Click the link to display the element manager for the selected element.

---





## ELEMENTS TAB

The **Elements** tab displays a table of all elements related to the network, zone or folder selected in the tree.

Status	Element Type	Name	IP Address	Version	Location	Gatekeeper Calls	Usage
offline	INVISION E...	192.168.0.2	192.168.0.2	1.0.8.8SW	GoFigure		
offline	ECS	evan-old	192.168.0.144	3.0.3.7			
offline	ECS	devecs	192.168.0.121	3.0.3.7			
offline	INVISION M...	192.168.0.2	192.168.0.2	2.2.56	GoFigure		
offline	INVISION G...	192.168.0.2	192.168.0.2	1.1.0.9.2	GoFigure		

**Figure 2-3** Network Tree—Elements Tab

The table in the **Elements** tab includes the following information about each element:

- Element status, indicated by an icon, as follows:
  -  Online
  -  Unmanaged
  -  Offline
  -  Faulty
- Element type (MCU, ECS and so on)
- Element name (acts as a link to its element manager)
- IP address
- Version number
- Location (as defined in the **Configure** tab of each element)
- Number of calls
- Traffic usage versus capacity

Any element listed in the tree with a question mark (?) is considered to be an inferred element by the system. This means that the element is not listed in the database, but is presumed to exist because another known element refers to the element. Inferred elements cannot be managed, therefore you are recommended either to initiate auto-detect to discover an element, add an element manually or connect an inferred element manually.

## ADDING AN ELEMENT

Click the **Add** button to add new elements. The **Add Element** dialog box is displayed, enabling you to add new elements manually to the database. Type a display name and enter the IP address. Select an element type and indicate whether the element is managed and configurable offline. Click **OK** to add the element to the network tree. In addition, you can modify, remove and find existing elements. For more information, see the [Finding and Managing Elements](#) chapter.

## ALARMS TAB




The **Alarms** tab displays a table of all current alarms related to the item selected in the tree. You can view alarms per element, zone or the entire network in one view.

Monitor   Hierarchy   Elements   <b>Alarms</b>   Events   Conferences   Calls   Global Services			
Severity	Date & Time	Message	Element
 warning	May 12, 2003 7:42:03 AM	Cisco Proxy override reset exter...	devecs (ECS - 192.168.0.121)
 critical	May 12, 2003 7:35:31 AM	PRI 1 remote frame alignment fail...	192.168.0.2 (INVISION Gateway)
 critical	May 12, 2003 7:35:31 AM	PRI 1 local frame alignment failure	192.168.0.2 (INVISION Gateway)

**Figure 2-4** Network Tree—Alarms Tab

## Events Tab

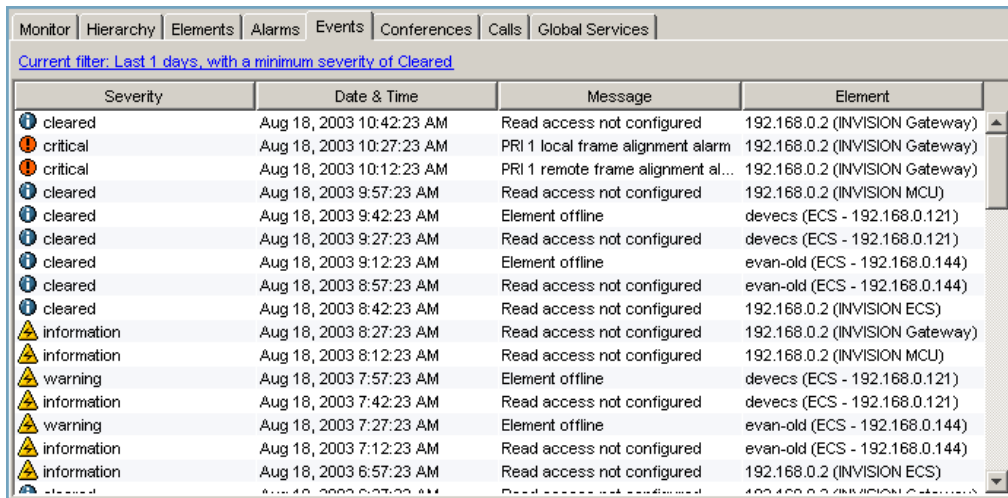
The **Alarms** tab includes the severity of each alarm, the time the event occurred and the alarm message that is related to the selected element. Alarm severity levels include the following:


















-  Major/Minor/Critical
-  Information
-  Warning

You can click the link in the right-hand column to access the relevant element managers. For more information, see the [Alarms View](#) chapter.

## EVENTS TAB

The **Events** tab displays a table of the events that have occurred in the system, which are related to the item selected in the tree.



Severity	Date & Time	Message	Element
 cleared	Aug 18, 2003 10:42:23 AM	Read access not configured	192.168.0.2 (INVISION Gateway)
 critical	Aug 18, 2003 10:27:23 AM	PRI 1 local frame alignment alarm	192.168.0.2 (INVISION Gateway)
 critical	Aug 18, 2003 10:12:23 AM	PRI 1 remote frame alignment al...	192.168.0.2 (INVISION Gateway)
 cleared	Aug 18, 2003 9:57:23 AM	Read access not configured	192.168.0.2 (INVISION MCU)
 cleared	Aug 18, 2003 9:42:23 AM	Element offline	devecs (ECS - 192.168.0.121)
 cleared	Aug 18, 2003 9:27:23 AM	Read access not configured	devecs (ECS - 192.168.0.121)
 cleared	Aug 18, 2003 9:12:23 AM	Element offline	evan-old (ECS - 192.168.0.144)
 cleared	Aug 18, 2003 8:57:23 AM	Read access not configured	evan-old (ECS - 192.168.0.144)
 cleared	Aug 18, 2003 8:42:23 AM	Read access not configured	192.168.0.2 (INVISION ECS)
 information	Aug 18, 2003 8:27:23 AM	Read access not configured	192.168.0.2 (INVISION Gateway)
 information	Aug 18, 2003 8:12:23 AM	Read access not configured	192.168.0.2 (INVISION MCU)
 warning	Aug 18, 2003 7:57:23 AM	Element offline	devecs (ECS - 192.168.0.121)
 information	Aug 18, 2003 7:42:23 AM	Read access not configured	devecs (ECS - 192.168.0.121)
 warning	Aug 18, 2003 7:27:23 AM	Element offline	evan-old (ECS - 192.168.0.144)
 information	Aug 18, 2003 7:12:23 AM	Read access not configured	evan-old (ECS - 192.168.0.144)
 information	Aug 18, 2003 6:57:23 AM	Read access not configured	192.168.0.2 (INVISION ECS)
 cleared	Aug 18, 2003 6:42:23 AM	Read access not configured	192.168.0.2 (INVISION Gateway)

**Figure 2-5** Network Tree—Traps Tab

The **Events** tab includes the event severity level, the date and time of the event and the event message. You can click the link in the **Element** column to access the relevant element managers. Click the link above the table to display the **Filter Traps** dialog box, which enables you to filter the events displayed in the tab by date and severity level. For more information, see the [Alarms View](#) chapter.

## CONFERENCES TAB

The **Conferences** tab provides a table for viewing the current status of all conferences being hosted on the network, zone or selected MCU.

MCU	Conference ID					Total Particip...	Reserved Pa...	Video bit rate	Zones
172.27.14.1	141010					4	4	320 kbps	4
172.27.36.248	248103842340					6	7	320 kbps	03

**Figure 2-6** Conferences Tab

The table includes the following information:

- MCU—IP address of the MCU on the which the conference is being hosted. Click on the link to view the element manager of the MCU (Administrator).
- Conference ID—Conference ID number. Click on the link to view the conference manager of the MCU (Conference Control).
- Layout icon—Video layout configuration of the conference.
- Camera icon—Indicates whether video is enabled for the conference.
- Speaker icon—Indicates whether audio is enabled for the conference.
- Data icon—Indicates whether data support is enabled for the conference.
- Total Participants—Number of current participants.

## Conferences Tab

- Reserved Participants—Number of reserved participants.
- Video Bit Rate—Maximum bit rate for the conference.
- Zone—Zone in which the conference is taking place.

Click the **Find** button above the table to display the **Find Conference** dialog box, which enables you to locate a particular conference in the table. For more information about the fields displayed in the **Conferences** tab, see the [Conferences and Calls View](#) chapter.

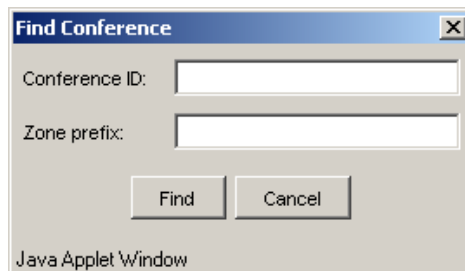
---

**Note** You can access the element manager of the MCU (Administrator) by clicking the link in the left hand column of each table row.

---

## FINDING A CONFERENCE

Click **Find** to display the **Find Element** dialog box, which enables you to locate a particular conference in the table. Enter the conference ID or the zone prefix and click **Find**. The row in the table matching your search criteria is highlighted.



**Figure 2-7** Find Conference Dialog Box

---

**Note** You can use the asterisk [\*] wildcard when searching for conferences.

---

## CALLS TAB

The **Calls** tab displays a table providing details of each call currently taking place on the selected element including the source and destination aliases and gatekeepers of the calling parties, call start time and allocated bandwidth.

Source Alias	Destination Alias	Source Gatekeeper	Destination Gatekee...	Start Time	Allocated BW (kbps)
2222	2081	devecs (ECS - 192.1...	evan-old (ECS - 192....	Jun 12, 2002 9:10:00...	0
evan	2081	devecs (ECS - 192.1...	evan-old (ECS - 192....	Jun 12, 2003 9:09:00...	100

**Figure 2-8** Network Tree—Calls Tab

The **Calls** tab allows you to disconnect calls either for each selected call or globally for all calls. You can also display extended calls by clicking on the table row and a call search option allows you to search by alias, IP address of the endpoint, service or conference ID.

## CONFIGURE TAB

The **Configure** tab displays the most commonly needed configuration parameters for the element selected in the tree.

The information displayed in the **Configure** tab is dependent on the type of element selected in the tree including the following:

- ECS
- MCU
- Gateway
- DCS
- MCM

---

**Note** When a network or a zone is selected in the tree, the **Configure** tab is not available.

---

## ECS

The ECS **Configure** tab allows you to configure ECS addressing, registration mode, routing mode, physical location, dial plan version, prefix handling and allow access by the ECS to a central database for network hierarchy management by the ECS Network Configurator (ENC).

The screenshot shows a web-based configuration interface for an ECS. At the top, there is a navigation bar with tabs: Monitor, Alarms, Events, Calls, Configure (selected), Services, Global Services, Bandwidth, Parent, Neighbors, Children, Logs, and Access. Below the navigation bar, the configuration fields are as follows:

- ECS ID: 172.20.36.36
- Registration mode: All (dropdown menu)
- Merge predefined and online aliases upon registration
- Routing mode: Call Setup (Q.931) and Call Control (H.245) (dropdown menu)
- Location: Chassis 2
- Dial plan version: Version 2 (dropdown menu)
- Strip Prefixes
- Strip Gateway Prefixes
- LRQ hop count: 0
- Use Central Database

**Figure 2-9** Network Tree—ECS: Configure Tab

You can configure the following parameters in the **Configure** tab of an ECS:

- ECS ID
- Registration mode:
  - **All**—Open zone policy where the ECS accepts any legal registrations from any endpoint.
  - **None**—Closed zone policy that prevents the ECS from accepting any registrations.
  - **Predefined**—Strict zone policy where the ECS only accepts registrations from predefined endpoints.
- If required, select **Merge predefined and online aliases upon registration** to enable the ECS to assign predefined aliases, identified either by alias or IP address/port number, to an endpoint when that endpoint registers.
- Routing mode:
  - **Direct**—Routes calls directly with ECS intervention.
  - **Call Setup (Q.931)**—Routes the Call Setup channel through the ECS.
  - **Call Setup (Q.931) and Call control (H.245)**—Enables the H.245 Proxy to route the Call Setup channel and the Control channel through the ECS.
- Location—Enter a string specifying the physical device on which the ECS installed, for display purposes.
- Dial plan version:
  - **Version 1**—Default setting.
  - **Version 2**—Enables the parameters defined in the **Dial Plan** section of the **Settings** tab in the RADVISION ECS and enables the [Global Services Tab](#), [Parent Tab](#) and [Children Tab](#).
- Strip prefixes—When selected, enables the ECS to strip zone prefixes in non-gateway calls (internal IP network calls).
- Strip Gateway Prefixes—When selected, enables the ECS to strip zone prefixes in gateway calls (IP-to-ISDN network calls).
- LRQ hop count—Enter a whole number from 1 to 98 to set the maximum number of gatekeepers that an LRQ message can pass. The LRQ hop count prevents deadlocking when an LRQ loop occurs involving ECS gatekeepers and non-RADVISION gatekeepers. At each gatekeeper in the loop, the LRQ hop count

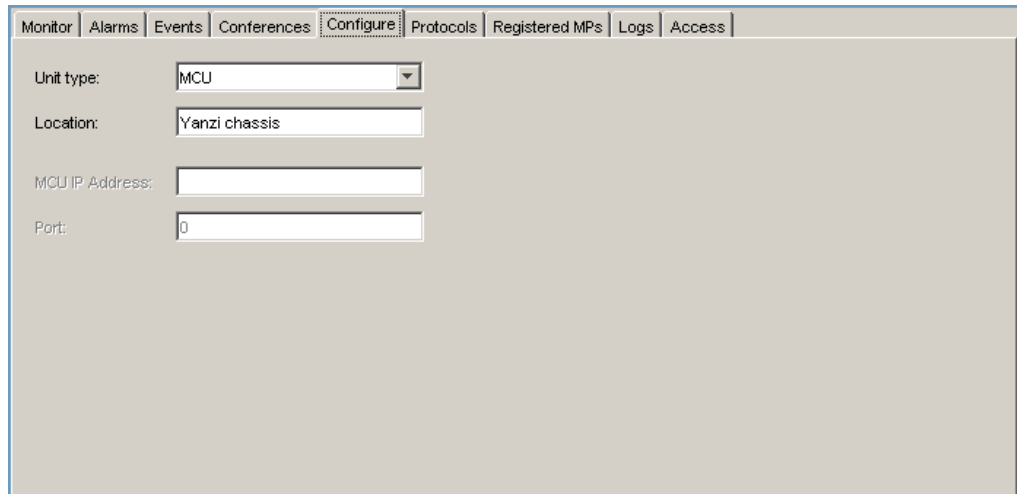
## Configure Tab

is reduced by 1 when that gatekeeper receives an LRQ. When a gatekeeper receives an LRQ and the LRQ hop count is 1, that gatekeeper reduces the LRQ hop count to 0 and sends an LRJ message.

- Use Central Database—When selected, enables the ECS to access the Central Database used by the ENC for network hierarchy management. This option is deselected automatically if you select the **Enable ECS Central Hierarchy Management** option in the [Hierarchy Tab](#).

## MCU

The MCU **Configure** tab enables you to set the unit type and configure addressing details.



Monitor	Alarms	Events	Conferences	Configure	Protocols	Registered MPs	Logs	Access
Unit type:	MCU							
Location:	Yanzi chassis							
MCU IP Address:								
Port:	0							

**Figure 2-10** Network Tree—MCU: Configure Tab (MCU version 3.0)

You can configure the following parameters in the **Configure** tab of an MCU according to the MCU version:

- **MCU version 3.x and later:**
  - ❖ Use internal gatekeeper—For use on Gateways and MCUs hosted on the INVISION platform.
  - **Unit Type:**
    - ❖ **MCU**—The MCU and MP components in the unit work together to provide Call Setup, conference control and media processing.
    - ❖ **MP Only**—The MP (Multipoint Processor) unit works in a clustered arrangement operating under the control of an MCU.
  - **Location**—Enter a string identifying the physical location of the MCU device.
  - **MCU IP Address**—MCU IP address. Configurable only on MP units.
  - **Port**—MCU communication port. Configurable only on MP units.
- **MCU Version 2.x**
  - Use internal gatekeeper—For use on Gateways and MCUs hosted on the INVISION platform.
  - **Gatekeeper IP Address**—IP address with which the MCU registers.
  - **Unit Type:**
    - ❖ **MCU**—Single station MCU providing Call Setup, conference control and media processing.
    - ❖ **MCU Clustered**—MCU operating as a Multipoint Controller that can manage up to six MP Only units in a clustered layout.
    - ❖ **MP Only**—The MP (Multipoint Processor) unit works in a clustered arrangement operating under the control of an MCU.

## Configure Tab

- Enable DCS—Enables the MCU to register to the configured DCS address.
  - ◆ DCS IP Address—IP address of the DCS with which the MCU registers.
  - ◆ Location—Type a description of the DCS location.

## GATEWAY

You can configure the following parameters in the **Configure** tab of a gateway:

- The IP address of the gatekeeper which the Gateway registers A string identifying the physical location of the Gateway.
- Use internal gatekeeper—For use on Gateways and MCUs hosted on the INVISION platform.

## DCS

You can configure the following parameters in the **Configure** tab of a DCS:

- Licensed ports—The number of licensed ports on the DCS.
- Enable Telnet—When selected, enables communication with the DCS via Telnet.
- Telnet port—DCS Telnet communication port.

## MCM

You can configure the following parameters in the **Configure** tab of a Cisco MCM:

- Gatekeeper enabled (no shutdown)—When selected, enables the Cisco MCM gatekeeper.
- GKTMP port—Port on which the Video Management System (VMS) Network Manager communicates with the Cisco MCM using the GKTMP communication protocol to get calls and registration information from the MCM.
- LRQ hop count—Enter a whole number from 1 to 98 to set the maximum number of gatekeepers that an LRQ message can pass. The LRQ hop count prevents deadlocking when an LRQ loop occurs involving ECS gatekeepers and non-RADVISION gatekeepers. At each gatekeeper in the loop, the LRQ hop count is reduced by 1 when that gatekeeper receives an LRQ. When a gatekeeper receives an LRQ and the LRQ hop count is 1, that gatekeeper reduces the LRQ hop count to 0 and sends an LRJ message.

## LOGS TAB

The **Logs** tab enables the Video Management System (VMS) Network Manager to keep a log of operations for the element selected in the tree.

---

**Note** A log of operations is not available for endpoints supported by the Video Management System (VMS) Network Manager. A log tab is not available for endpoints when selected in the Network Tree view.

---

**Figure 2-11** Network Tree—Logs Tab

The information displayed in the **Logs** tab is dependent on the type of element that is selected in the tree. The **Logs** tab enables you to define the log for the various elements, as follows:

### ECS

Select **Save logs** and select the level of detail to include in the log.

### MCU

Select **Save logs**, type the log file name and define the level of detail to include in the log.

## Access Tab

### Gateway

Select **Save logs**, type the log file name and define the level of detail to include in the log.

### MCM

Select **Save logs**, type the log file name and define the level of detail to include in the log.

---

**Note** In addition, you can click the link to view the logs directory from any of the **Log** tabs described above. For more information on log parameters, see the [Settings View](#) chapter.

---

## ACCESS TAB

The **Access** tab allows you to define custom SNMP access settings for the currently selected element. Custom settings differ from the default settings configured for elements of this type in the **Element Access** tab of the **Settings** section.

Access settings allow access to element managers without having to first go through the **Login** screens for each element. For more information about access settings, see the [Settings View](#) chapter.

The screenshot shows a web-based configuration interface for the 'Access Tab'. At the top right, there are 'Upload' and 'Refresh' buttons. Below them is a navigation menu with tabs for 'Monitor', 'Alarms', 'Events', 'Calls', 'Configure', and 'Services'. Under 'Configure', there are sub-tabs for 'Global Services', 'Parent', 'Children', 'Neighbors', 'Subzones', 'Bandwidth', 'Logs', and 'Access'. The 'Access' tab is currently selected. The main content area contains a checkbox labeled 'Use default' which is checked. Below this are five input fields: 'SNMP read community:' with a masked value '\*\*\*\*\*', 'SNMP write community:' with a masked value '\*\*\*\*\*', 'User name:' with the value 'admin', 'Password:' which is empty, and 'HTTP port:' with the value '80'.

**Figure 2-12** Network Tree—Access Tab

### Use default

Check to use the default access settings for the element type. When unchecked, all other tab options are disabled. Availability of the following access configuration parameters depends on the element type selected:

### Element type

Drop-down list displayed when the selected element is an inferred gatekeeper. Choose ECS or MCM to display the appropriate access configuration parameters.

### Connect

Click to connect to an inferred element and add it to the Video Management System (VMS) Network Manager database. The access parameters of the element must be correctly configured for the operation to succeed.

Configure the following parameters:

- SNMP read community
- SNMP write community
- User name
- Password
- HTTP port
- Telnet password (MCU, DCS, Cisco MCM)
- Telnet user name (Cisco MCM only)
- Enable Telnet (Cisco MCM only)

---

**Warning** The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed.

---

---

**Tip** You can view SNMP Community names by selecting the **View SNMP Community names** option in the **View** menu, if the option is already enabled using the [Configuration Utility](#).

---

## Additional Network Tabs

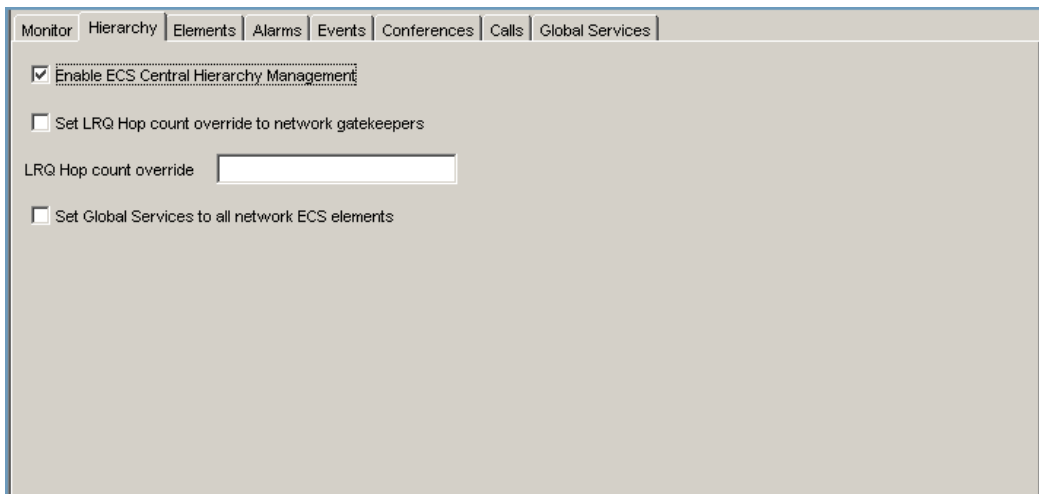
### ADDITIONAL NETWORK TABS

When the Network node is selected in the tree, additional tabs are displayed, allowing you to centrally manage the ECS hierarchy on the network and configure global services, including the following:

- [Hierarchy Tab](#)
- [Global Services Tab](#)

### HIERARCHY TAB

The **Hierarchy** tab allows you to enable the Video Management System (VMS) Network Manager to perform central ECS hierarchy management of ECS Parent, Children and Neighbor relationships and configure global services. This option replaces the ECS Network Configurator (ENC).



The screenshot shows a web interface with a tabbed menu at the top containing: Monitor, Hierarchy, Elements, Alarms, Events, Conferences, Calls, and Global Services. The 'Hierarchy' tab is selected. Below the tabs, there are several configuration options:

- Enable ECS Central Hierarchy Management
- Set LRQ Hop count override to network gatekeepers
- LRQ Hop count override:
- Set Global Services to all network ECS elements

**Figure 2-13** Network Tree—Hierarchy Tab (Network)

You can configure the following parameters in the **Hierarchy** tab:

- Enable ECS Central Hierarchy Management (ENC users)—Automatically disables the **Use Central Database** option for ECS elements which support ENC functionality to allow Video Management System (VMS) Network Manager to manage the gatekeeper hierarchy.
- Set LRQ Hop count override to network gatekeepers—Configures the LRQ hop count globally for all gatekeepers including the ECS and Cisco MCM.
- LRQ Hop count override—Enter a whole number from 1 to 98 to set the maximum number of gatekeepers that an LRQ message can pass. The LRQ hop count prevents deadlocking when an LRQ loop occurs involving ECS gatekeepers and non-RADVISION gatekeepers. At each gatekeeper in the loop, the LRQ hop count is reduced by 1 when that gatekeeper receives an LRQ. When a gatekeeper receives an LRQ and the LRQ hop count is 1, that gatekeeper reduces the LRQ hop count to 0 and sends an LRJ message.
- Set Global Services to all network ECS elements—Configures the global services, defined in the [Global Services Tab](#), for all ECS elements supporting Dial Plan Version 2.0.

## GLOBAL SERVICES TAB

The **Global Services** tab displays the list of global services which can be configured for all ECS elements in the network.

---

**Note** The **Global Services** tab is also enabled when you select ECS elements configured for Dial Plan Version 2.0. INVISION ECS and ECS version 1.0 do not support Dial Plan Version 2.0. For more information, see the [Configure Tab](#) section.

---

## Additional Network Tabs

Prefix	Description	Predefined
04	Fall back service	no
02	Service 02	no
34	Generic conference	no

**Figure 2-14** Network Tree—Global Services Tab (Network)

The **Global Services** tab displays the following information:

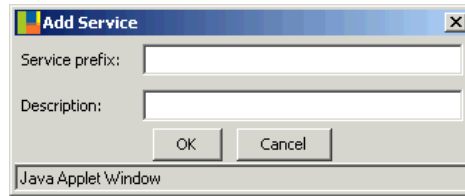
- Services prefix used to access the service
- Service description
- Whether the global service is being retrieved from the Central Database

### ADDING A GLOBAL SERVICE

Click **Add** to display the **Add Service** dialog box, which enables you to configure new global services, as follows:

- Type the prefix used to access the global service.
- Type a description of the global service.

Click **OK**. The new global service is added to the displayed list.



**Figure 2-15** Add Service Dialog Box—Global Services

---

**Note** You can modify and delete existing global services using the **Edit** and **Delete** buttons.

---

## ADDITIONAL ECS TABS

When an ECS is selected in the tree, additional tabs are displayed, which enable you to define the manage services, define subzones, control bandwidth and configure Parent, Neighbor and Child gatekeepers, including the following:

- Services Tab
- Subzones Tab
- Bandwidth Tab (ECS version 3.2 or earlier)
- Bandwidth Tab (ECS version 3.5)
- Parent Tab
- Children Tab
- Neighbors Tab

## SERVICES TAB

The **Services** tab displays the list of predefined and online services supported by the ECS selected in the tree.

Prefix	Description	Status	Conference Hunting	In-Zone Default	Out of Zone
	Forward	predefined	no	decline	decline
	Zone prefix 1	predefined	no	allow	allow
	Zone prefix 2	predefined	no	allow	allow
	Exit Zone	predefined	no	decline	decline
60		predefined	no	allow	allow
82		predefined	no	allow	allow
83		predefined	no	allow	allow
86		predefined	no	allow	allow
9*		predefined	no	allow	allow
165		predefined	no	allow	allow
261	261	predefined	no	allow	allow
611		predefined	no	allow	allow
613		predefined	no	allow	allow
617		predefined	no	allow	allow
64*		predefined	no	allow	allow
671		predefined	no	allow	allow

**Figure 2-16** Network Tree—Services Tab (ECS)

The Services tab displays the following information:

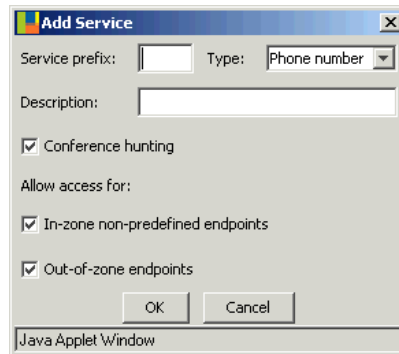
- Prefix used to access the service
- Service description
- Whether the service is predefined or online (meaning, service status)
- Whether conference hunting is enabled for the service
- Default policy for in-zone endpoints
- Service policy for out-of-zone endpoints

## ADDING A SERVICE

Click **Add** to display the **Add Service** dialog box, which enables you to configure new services supported by the selected ECS, as follows:

- Type the prefix used to access the service.
- Select the service type (**Phone number**, **Name**, **URL address**, **E-mail address**).
- Type a description of the service.
- Select whether to enable conference hunting.
- Select whether to allow access to in-zone endpoints.
- Select whether to allow access to out-of-zone endpoints.

Click **OK**. The new service is added to the displayed list.



**Figure 2-17** Add Services Dialog Box (ECS)

---

**Note** You can modify and delete existing services using the **Edit** and **Delete** buttons.

---

## SUBZONES TAB

The **Subzones** tab is available for ECS version 3.5 and enables you to view and configure subzone settings and rules for use in conjunction with the bandwidth settings.

For more information about using subzones to configure bandwidth policy, see [Appendix B](#).

## Additional ECS Tabs

### WHAT ARE SUBZONES?

A subzone is a group of endpoints belonging to a subsection of a Gatekeeper Zone. The subzone is defined by subzone rules. Subzone rules are defined according to one of the following criteria:

- IP range
- IP subnet

For more information about configuring subzone rules, see [Adding or Modifying Subzone Rules](#) on page 36.

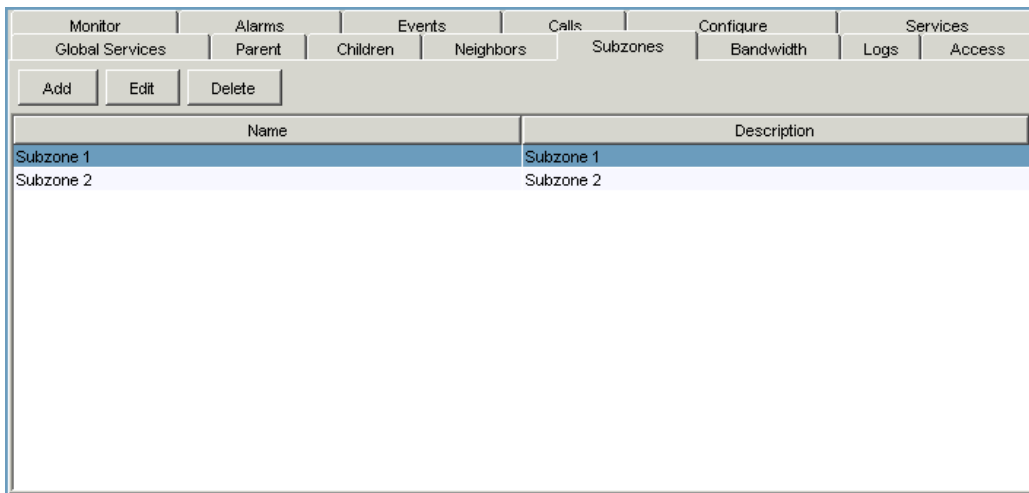
### WHY USE SUBZONES?

You can use subzone rules to control the bandwidth available between the departments of your company. You can configure a single subzone for each department including all and only the endpoints within that department. Defining appropriate subzone rules allows you to allocate a different bandwidth to connections between subzones.

Alternatively, you can use subzones to control the bandwidth available between your branch offices. Configure a single subzone for each branch office and define subzone rules that allow a different bandwidth connection per branch.

### ABOUT THE SUBZONES TAB

The **Subzones** tab allows you to configure subzones and define subzone rules.



**Figure 2-18** Network Tree—Subzones (ECS version 3.5)

The **Subzones** tab displays the following information:

- Name—Displays the name of the specified subzone.
- Description—Displays the description of the specified subzone.
- Total—Displays the total number of subzones configured.

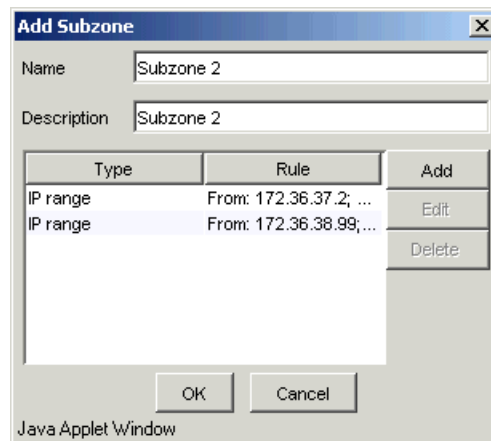
## ADDING A SUBZONE

Click **Add** to open the **Add Subzone** dialog box. Alternatively, double-click an existing subzone or select a subzone to modify and click **Edit** to open the **Edit Subzone** dialog box. The dialog box allows you to specify subzone name and description and to view, add or modify subzone rules.

The following options are available in the **Add Subzone** dialog box:

- Name—Type the required subzone name.
- Description—Type the required subzone description.
- Subzone rules—Include a list of subzone rules which provide details of the **Type** and **Rule**. Add subzone rules using the **Add Subzone Rule** dialog box. For more information, see [Adding or Modifying Subzone Rules](#) on page 36.

Click **OK** to add the new or modified subzone settings to the ECS database.



**Figure 2-19** Add Subzone Dialog Box

---

**Note** You can modify or delete existing subzones using the **Edit** and **Delete** buttons.

---

## ADDING OR MODIFYING SUBZONE RULES

Click **Add** to display the **Add Subzone Rule** dialog box. To modify an existing subzone rule, double click the required subzone rule, or select the required subzone rule and click **Edit** to display the **Edit Subzone Rule** dialog box.

You can add or modify a subzone rule based on IP range or on IP subnet. IP range is the default option.

---

**Warning** Make sure there are no clashes between any IP range rule and any subnet IP rule. Clashes between rules may cause the ECS to behave unpredictably.

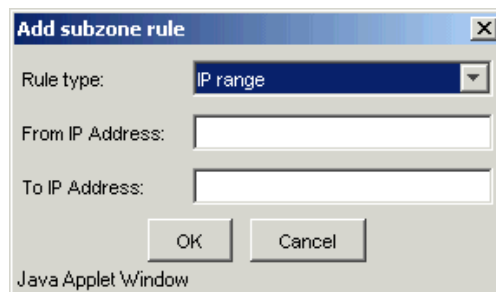
---

### IP Range Rules

The **Add Subzone Rule** and **Edit Subzone Rule** dialog boxes include the following options:

- Rule type—Displays **IP range** by default.
- From IP Address—Type the lower limit of the range of IP addresses which will activate the rule.
- To IP Address—Type the upper limit of the range of IP addresses which will activate the rule.

Click **OK** to add the new or modified subzone rules.

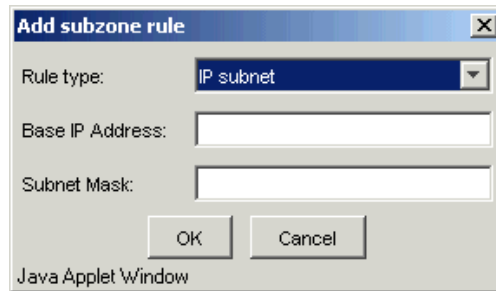


**Figure 2-20** Add Subzone Rule Dialog Box—IP Range

## IP Subnet Rules

The **Add Subzone Rule** and **Edit Subzone Rule** dialog boxes include the following options:

- Rule type—Select **IP subnet** from the drop-down list.
- Base IP address—Type the base IP address that will activate the rule.
- Subnet mask—Type the subnet mask that will activate the rule.



**Figure 2-21** Add Subzone Rule Dialog Box—IP Subnet

Click **OK** to add the new or modified subzone rules.

---

**Note** You can modify or delete existing subzones rules using the **Edit** and **Delete** buttons.

---

## BANDWIDTH TAB (ECS VERSION 3.2 OR EARLIER)

The **Bandwidth** tab for ECS elements up to version 3.2 displays bandwidth information related to the selected ECS and allows you to manage bandwidth rates for outgoing and incoming inter-zone calls, in-zone calls and per terminal. For more information about configuring bandwidth for ECS version 3.5 elements, see [Bandwidth Tab \(ECS version 3.5\)](#) on page 39. For more information about subzones, see [Subzones Tab](#) on page 33.

Monitor	Alarms	Events	Calls	Configure	Services	Global Services	Bandwidth	Parent	Neighbors	Children	Logs	Access
Maximum incoming inter-zone bandwidth (kbps):												
<input type="text" value="200000"/>												
Maximum outgoing inter-zone bandwidth (kbps):												
<input type="text" value="200000"/>												
Maximum in-zone bandwidth (kbps):												
<input type="text" value="200000"/>												
Maximum bandwidth per terminal (kbps):												
<input type="text" value="20000"/>												

**Figure 2-22** Network Tree—Bandwidth Tab (up to ECS version 3.2)

The **Bandwidth** tab displays the following information:

- Maximum incoming bandwidth (in Kbps) for calls from another zone
- Maximum outgoing bandwidth (in Kbps) for calls to another zone
- Maximum internal bandwidth (in Kbps) for calls within the zone
- Maximum bandwidth per terminal (in Kbps)

The **Bandwidth** tab enables you to define the values of each of these bandwidth settings. Click **Upload** after modifying the bandwidth values to update the settings in the ECS database.

## BANDWIDTH TAB (ECS VERSION 3.5)

The **Bandwidth** tab enables you to define subzones and subzone rules, and to determine bandwidth policy between zones and subzones for ECS version 3.5 or later. For information on subzones, see [Subzones Tab](#) on page 33.

For a sample bandwidth policy using subzones, see [Sample Topology with Subzones](#) on page 135.

Monitor	Alarms	Events	Calls	Configure	Services		
Global Services	Parent	Children	Neighbors	Subzones	Bandwidth	Logs	Access
Inter-subzone rules							
Name	Description	Allowed	Used	Available	Dedicated	Add	
Subzone Default	Subzone default b...	100000	0	100000	no	Edit	
						Delete	
Inter-zone rules							
Name	Description	Allowed	Used	Available	Dedicated	Add	
ECS Default	ECS default band...	100000	0	100000	no	Edit	
Test	iView Test	200000	0	200000	no	Delete	

**Figure 2-23** Network Tree—Bandwidth Tab (ECS version 3.5)

The **Bandwidth** tab displays the following information.

**Note** Details are displayed for both inter-subzone rules and for inter-zone rules.

- Name—Displays the name of the specified rule.
- Description—Displays the description of the specified rule.
- Allowed—Displays the total bandwidth (in Kbps) allowed by the specified rule.
- Used—Displays the bandwidth (in Kbps) currently used by calls governed by the specified rule.

- Available—Displays the free bandwidth (in Kbps) currently available to calls governed by the specified rule.

---

**Note** Displays 0 when available – used bandwidth < 0.

---

- Dedicated—Indicates whether or not the rule applies to a specific dedicated connection only. For more information, see [Dedicated Rules](#) on page 139.

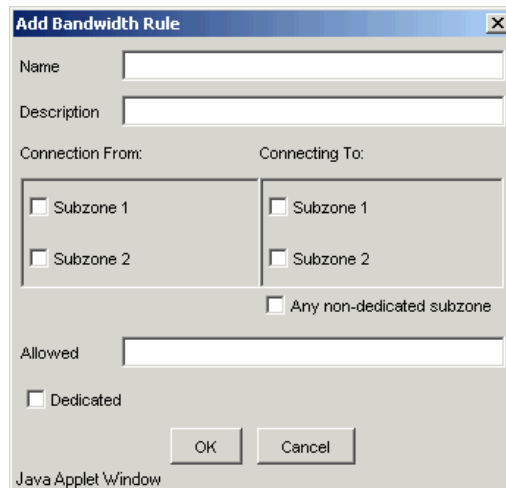
#### ADDING OR MODIFYING INTER-SUBZONE RULES

Click **Add** to display the **Add Bandwidth Rules** dialog box which allows you to create an inter-subzone bandwidth rule. To modify an existing inter-subzone rule, double click the required inter-subzone rule, or select the required inter-subzone rule and click **Edit** to display the **Edit Bandwidth Rules** dialog box.

---

**Note** If you select the **Subzone Default** entry, the **Edit Bandwidth Rule** dialog box displays default settings only. For more information, see [Viewing or Modifying the Default Inter-subzone Rule](#) on page 41.

---



**Figure 2-24** Add Bandwidth Rules Dialog Box (Inter-subzone)

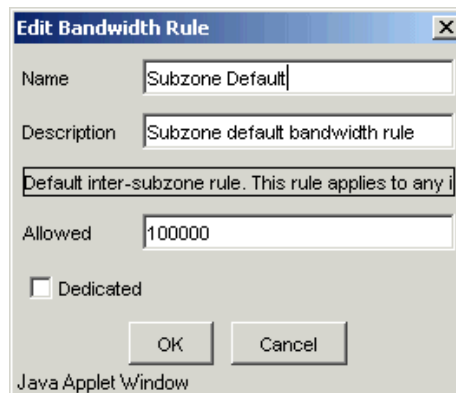
The following options are available in the **Add Bandwidth Rules** dialog box:

- Name—Type the required name of the inter-subzone rule.
- Description—Type the required description of the inter-subzone rule.
- Connecting—Select to apply the specified inter-subzone rule to specific subzones only. Select the required subzones from the lists displayed.
- Any non-dedicated subzones—Check to apply the specified inter-subzone rule to all subzones within the zone.
- Allowed—Type the bandwidth (in Kbps) allowed by the specified inter-subzone rule.
- Dedicated—When checked, the call is not included in the used bandwidth calculation. A dedicated rule applies to a specific dedicated connection only. For more information, see [Dedicated Rules](#) on page 139.

#### VIEWING OR MODIFYING THE DEFAULT INTER-SUBZONE RULE

The default inter-subzone rule applies to any intra-zone call that does not match any of the configured inter-subzone bandwidth rules.

Double click the **Subzone Default** inter-subzone rule, or select the **Subzone Default** inter-subzone rule and click **Edit**. The **Edit Bandwidth Rules** dialog box displays indicating default settings.



**Figure 2-25** *Edit Bandwidth Rules Dialog Box—Default*

The following information is displayed in the default **Edit Bandwidth Rule** dialog box:

- Name—Displays the name of the default inter-subzone rule.
- Description—Displays the description of the default inter-subzone rule.
- Allowed bandwidth—Type the bandwidth (in Kbps) allowed by the default inter-subzone rule.
- Dedicated—A default rule cannot be dedicated. Disabled for the default inter-subzone rule.

#### ADDING OR MODIFYING INTER-ZONE RULES

Click **Add** to display the **Add Bandwidth Rules** dialog box which allows you to create an inter-zone bandwidth rule. To modify an existing inter-zone rule, double click the required inter-zone rule, or select the required inter-zone rule and click **Edit** to display the **Edit Bandwidth Rules** dialog box.

---

**Note** If you select the **Zone Default** entry, the **Edit Bandwidth Rule** dialog box displays default settings only. For more information, see [Viewing or Modifying the Default Inter-subzone Rule](#) on page 41.

---



**Figure 2-26** Inter-zone Bandwidth Rules Dialog Box

The following options are available in the **Inter-zone Bandwidth Rules** dialog box:

**Name**

Type the required name of the inter-zone rule.

**Description**

Type the required description of the inter-zone rule.

**Gatekeeper IP**

Select the required destination gatekeepers to which the rule is applied.

**Add**

Click **Add** to display the **Add Gatekeeper** dialog box for adding additional gatekeepers to the displayed list.

**Allowed**

Type the bandwidth (in Kbps) allowed by the specified inter-zone rule.

**Outgoing**

Type the bandwidth (in Kbps) that you wish you to reserve for outgoing calls only. Reserved bandwidth is deducted from the total allowed bandwidth.

**Dedicated**

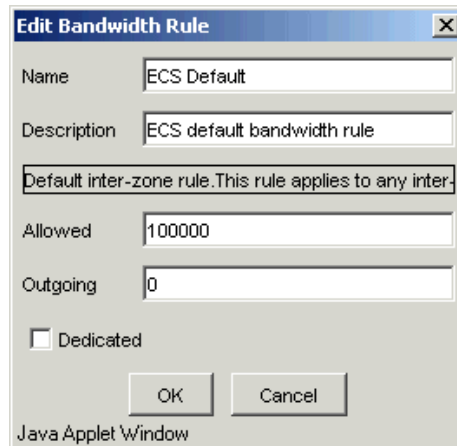
When checked, the call is not included in the used bandwidth calculation.

## Additional ECS Tabs

### VIEWING OR MODIFYING THE DEFAULT INTER-ZONE RULE

The default inter-zone rule applies to any inter-zone call that does not match any of the configured inter-zone bandwidth rules.

Double click the **ECS Default** inter-zone rule, or select the **ECS Default** inter-zone rule and click **Edit**. The **Edit Bandwidth Rules** dialog box displays indicating default settings.



**Figure 2-27** Inter-zone Bandwidth Rules Dialog Box—Default

The following information is displayed in the default **Inter-zone Bandwidth Rules** dialog box:

- Name—Displays the name of the default inter-zone rule.
- Description—Displays the description of the default inter-zone rule.
- Allowed—Type the bandwidth (in Kbps) allowed by the default inter-zone rule.
- Outgoing—Type the bandwidth (in Kbps) that you wish you to reserve for outgoing calls only.
- Dedicated—A default rule cannot be dedicated. Disabled for the default inter-zone rule.

## PARENT TAB

The **Parent** tab enables you to configure a Parent gatekeeper for the ECS, to define a list of parent filters and to choose whether or not to route calls to unresolved zones via the Cisco Proxy.

---

**Note** You can also configure the parent gatekeeper automatically using the Video Management System (VMS) Network Manager **Drag and Drop** feature. In the Network Tree, drag and drop the ECS element into the zone of the gatekeeper you wish to configure as the Parent gatekeeper. The ECS **Parent** tab is automatically updated with the Parent gatekeeper details.

---

## ABOUT PARENT FILTERS

The ECS sends an LRQ to the Parent Gatekeeper when the zone prefix of the call matches one of the defined parent filters. If the ECS fails to match the zone prefix of the call with any of the defined parent filters, the ECS either rejects the call or forwards the call according to the **Call Fallback** settings configured in the ECS element manager. Where no filters are defined, the ECS passes the call to the Parent Gatekeeper. The ECS allows a maximum of ten parent filters. For more information, see the *ECS User Guide*.

**Figure 2-28** Network Tree—Parent Tab

## Additional ECS Tabs

You can configure the following parameters in the **Parent** tab:

- **Enable**—When checked, enables you to add a Parent Gatekeeper to the ECS.
- **IP Address**—Enter the IP address of the Parent Gatekeeper.
- **Port**—Enter the port number of the Parent Gatekeeper.
- **Description**—Type a description of the Parent Gatekeeper.
- **Parent Filters**—Displays the list of defined parent filters.
- **Add**—Click the **Add** button to add a new parent filter to the ECS database.
- **Edit**—Double-click a parent filter from the list or select a parent filter from the list and click the **Edit** button to modify an existing parent filter.
- **Delete**—Select a parent filter from the list and click the **Delete** button to remove the specified parent filter from the list.

---

**Note** The parent tab is enabled when the ECS is configured to support **Dial Plan Version 2.0** and **Use Central Database** is deselected in the [Configure](#) tab of the selected ECS. The **Parent** tab is not available to ECS v1.0 and INVISION ECS.

---

### ADDING A PARENT FILTER

Click the **Add** button to open the **Add Filter** dialog box. Alternatively, double-click the relevant parent filter from the list or select a parent filter from the list and click the **Edit** button to open the **Edit Filter** dialog box.

The following option is available in the **Add Filter** or **Edit Filter** dialog box:

- **Filter**—Enter or modify the prefix that identifies the filter.

Click **OK** to add the new parent filter information to the ECS database.

---

**Note** You can modify and delete existing filters using the **Edit** and **Delete** buttons.

---

## CHILDREN TAB

The **Children** tab enables you to view, configure and modify Child Gatekeepers of the ECS.

---

**Note** You can also configure a child gatekeeper automatically using the Video Management System (VMS) Network Manager **Drag and Drop** feature. In the Network Tree, drag and drop the ECS element you wish to configure as the child gatekeeper into the zone of the current ECS. The **Children** tab of the parent ECS is automatically updated with the Child gatekeeper details.

---

Description	Prefixes	IP address	Port	Proxy	Central DB

**Figure 2-29** Network Tree—Children Tab

The **Children** tab displays the following information:

- Description—Displays the Child Gatekeeper description in free text. This field appears when the **Use Central Database** option is unchecked in the [Configure](#) tab.
- Prefixes—Displays the zone prefix. For information on zone prefixes, see the appropriate section in the *ECS User Guide*.
- IP Address—Displays the IP address of the Child Gatekeeper.
- Port—Displays the port number of the Child Gatekeeper.

## Additional ECS Tabs

- Proxy—Indicates whether or not the ECS routes calls from this zone to the Neighbor gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see the *Cisco Proxy Support* section in the *ECS User Guide*.
- Central Database—Indicates whether or not the Child Gatekeeper was retrieved from the Central Database. For information on the Central Database, see the *Central Database* section in the *ECS User Guide*.

---

**Note** Where available, the **Parent** tab is enabled when the ECS is configured to support **Dial Plan Version 2.0** and **Use Central Database** is deselected in the [Configure](#) tab of the selected ECS. The **Parent** tab is not available in ECS v1.0 or in the INVISION ECS.

---

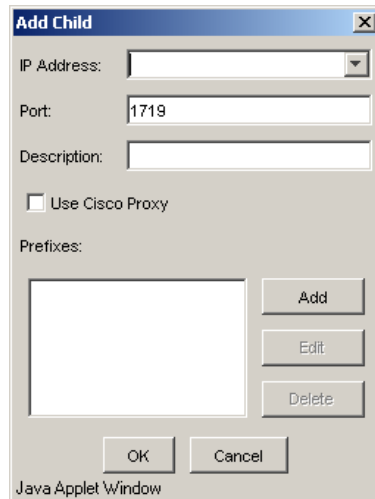
## ADDING A CHILD

Click the **Add** button to open the **Add Child** dialog box. Alternatively, double-click the relevant Child Gatekeeper in the **Children** tab or select a **Child Gatekeeper** and click the **Edit** button to open the **Edit Child** dialog box.

The following options are available in the **Add Child** or **Edit Child** dialog box:

- IP Address—Enter or modify the IP address of the Child Gatekeeper.
- Port—Enter or modify the port number of the Child Gatekeeper.
- Description—Enter or modify the description of the Child Gatekeeper.
- Use Cisco Proxy—Select to indicate whether or not the ECS should route calls from this zone to the Neighbor gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see the *Cisco Proxy Support* section in the *ECS User Guide*.
- Prefixes—Displays the list of defined child prefixes. The ECS sends an LRQ to the Child Gatekeeper when the zone prefix of the call matches one of the defined child prefixes. If the ECS fails to match the zone prefix of the call with any of the defined Child Gatekeeper prefixes, the ECS passes the call to a Neighbor Gatekeeper.

Click the **OK** button to add the Child Gatekeeper to the ECS database.



**Figure 2-30** Add Child Dialog Box

---

**Note** The **Add**, **Edit** and **Delete** options are disabled when you check the **Use Central Database** option in the [Configure](#) tab.

---

### ADDING OR MODIFYING A CHILD PREFIX

Click the **Add** button to open the **Add Prefix** dialog box. Alternatively, double-click the relevant child prefix from the list or select a child prefix from the list and click the **Edit** button to open the **Edit Prefix** dialog box. The dialog box enables you to add a child prefix to the ECS database or modify an existing child prefix.

## Additional ECS Tabs

The following options are available in the **Add Prefix** or **Edit Prefix** dialog box:

- Prefix—Enter or modify the child prefix.

Click the **OK** button to add the new child prefix information to the ECS database.

---

**Note** You can modify and delete existing child gatekeeper prefixes using the **Edit** and **Delete** buttons.

---

## NEIGHBORS TAB

The **Neighbors** tab enables you to view, configure and modify Neighbor Gatekeepers of the ECS for resolving destination IP addresses when the source endpoint is not in the same zone as the destination endpoint. For more information about Neighbor Gatekeepers, see the appropriate *ECS User Guide*.

Description	Prefix	IP Address	Port	Proxy	GK ID	Central DB	LDAP
MCM 172.27.20.1	6	172.27.20.1	1719	disabled		no	no

**Figure 2-31** Network Tree—Neighbors Tab

The **Neighbors** tab displays the following information:

- Description—Displays the Neighbor Gatekeeper description.
- Prefix—Displays the zone prefix.
- ID Address—Displays the Neighbor Gatekeeper IP address.
- Port—Displays the port number of the Neighbor Gatekeeper.

- Proxy—Indicates whether or not the ECS routes all calls from this zone to the Neighbor Gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see the Cisco Proxy Support section in the *ECS User Guide*.
- GK ID—Displays the Neighbor Gatekeeper identifier.
- Central DB—Indicates whether or not the Neighbor Gatekeeper was retrieved from the Central Database.
- LDAP—Indicates whether or not the Neighbor Gatekeeper was retrieved from the LDAP server. For information on the LDAP server, see the *LDAP* section in the *ECS User Guide*.

## ADDING A NEIGHBOR

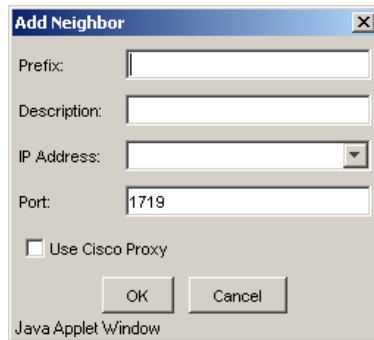
Click the **Add** button to open the **Add Neighbor** dialog box. Alternatively, double-click the relevant neighbor gatekeeper in the **Neighbors** tab or select a neighbor gatekeeper and click the **Edit** button to open the **Edit Neighbor** dialog box.

The following options are available in the **Add Neighbor** or **Edit Neighbor** dialog box:

- Prefix—Enter or modify the Neighbor Gatekeeper zone prefix. For information on zone prefixes, see the *ECS User Guide*.
- Description—Enter or modify the description of the Neighbor Gatekeeper.
- IP Address—Enter or modify the IP address of the Neighbor Gatekeeper.
- Port—Enter or modify the port number of the Neighbor Gatekeeper.
- Use Cisco proxy—Check to instruct the ECS to route all calls from this zone to the Neighbor Gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see the *Cisco Proxy Support* section in the *ECS User Guide*.

Click **OK** to add the Neighbor to the ECS database.

## Additional Endpoints Tab



The 'Add Neighbor' dialog box contains the following fields and controls:

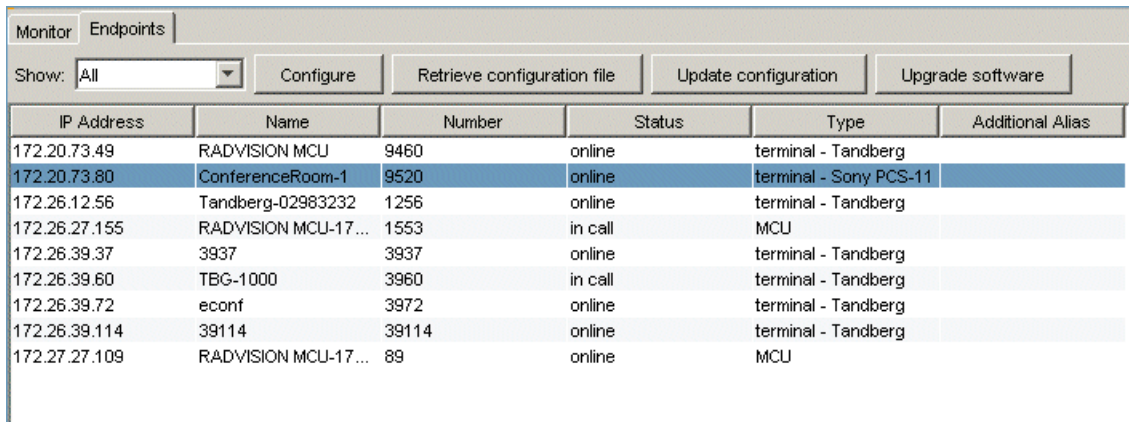
- Prefix: [Text Input]
- Description: [Text Input]
- IP Address: [Dropdown Menu]
- Port: [Text Input, value: 1719]
- Use Cisco Proxy
- OK [Button]
- Cancel [Button]
- Java Applet Window [Text]

**Figure 2-32** Add Neighbor Dialog Box

**Note** The **Add**, **Edit** and **Delete** buttons are disabled when you check the **Use Central Database** option in the **Configure** tab.

## ADDITIONAL ENDPOINTS TAB

The **Endpoints** tab displays endpoint information for the zone and allows you to manage access, addressing, dialing and upgrading for a range of endpoint types



The 'Endpoints' tab interface includes a 'Monitor' button, a 'Show:' dropdown menu set to 'All', and four action buttons: 'Configure', 'Retrieve configuration file', 'Update configuration', and 'Upgrade software'. Below these is a table with the following data:

IP Address	Name	Number	Status	Type	Additional Alias
172.20.73.49	RADVISION MCU	9460	online	terminal - Tandberg	
172.20.73.80	ConferenceRoom-1	9520	online	terminal - Sony PCS-11	
172.26.12.56	Tandberg-02983232	1256	online	terminal - Tandberg	
172.26.27.155	RADVISION MCU-17...	1553	in call	MCU	
172.26.39.37	3937	3937	online	terminal - Tandberg	
172.26.39.60	TBG-1000	3960	in call	terminal - Tandberg	
172.26.39.72	econf	3972	online	terminal - Tandberg	
172.26.39.114	39114	39114	online	terminal - Tandberg	
172.27.27.109	RADVISION MCU-17...	89	online	MCU	

**Figure 2-33** Network Tree—Endpoints Tab

The **Endpoints** tab displays the following buttons:

- [Configure](#)—see [Controlling an Endpoint](#).
- [Retrieve configuration file](#)—see [Retrieving Configuration Parameters](#) on page 57.
- [Update configuration](#)—see [Updating Selected Endpoints](#) on page 58.
- [Upgrade software](#)—see [Upgrading Software](#) on page 59.

---

**Note** The **Retrieve configuration file**, **Update configuration** and **Upgrade software** buttons are available for Sony PCS-1, PCS-11, PCS-G70 and PCS-TL50 endpoints. For PCS-1600 only the **Update configuration** button is available.

---

The **Endpoints** tab displays for each endpoint the following information:

- IP address
- Name
- Number
- Status (online, offline, in call)
- Endpoint type (terminal, MCU, Gateway)
- Additional alias

## CONTROLLING AN ENDPOINT

You manage an endpoint by selecting the endpoint and clicking **Configure** to open the **Endpoint Control** dialog box. Alternatively, double-click the relevant endpoint row in the list. The dialog box enables you to modify endpoint configuration and access parameters and to dial to other endpoints on the network.

If the endpoint type is not configured, the [Access](#) tab displays. You select from a range of endpoint types recognized by the Video Management System (VMS) Network Manager and provide security details as required in order to manage the endpoint.

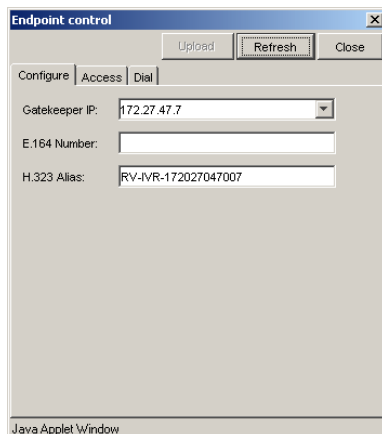
The **Endpoint Control** dialog box includes the following tabs:

- [Configure](#)
- [Access](#)
- [Dial](#)

## Additional Endpoints Tab

### CONFIGURE

The **Configure** tab of the **Endpoint Control** dialog box allows you to modify the endpoint gatekeeper addressing, E.164 number and alias.



**Figure 2-34** *Endpoint Control: Configure*

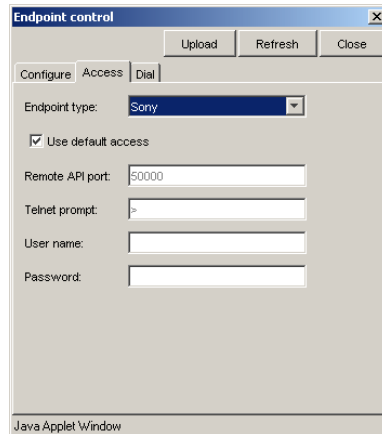
Configure the **Configure** tab as follows:

- Gatekeeper IP—Select a gatekeeper IP address from the drop-down list of gatekeepers available on the network.
- Type an E.164 number for the endpoint.
- Type an H.323 alias for the endpoint.

Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.

## ACCESS

The **Access** tab of the **Endpoint Control** dialog box allows you to view and configure the access settings that enable the Video Management System (VMS) Network Manager to manage the endpoint.



**Figure 2-35** *Endpoint Control: Access*

Configure the **Access** tab as follows:

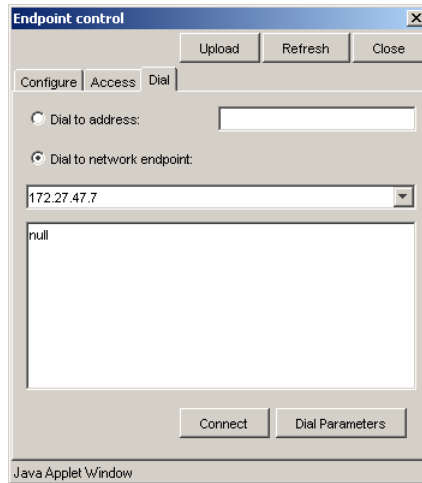
- **Endpoint Type**—Select an endpoint from the list of supported endpoints.
- **Use default access**—Check to use default access settings defined by the endpoint. When unchecked, you can modify the **Remote API port** and **Telnet prompt** for Tandberg endpoints only.
- **Remote API port**—The endpoint API port. Editable for Tandberg endpoints only.
- **Telnet prompt**—The Telnet prompt character string. Editable for Tandberg endpoints only.
- **User name**—The user name required for communicating with the endpoint.
- **Password**—The password required for communicating with the endpoint.

Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.

## Additional Endpoints Tab

### DIAL

The **Dial** tab of the **Endpoint Control** dialog box allows you to specify an address or endpoint to which the current endpoint dials.



**Figure 2-36** *Endpoint Control: Dial*

Configure the **Dial** tab as follows:

- **Dial to address**—When selected, the endpoint makes a call to the specified address.
- **Dial to network endpoint**—Select from a list of endpoints on the network to which the endpoint dials a call.
- **Log**—Displays a log events for the current call.
- **Connect**—Connects the endpoint in a call at the specified address or with the selected endpoint.
- **Dial Parameters**—Displays the **Dial Parameters** dialog box in which you specify the call type and whether the call is restricted to other incoming callers.

Click **Upload** to add the new settings to the endpoint or **Refresh** to update the new settings.

## RETRIEVING CONFIGURATION PARAMETERS

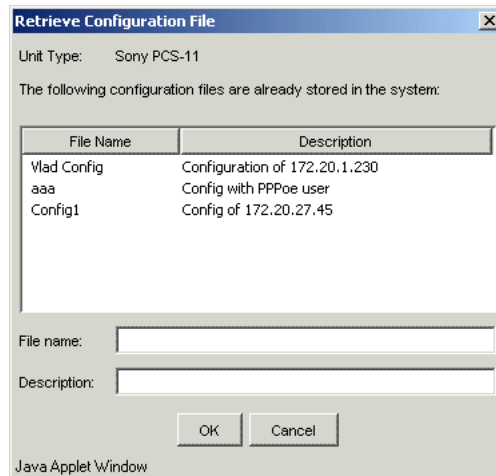
The **Retrieve configuration file** button enables you to retrieve the configuration parameters from an endpoint and saves configuration information to a file accessed from the **Configuration Files** tab in the **Endpoint Management** tab of the **Settings** section. For more information, see [Configuration Files](#) on page 111.

To access a configuration file, click the **Retrieve Configuration file** button. The **Retrieve Configuration File** dialog box displays.

---

**Note** You can select multiple endpoints from the list by holding down the **Ctrl** key on your keyboard and left clicking the mouse.

---



**Figure 2-37** Retrieve Configuration File Dialog Box

## Additional Endpoints Tab

The **Retrieve Configuration File** dialog box displays a list of the configuration files that were previously retrieved. Type the following information in the **Retrieve Configuration File** dialog box:

- File Name—Type the name that you would like to give to the configuration file.
- Description—Type a description of the file.

Click **OK** to save the file in the Video Management System (VMS) Network Manager database.

Click **Cancel** to cancel the operation.

## UPDATING SELECTED ENDPOINTS

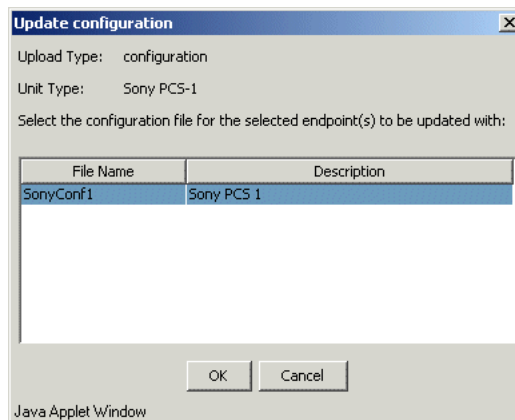
The **Update configuration** button enables you to update selected endpoints with a configuration file that has been previously retrieved and saved in the Network Manager database in the **Configuration Files** tab in the **Endpoint Management** tab of the **Settings** section. For more information, see [Configuration Files](#) on page 111.

To update an endpoint, click the **Update configuration** button. The **Update configuration** dialog box displays.

---

**Note** Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included.

---



**Figure 2-38** Update Configuration Dialog Box

The **Update configuration** dialog box displays a list of the configuration files stored in the Video Management System (VMS) Network Manager database that are associated with the selected endpoint types.

- Select the file with which you want to update the selected endpoints.

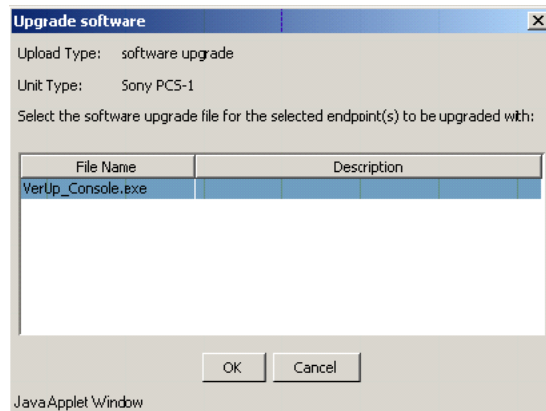
Click **OK**. Update of the endpoints begins.

Click **Cancel** to cancel the operation.

## UPGRADING SOFTWARE

The **Upgrade software** button enables you to upgrade the software version of selected endpoints with a software file that has been previously saved in the Network Manager database in the **Software Upgrade Files** tab in the **Endpoint Management** tab of the **Settings** section. For more information, see [Software Upgrade Files](#) on page 109.

To update an endpoint, click the **Upgrade software** button. The **Upgrade software** dialog box displays.



**Figure 2-39** Upgrade Software Dialog Box

## Additional Endpoints Tab

The **Upgrade Software** dialog box displays a list of the software upgrade files stored in the Video Management System (VMS) Network Manager database that are associated with the selected endpoint types.

- Select the file with which you want to update the selected endpoints.

---

**Note** You can select multiple endpoints from the list by holding down the **Ctrl** key on your keyboard and left clicking the mouse.

---

Click **OK** and the upgrade of the endpoints begins. The **Upload Log** dialog box displays the status of the upgrade. For more information on the **Upload Log** tab, see [Upload Log](#) on page 113.

## UPGRADING SONY ENDPOINTS

This section applies to the following Sony endpoints only:

- PCS1
- PCS-11
- PCS-G70
- PCS-TL50



### To upgrade SONY endpoints perform the following activities

1. Request from your Sony distributor the software upgrade file that can be used with the Video Management System (VMS) Network Manager.
2. Save the file that you received from the distributor in the Video Management System (VMS) Network Manager database. For more information, see [Adding a Software Upgrade File](#) on page 109.
3. Upgrade the endpoints software with the file that was received from the distributor. For more information, see [Software Upgrade Files](#) on page 109.

---

**Note** Only generic parameters are retrieved. Endpoint-specific parameters, such as the endpoint IP address, are not included.

---

## ADDITIONAL MCU TABS

When an MCU is selected in the tree, additional tabs are displayed allowing you to view services and manage MP units, including the following:

- Protocols (version 3.x)
- Registered MPs (version 3.x or later)
- Multipoint Processors (version 2.x)
- Video Processors (version 2.x)
- Services

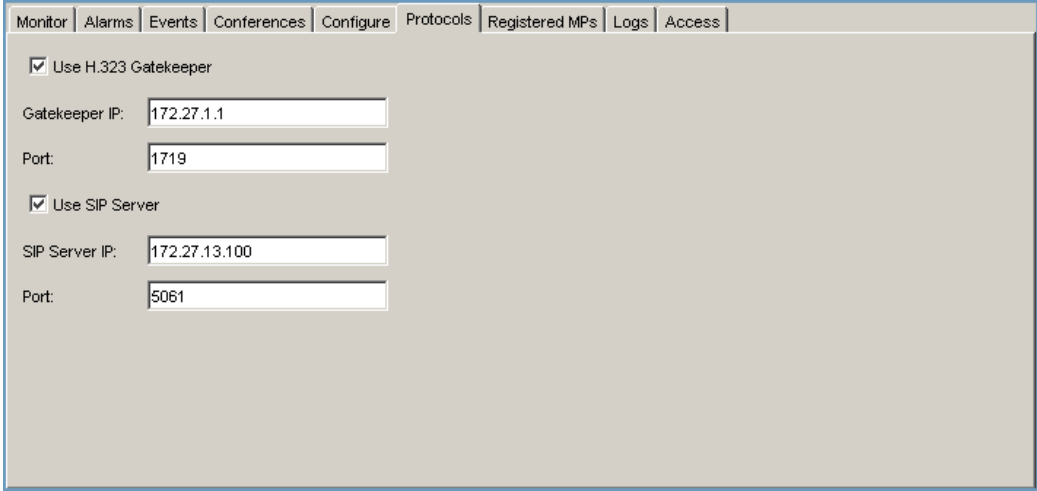
---

**Note** The tabs displayed vary according to the MCU version.

---

## PROTOCOLS (VERSION 3.X)

The **Protocols** tab allows you to configure how the MCU works with H.323 and SIP call routing devices.



The screenshot shows the 'Protocols' configuration tab in a web interface. The tab is selected among others: Monitor, Alarms, Events, Conferences, Configure, Protocols, Registered MPs, Logs, and Access. The configuration area contains two sections, each with a checked checkbox and two input fields. The first section is for H.323 Gatekeeper, with fields for IP (172.27.1.1) and Port (1719). The second section is for SIP Server, with fields for IP (172.27.13.100) and Port (5061).

**Figure 2-40** Network Tree—MCU: Protocols

The **Protocols** tab displays the following information:

- Use H.323 Gatekeeper
- Gatekeeper IP
- Port
- Use SIP Server
- SIP Server IP
- Port

**REGISTERED MPs  
(VERSION 3.X OR  
LATER)**

The **Registered MPs** tab allows you to view the list of MPs currently registered with the MCU.

Monitor   Alarms   Events   Conferences   Configure   Protocols   Registered MPs   Logs   Access		
Type	Address	Description
mvp	172.27.14.4	ver 1.1.0a:EMP
mvp	172.27.14.2	ver 1.1.0a:EMP
mp	172.27.14.1	ver 3.0.60P:MP
mp	172.27.14.3	ver 3.0.60P:MP

**Figure 2-41** Network Tree—MCU: Registered MPs

The **Registered MPs** tab displays the following information:

- Type—Displays the type of MP unit registered with the current MCU. MP unit types supported include:
  - MP—The local MP component of the current MCU or an MCU operating in *MP Only* mode. Performs basic media processing such as audio transcoding, video processing and video switching.
  - MVP—Unit performing advanced media processing such as video processing and video switching.

- VPS—Unit performing media processing such as video bandwidth and picture size transcoding.
- DCS—Providing T.120 data collaboration services.
- Address—Address of the MP unit. This may be the same as the current MCU if the MP is the media processing component of the current unit.
- Description—Version number and type.

## MULTIPOINT PROCESSORS (VERSION 2.X)

The **MP List** tab enables you to define the MPs being controlled by a version 2.x MCU in a clustered layout (local MPs or MCUs configured as MP only). Up to six MPs can be controlled by a single MCU in this type of layout.

Description	IP Address	Status
The Local MP	172.27.36.10	enabled
172.27.36.242	172.27.36.242	enabled

**Figure 2-42** Network Tree—MCU: MP List Tab

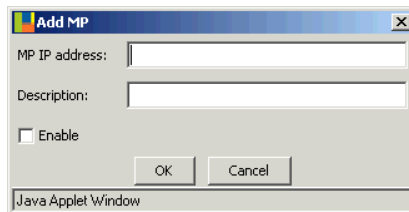
The **MP List** tab displays the following information about each MP:

- Description of the MP
- IP address
- Current status (enabled or disabled)

## Additional MCU Tabs

### ADDING AN MP

Click **Add** to display the **Add MP** dialog box, which enables you to define the IP address and optional description of MPs being controlled by the selected MCU. Select **Enable** to activate the MP. Click **OK**. The new MP is added to the displayed list.

A dialog box titled "Add MP" with a close button (X) in the top right corner. It contains two text input fields: "MP IP address:" and "Description:". Below these fields is a checkbox labeled "Enable". At the bottom of the dialog are two buttons: "OK" and "Cancel". The text "Java Applet Window" is visible at the very bottom of the dialog box.

**Figure 2-43** Add MP Dialog Box

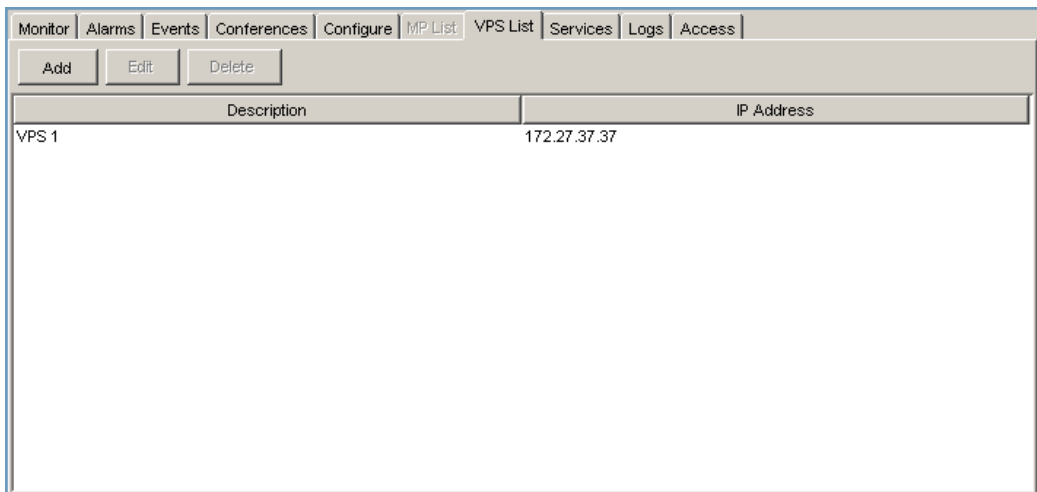
---

**Note** You can modify and delete existing MPs using the **Edit** and **Delete** buttons.

---

### VIDEO PROCESSORS (VERSION 2.X)

The **VPS List** tab displays information about any VPS elements used by the selected version 2.x MCUs.

A screenshot of a web interface showing the "VPS List" tab. The interface has a menu bar at the top with tabs: Monitor, Alarms, Events, Conferences, Configure, MP List, VPS List, Services, Logs, and Access. Below the menu bar are three buttons: Add, Edit, and Delete. The main area is a table with two columns: "Description" and "IP Address". There is one row in the table with the text "VPS 1" in the "Description" column and "172.27.37.37" in the "IP Address" column.

Description	IP Address
VPS 1	172.27.37.37

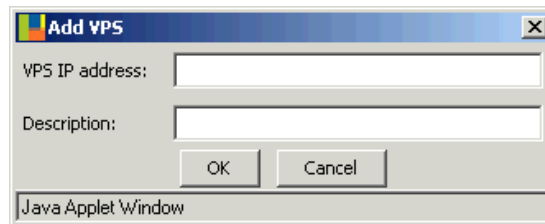
**Figure 2-44** Network Tree—VPS List (MCU)

The **VPS List** tab displays the following information:

- Description of the VPS
- IP address

#### ADDING A VPS ELEMENT

Click **Add** to define additional VPS elements. The **Add VPS** dialog box is displayed, enabling you to type the IP address and description of the new VPS element. Click **OK** to add the new VPS element to the table.



**Figure 2-45** Add VPS Dialog Box

---

**Note** You can modify and delete existing VPS elements using the **Edit** and **Delete** buttons.

---

## SERVICES

The **Services** tab displays the list of services supported by the selected MCU. You can edit services by clicking on the link to the MCU element manager.

Monitor	Alarms	Events	Conferences	Configure	Protocols	Registered MPs	Services	Logs	Access
<a href="#">Please edit this table using the element manager.</a>									
Prefix	Description	Participants	Media	Layout	Bit Rate	Data	Video For...	Picture For...	Frame Rate
766811*	4 Split CP 384	5+	video		320 kbps	disabled	H.261	CIF	15
766812*	4 Split CP 128	3+	video		110 kbps	disabled	H.261	CIF	15
60	Voice	3+	voice		none	enabled	H.261	CIF	30
611	VA 128	3+	video		128 kbps	disabled	H.263	QCIF	30
613	VA 384	3+	video		320 kbps	enabled	H.261	CIF	30
617	VA 768	3+	video		704 kbps	enabled	H.261	CIF	30
6414	CP 128 4 Split	3+	video		128 kbps	disabled	H.261	CIF	15
6434	CP 384 4 Split	3+	video		320 kbps	disabled	H.261	CIF	15
6417	CP 128 7 Split	3+	video		128 kbps	disabled	H.261	CIF	15
64116	CP 128 16 ...	3+	video		128 kbps	disabled	H.261	CIF	15
6437	CP 384 7 Split	3+	video		320 kbps	disabled	H.261	CIF	15
64316	CP 384 16 ...	3+	video		320 kbps	disabled	H.261	CIF	15
6614	CP 128 Sym...	3+	video		110 kbps	disabled	H.261	CIF	15
6617	CP 128 Sy...	3+	video		110 kbps	disabled	H.261	CIF	15
66116	CP 128 Sy...	3+	video		110 kbps	disabled	H.261	CIF	15
6634	CP 384 Sy...	3+	video		320 kbps	disabled	H.261	CIF	15
6637	CP 384 Sy...	3+	video		320 kbps	enabled	H.261	CIF	15

**Figure 2-46** Network Tree—Services Tab (MCU)

The **Services** tab displays the following information:

- Prefix used to access the service
- Service description
- Number of parties allowed in the conference
- Media (such as video)
- Layout setting
- Bit rate (maximum bit rate)
- T.120 setting (enabled or disabled)
- Video format
- Picture format
- Frame rate

**Note** To edit the information in the table, click the link above the table to access the element manager.

## ADDITIONAL GATEWAY TAB

When a Gateway is selected in the tree, an additional tab is displayed, enabling you to view and add services.

### SERVICES

The **Services** tab displays the list of services supported by the selected Gateway.

Monitor	Alarms	Events	Configure	Services	Logs	Access
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Add</span> <span>Edit</span> <span>Delete</span> </div>						
Prefix	Description	Call Type	Bit Rate			
9384	384	H.320	384			
9128	128	H.320	128			
9768	768	H.320	768			
9256	256	H.320	256			
9512	512	H.320	512			
91472	1472	H.320	1472			
91920	1920	H.320	1920			
92000	auto	H.320	auto			
91922	192	H.320	192			
964	64K	H.320	64			

**Figure 2-47** Network Tree—Services Tab (GW)

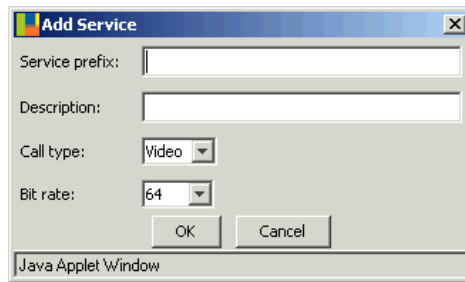
The **Services** tab displays the following information:

- Prefix used to access the service
- Service description
- Call type (**Voice** or **Video**)
- Bit rate

## Additional Cisco MCM Tabs

### ADDING A SERVICE

Click **Add** to display the **Add Service** dialog box, which enables you to configure new services. Type the prefix of the service and the service description, then select the call type (**Video** or **Voice**) and the bit rate. Click **OK**. The new service is added to the displayed list.



**Figure 2-48** Add Service Dialog Box (GW)

---

**Note** You can modify and delete existing services using the **Edit** and **Delete** buttons.

---

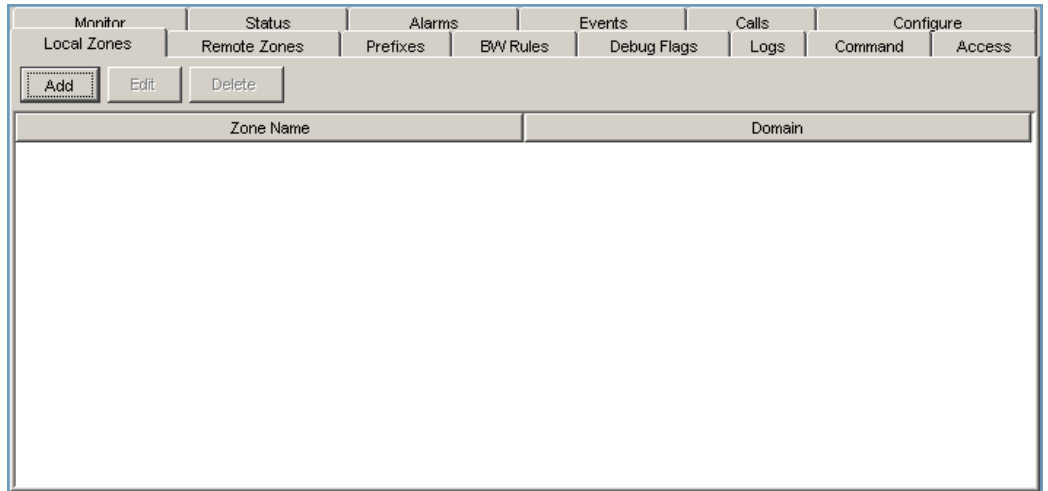
## ADDITIONAL CISCO MCM TABS

When a Cisco MCM is selected in the tree, additional tabs are displayed, enabling you to view and configure MCM-specific tabs, including the following:

- Local Zones
- Remote Zones
- Prefixes
- BW Rules
- Debug Flags
- Command

## LOCAL ZONES

The **Local Zones** tab enables you to view and configure local MCM sub-zones used for bandwidth control purposes.



**Figure 2-49** Network Tree—MCM: Local Zones

The **Local Zones** tab displays the following information:

- Zone Name
- Domain

### ADDING A LOCAL ZONE

Click **Add** to display the **Add Local Zone** dialog box which enables you to define local zones for the MCM. Type a zone name and the zone domain. Click **OK** and the zone is added to the **Local Zones** list.

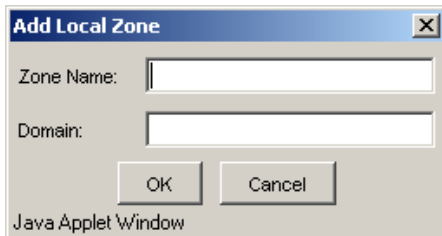


Figure 2-50 Add Local Zone Dialog Box

---

**Note** You can modify and delete existing local zones using the **Edit** and **Delete** buttons.

---

## REMOTE ZONES

The **Remote Zones** tab enables you to view, configure and modify remote Cisco MCMs for resolving destination IP addresses when the source endpoint is not in the same zone as the destination endpoint.

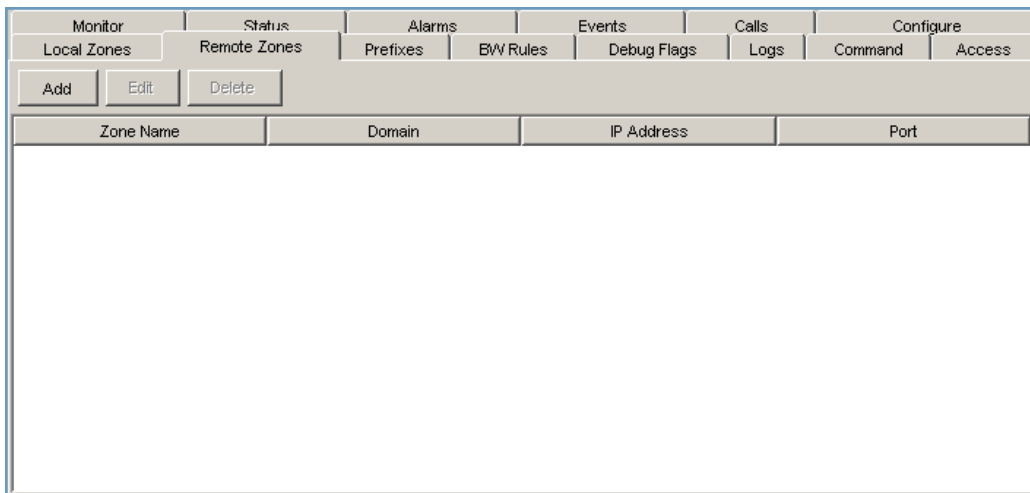


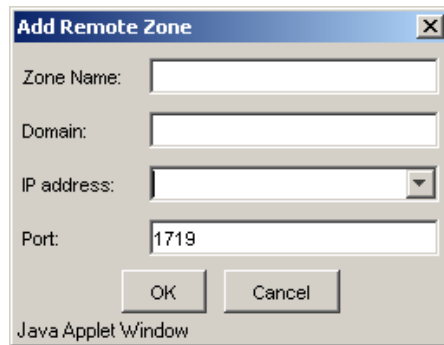
Figure 2-51 Network Tree—MCM: Remote Zones

The **Remote Zones** tab displays the following information:

- Zone Name
- Domain
- IP Address
- Port

#### ADDING A REMOTE ZONE

Click **Add** to display the **Add Remote Zone** dialog box which enables you to define remote zones for the MCM. Type a zone name, zone domain, IP address and port. Click **OK** and the zone is added to the **Remote Zones** list.



**Figure 2-52** Add Remote Zone Dialog Box

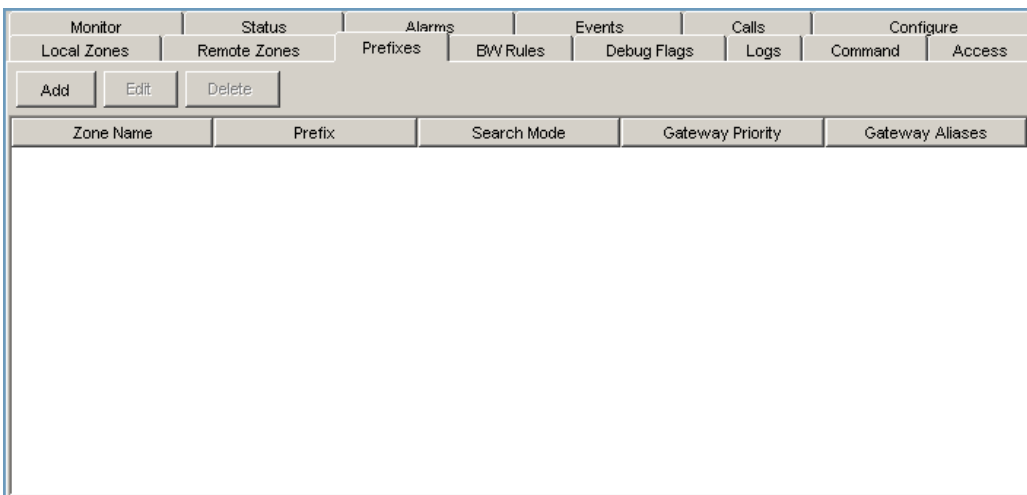
---

**Note** You can modify and delete existing remote zones using the **Edit** and **Delete** buttons.

---

## PREFIXES

The **Prefixes** tab enables you to assign prefixes to local and remote MCM zones, configure the method for sending LRQ messages to each destination for address resolution and assign gateway priorities.



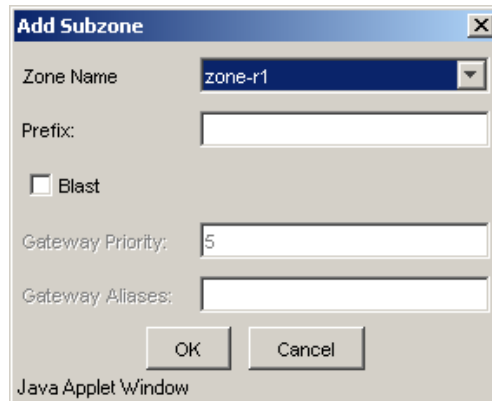
**Figure 2-53** Network Tree—MCM: Prefixes

The **Prefixes** tab displays the following information:

- Zone Name
- Prefix
- Search Mode—Blast or sequential
- Gateway Priority
- Gateway Aliases

## ADDING A PREFIX

Click **Add** to display the **Add Prefix** dialog box which enables you to configure prefixes with which the MCM performs address resolution, specify prefix values, send LRQ messages simultaneously and configure gateway priorities per zone. Select a zone, enter a prefix number and select **Blast** for sending LRQ messages simultaneously. Click **OK** to add the zone to the **Prefixes** list.



**Figure 2-54** Add Prefixes Dialog Box

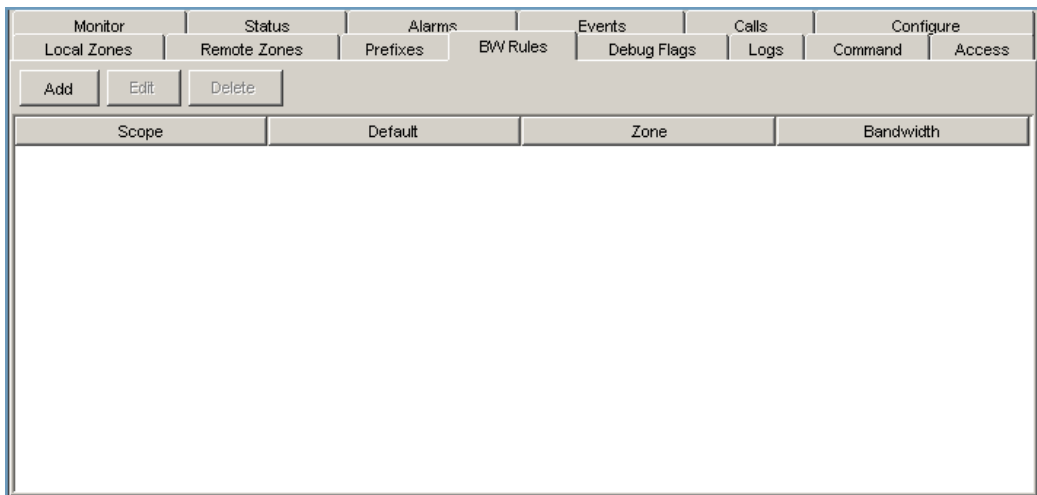
---

**Note** You can modify and delete existing prefixes using the **Edit** and **Delete** buttons.

---

## BW RULES

The **BW Rules** tab enables you control the bandwidth of H.323 traffic both in the MCM zone and between the MCM and other zones. You can also specify bandwidth rules per session or specific zones. A default setting specifies a bandwidth rule for all zones with which the MCM operates.



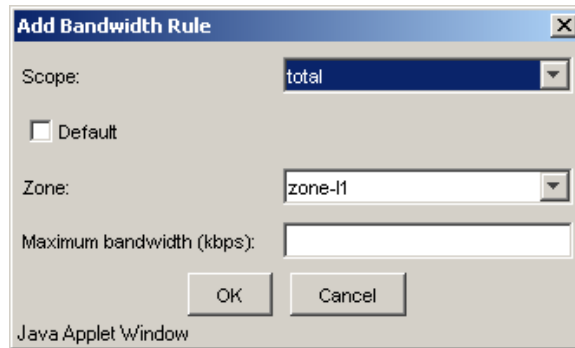
**Figure 2-55** Network Tree—MCM: BW Rules

The **BW Rules** tab displays the following information:

- Scope:
  - Total—Indicates the total amount of bandwidth for H.323 traffic allowed in this zone.
  - Remote—Indicates the total amount of bandwidth for H.323 traffic from this zone to all other zones.
  - Interzone—Indicates the total amount of bandwidth for H.323 traffic from this zone to another zone.
  - Session—Indicates the maximum bandwidth allowed for a session in the zone.
- Default—Indicates the default value for all zones is configured in this rule.
- Zone
- Bandwidth

## ADDING A BANDWIDTH RULE

Click **Add** to display the **Add Bandwidth Rules** dialog box which enables you to specify bandwidth limitations on H.323 traffic between both within the zone and between other zones either per session or per zone. Select the scope of the bandwidth rule, indicate whether the rule is the default for all zones, select a zone and maximum bandwidth rate. Click **OK** and the bandwidth rule is added to the **BW Rules** list.



**Figure 2-56** Add Bandwidth Rules Dialog Box

---

**Note** You can modify and delete existing bandwidth rules using the **Edit** and **Delete** buttons.

---

## DEBUG FLAGS

The **Debug Flags** tab enables you to view and configure MCM debugging commands.

Monitor		Status		Alarms		Events		Calls		Configure	
Local Zones		Remote Zones		Prefixes		B/W Rules		Debug Flags		Logs	
Command		Access									
Add		Edit		Delete							
Debug Command				Description				Status			
debug all				Enable all debugging				disabled			

**Figure 2-57** Network Tree—MCM: Debug Flags

The **Debug flags** tab displays the following information:

- Debug Command
- Description
- Status

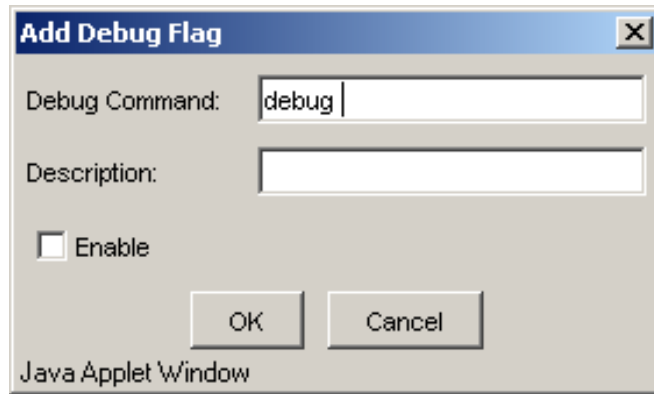
### ADDING A DEBUG FLAG

Click **Add** to display the **Add Debug Flag** dialog box which enables you to specify MCM debug flags. Type the debug flag name, a description and select to enable the flag. Click **OK** and the debug flag is added to the **Debug Flags** list and if selected, the debug flag is enabled.

---

**Warning** Set debug flags with caution as too many may inhibit the performance of the MCM on the network.

---



**Figure 2-58** Add Debug Flag Dialog Box

---

**Note** You can modify and delete existing debug commands using the **Edit** and **Delete** buttons.

---

## COMMAND

The **Command** tab enables you to use the Video Management System (VMS) Network Manager web interface to view MCM gatekeeper monitoring information and perform configuration. A default set of commands are available and you may also enter additional commands in the **Command** text box. The tab window displays the results.

## Additional Cisco MCM Tabs

The screenshot shows the Cisco MCM interface with the following tabs: Monitor, Status, Alarms, Events, Calls, Configure, Local Zones, Remote Zones, Prefixes, B/W Rules, Debug Flags, Logs, Command, and Access. The 'Command' tab is active, and the command 'show gatekeeper endpoints' is entered in the text box. The 'Show' button is highlighted. The output of the command is displayed in the main window:

```
show gatekeeper endpoints
                        GATEKEEPER ENDPOINT REGISTRATION
                        =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name      Type  F
-----
172.27.20.1     11720 172.27.20.1    24999  MCML           H323-GW  --
   H323-ID: proxy16
172.27.36.80    1820  172.27.36.80   1719  MCML           H320-GW
   H323-ID: Amit
172.27.36.80    1620  172.27.36.80   1619  MCML           TERM
   E164-ID: 8034
Total number of active registrations = 3

2600-1#
```

**Figure 2-59** Network Tree—MCM: Command

### USING MCM COMMANDS

You can retrieve information automatically from the MCM using a set of predefined commands from the drop-down list or manually by entering MCM commands in the text box and clicking **Show**. The results are displayed in the tab window.

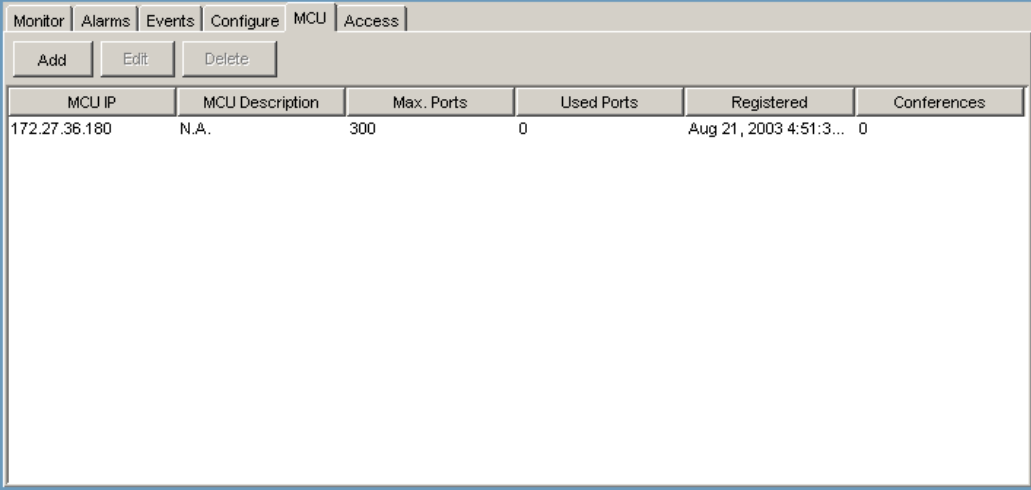
You can perform MCM gatekeeper configuration by entering the command in the text box and clicking **Configure**. Clicking the **Configure** button performs all the Telnet commands necessary to access the appropriate MCM gatekeeper configuration level for performing the command you specified in the text box.

## ADDITIONAL DCS TAB

When a DCS is selected in the tree, an additional tab is displayed, enabling you to view information about MCUs supported by the DCS for T.120 data collaboration and to add MCUs to the list.

### VIEWING MCUS

The **MCU** tab displays the list of MCUs which use the DCS for conducting T.120 data collaboration sessions and allows you to configure the maximum number of ports which the MCU can use.



MCU IP	MCU Description	Max. Ports	Used Ports	Registered	Conferences
172.27.36.180	N.A.	300	0	Aug 21, 2003 4:51:3...	0

**Figure 2-60** Network Tree—DCS: MCU tab

The **MCU** tab displays the following information:

- MCU Address—IP address of MCU.
- MCU Description—Description of the MCU, free text.
- Max. Ports—Displays the number of ports available on the DCS for use by the MCU.
- Used Ports—Displays the number of ports currently in use by the DCS for communication with the MCU highlighted in the list.
- Registration Time—Time registration between the DCS and MCU occurred.
- Conferences—Displays the number of MCU conferences on which DCS ports are currently occupied for T.120 data sessions.

## Additional DCS Tab

### ADDING AN MCU

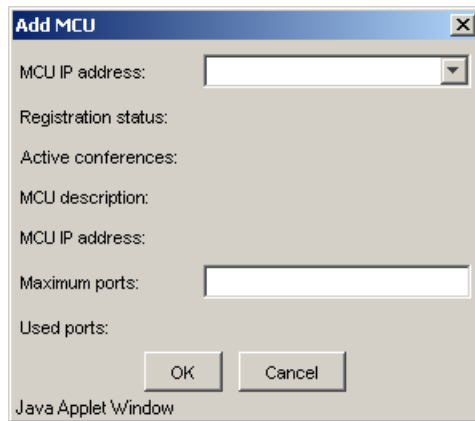
Click **Add** to display the **Add MCU** dialog box. Enter the MCU IP address and the maximum number of DCS ports available for use by the MCU.

---

**Note** It is recommended that you enter a value in this field for unconfigured version 2.xx MCUs.

---

Click **Upload** to update the DCS with the MCU settings.



**Figure 2-61** Network Tree—DCS: Add MCU Dialog Box

---

**Note** You can modify and delete existing MCUs using the **Edit** and **Delete** buttons.

---

# 3

## NETWORK TABLE VIEW

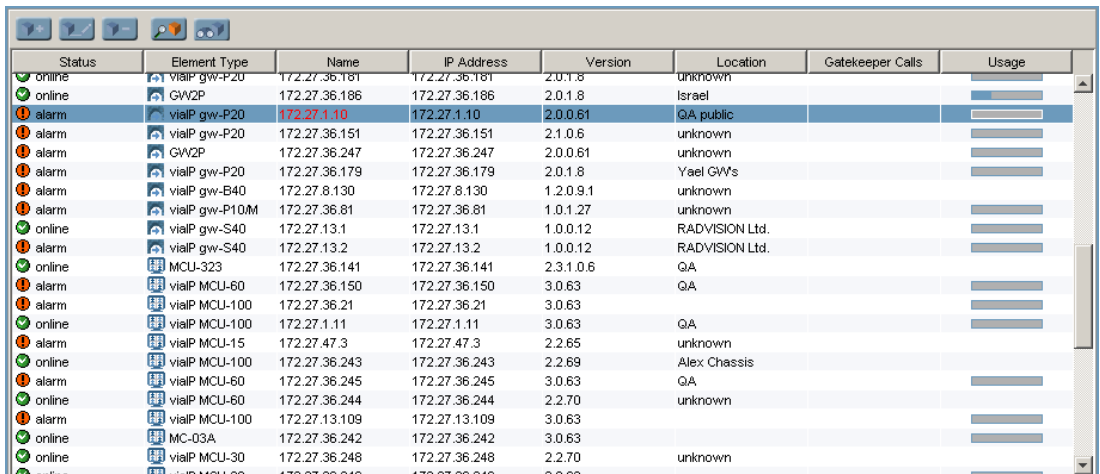
### WHAT'S IN THIS CHAPTER

This chapter provides a description of the Network Table view and includes the following:

- [About the Network Table View](#)

### ABOUT THE NETWORK TABLE VIEW

The **Network Table** view displays information about all the elements in the IP conferencing network in a single table and provides element editing, search and auto-detect capabilities.



Status	Element Type	Name	IP Address	Version	Location	Gatekeeper Calls	Usage
online	vialP gw-P20	172.27.36.181	172.27.36.181	2.0.1.8	unknown		
online	GW2P	172.27.36.186	172.27.36.186	2.0.1.8	Israel		
alarm	vialP gw-P20	172.27.1.10	172.27.1.10	2.0.0.61	QA public		
alarm	vialP gw-P20	172.27.36.151	172.27.36.151	2.1.0.6	unknown		
alarm	GW2P	172.27.36.247	172.27.36.247	2.0.0.61	unknown		
alarm	vialP gw-P20	172.27.36.179	172.27.36.179	2.0.1.8	Yael GW's		
alarm	vialP gw-B40	172.27.8.130	172.27.8.130	1.2.0.9.1	unknown		
alarm	vialP gw-P10M	172.27.36.81	172.27.36.81	1.0.1.27	unknown		
online	vialP gw-S40	172.27.13.1	172.27.13.1	1.0.0.12	RADVISION Ltd.		
alarm	vialP gw-S40	172.27.13.2	172.27.13.2	1.0.0.12	RADVISION Ltd.		
online	MCU-323	172.27.36.141	172.27.36.141	2.3.1.0.6	QA		
alarm	vialP MCU-60	172.27.36.150	172.27.36.150	3.0.63	QA		
alarm	vialP MCU-100	172.27.36.21	172.27.36.21	3.0.63			
online	vialP MCU-100	172.27.1.11	172.27.1.11	3.0.63	QA		
alarm	vialP MCU-15	172.27.47.3	172.27.47.3	2.2.65	unknown		
online	vialP MCU-100	172.27.36.243	172.27.36.243	2.2.69	Alex Chassis		
alarm	vialP MCU-60	172.27.36.245	172.27.36.245	3.0.63	QA		
online	vialP MCU-60	172.27.36.244	172.27.36.244	2.2.70	unknown		
alarm	vialP MCU-100	172.27.13.109	172.27.13.109	3.0.63			
online	MC-03A	172.27.36.242	172.27.36.242	3.0.63			
online	vialP MCU-30	172.27.36.248	172.27.36.248	2.2.70	unknown		

Figure 3-1 Network Table

## About the Network Table View

The **Network Table** view includes the following information about each element:

- Element status
- Element type
- Element name
- IP address
- Version number
- Location
- Gatekeeper calls
- Resource usage versus capacity

The information in the Network Tree can be sorted by clicking the column headers.

---

**Note** Click any of the links displayed in the **Name** column to display the relevant element manager for that element.

---

## ELEMENT CONTROL

The Network Map view contains five buttons which allow you to perform the following:

- Add element
- Edit element
- Delete element
- Find element
- Auto-detect elements

For more information about these actions, see the [Finding and Managing Elements](#) chapter.

---

**Note** These buttons are also available in [Network Tree View](#) and the [Network Map View](#).

---

# 4

## NETWORK MAP VIEW

---

### WHAT'S IN THIS CHAPTER

This chapter provides a description of the Network Map View and includes the following:

- [About the Network Map View](#)

### ABOUT THE NETWORK MAP VIEW

The **Network Map** view displays information about the IP conferencing network in the form of graphic maps created for each node in the Network hierarchy. For more information, see the [About the Network Tree View](#) section.

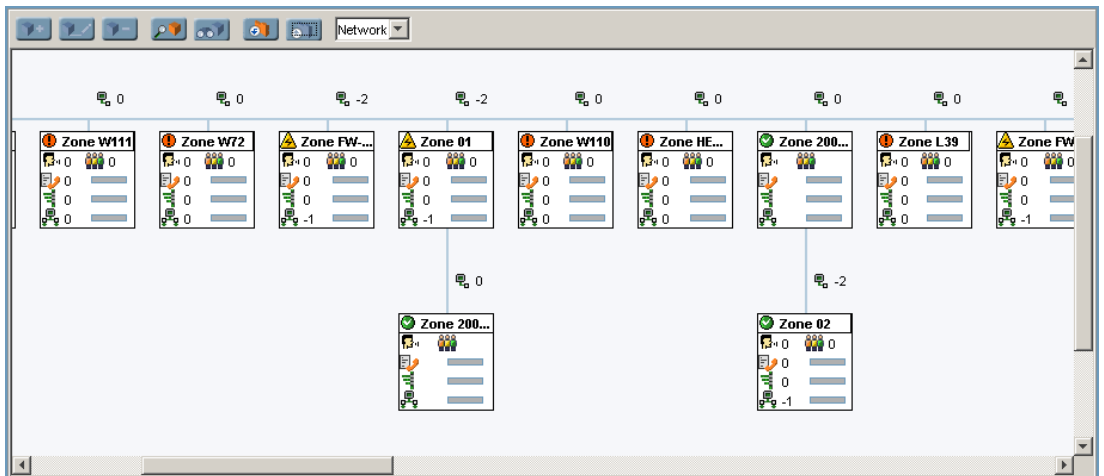


Figure 4-1 Network Map View

## About the Network Map View

The top level of the **Network Map** view displays the network root and the zones into which the network is divided. Each square represents either the network root, a zone (or user-defined folder) or a single element. Each square includes the following information:

- Current status
- Number of calls
- Number of conferences
- Number of registered participants versus capacity
- Number of B-channels handled by gateways versus capacity
- Total bandwidth handled by gatekeepers versus capacity

In addition, inter-zone bandwidth information is displayed above the zones when relevant.

---

**Note** Call and conference statistics for OnLan Gateways and OnLan MCUs are not included in summary details for selected elements.

---

## ELEMENT CONTROL

The Network Map view contains five buttons which allow you to perform the following:

- Add element
- Edit element
- Delete element
- Find element
- Auto-detect elements

For more information about these actions, see the [Finding and Managing Elements](#) chapter.

---

**Note** These buttons are also available in [Network Tree View](#) and the [Network Table View](#).

---

## NAVIGATING THE NETWORK MAP

The Network Map view enables you to drill down from the zone level (or folder) to the element level by double-clicking a square. Use the **Up** and **Down** icons to navigate between map levels. Use the drop-down list to select which view to display. You can add, edit and delete elements from the Network Map View using the buttons displayed above the map.

# 5

## ALARMS VIEW

---

### WHAT'S IN THIS CHAPTER

This chapter provides a description of the Alarms view of the Video Management System (VMS) Network Manager and includes the following:

- Alarms Tab
- Events Tab

### ALARMS TAB



The **Alarms** tab enables you to view and sort the alarms generated by the elements in the network according to alarm status, alarm message, date and time or element.

Severity	Date & Time	Message	Element
⚠ warning	Apr 17, 2002 2:27:00 PM	Element offline	172.20.27.155 (viaIP MCU-30)
⚠ warning	Sep 9, 2001 4:40:20 PM	Element offline	172.20.55.200 (viaIP gw-P20)
⚠ warning	Aug 10, 2002 9:07:00 PM	Element offline	AMIRF (DCS - 172.20.1.20)
⚠ warning	Aug 11, 2002 8:07:00 AM	Element offline	172.20.55.103 (GW2P)
⚠ warning	Jun 10, 1999 10:27:00 PM	Element offline	172.20.35.35 (viaIP gw-P20)

**Figure 5-1** Alarms Tab

## Events Tab

The **Alarms** view displays the following information:

- Alarm status. For example, **Warning**  or **Major/Minor** .
- Text message describing the alarm.

---





















**Note** You can access the relevant element manager by clicking the link in the **Element** column of each table row.

---

## EVENTS TAB

The **Events** tab enables you to sort the events reported by the system according to event severity, event time, event message and element. In addition, you can filter the events according to time period and severity level.

Current filter: Last 1 days, with a minimum severity of Cleared

Severity	Date & Time	Message	Element
 major	Oct 3, 2002 8:13:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 minor	Oct 3, 2002 7:58:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 7:43:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 7:28:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 major	Oct 3, 2002 7:13:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 minor	Oct 3, 2002 6:58:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 major	Oct 3, 2002 6:43:28 AM	PRI 2 remote frame alignment alarm	<a href="#">172.20.55.200 (viaIP gw-P20)</a>
 major	Oct 3, 2002 6:28:28 AM	PRI 2 local frame alignment alarm	<a href="#">172.20.55.200 (viaIP gw-P20)</a>
 major	Oct 3, 2002 6:13:28 AM	PRI offline	<a href="#">172.20.55.200 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 5:58:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 5:43:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 major	Oct 3, 2002 5:28:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 minor	Oct 3, 2002 5:13:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 4:58:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 4:43:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 major	Oct 3, 2002 4:28:28 AM	PRI offline	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 minor	Oct 3, 2002 4:13:28 AM	Gateway not registered with gatekeeper	<a href="#">172.20.35.35 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 3:58:28 AM	PRI 2 remote frame alignment alarm	<a href="#">172.20.55.200 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 3:43:28 AM	PRI 2 local frame alignment alarm	<a href="#">172.20.55.200 (viaIP gw-P20)</a>
 cleared	Oct 3, 2002 3:28:28 AM	PRI offline	<a href="#">172.20.55.200 (viaIP gw-P20)</a>

**Figure 5-2** Events Tab

The **Events** tab displays the following information:

Event severity level (Minor, Cleared, Intermediate, Warning, Minor, Major, Critical).

Date and time of the event.

- Text message describing the event.

---

**Note** You can access the relevant element manager by clicking the link in the **Element** column of each table row.

---

## FILTERING TRAPS

Select **Filter traps** from the **View** menu to display the **Filter Traps** dialog box, which enables you to define the time period and minimum severity levels of the events to display. Enter filter criteria and click **OK**. The events that correspond to your selection are displayed in the table.



**Figure 5-3** *Filter Traps Dialog Box*

---

**Note** You can also display the **Filter Traps** dialog box by clicking the link above the table.

---



# 6

## CONFERENCES AND CALLS VIEW

---

### WHAT'S IN THIS CHAPTER

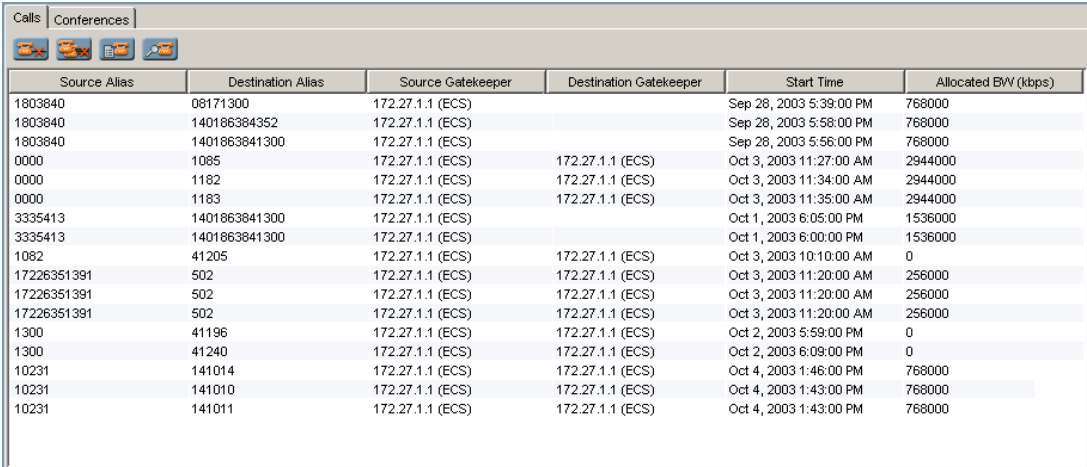
This chapter provides a description of the Conferences and Calls view of the Video Management System (VMS) Network Manager for managing calls and conferences and includes the following:

- [Calls Tab](#)
- [Conferences Tab](#)

## Calls Tab

## CALLS TAB

The **Calls** tab displays a table providing details of each call currently taking place on the selected element including source and destination aliases, source and destination gatekeepers of the calling parties, call start time and allocated bandwidth.



The screenshot shows a software interface with a 'Calls' tab selected. Below the tab are several icons. The main area is a table with the following columns: Source Alias, Destination Alias, Source Gatekeeper, Destination Gatekeeper, Start Time, and Allocated BW (kbps). The table contains 20 rows of call data.

Source Alias	Destination Alias	Source Gatekeeper	Destination Gatekeeper	Start Time	Allocated BW (kbps)
1803840	08171300	172.27.1.1 (ECS)		Sep 28, 2003 5:39:00 PM	768000
1803840	140186384352	172.27.1.1 (ECS)		Sep 28, 2003 5:58:00 PM	768000
1803840	1401863841300	172.27.1.1 (ECS)		Sep 28, 2003 5:56:00 PM	768000
0000	1085	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 11:27:00 AM	2944000
0000	1182	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 11:34:00 AM	2944000
0000	1183	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 11:35:00 AM	2944000
3335413	1401863841300	172.27.1.1 (ECS)		Oct 1, 2003 6:05:00 PM	1536000
3335413	1401863841300	172.27.1.1 (ECS)		Oct 1, 2003 6:00:00 PM	1536000
1082	41205	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 10:10:00 AM	0
17226351391	502	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 11:20:00 AM	256000
17226351391	502	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 11:20:00 AM	256000
17226351391	502	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 3, 2003 11:20:00 AM	256000
1300	41196	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 2, 2003 5:59:00 PM	0
1300	41240	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 2, 2003 6:09:00 PM	0
10231	141014	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 4, 2003 1:46:00 PM	768000
10231	141010	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 4, 2003 1:43:00 PM	768000
10231	141011	172.27.1.1 (ECS)	172.27.1.1 (ECS)	Oct 4, 2003 1:43:00 PM	768000

**Figure 6-1** Conferences and Calls View—Calls Tab

The **Calls** tab also allows you to disconnect ECS calls, either for each selected call or globally for all calls. You can display extended details per call by clicking on the table row and a call search option allows you to search by alias, IP address of the endpoint, service or conference ID.

## CONFERENCES TAB

The **Conferences** tab provides a table for viewing the current status of all conferences being hosted on the network, zone or selected MCU.

MCU	Conference ID					Total Participants	Local Participants	Reserved Partici...	Video bit rate	Zones
172.27.47.5	87123					2	2	3	320 kbps	
172.27.36.13	85222					3	3	3	320 kbps	
172.27.40.40	5656					2	2	3	640 kbps	
172.27.40.4	776					2	2	3	640 kbps	
172.27.36.21	67123					2	2	3	640 kbps	
172.27.14.3	888					2	2	3	320 kbps	
172.27.36.242	34					2	2	3	64 kbps	
172.27.36.246	66					2	2	3	128 kbps	

**Figure 6-2** Conferences Tab


The **Conferences** tab includes the following information:

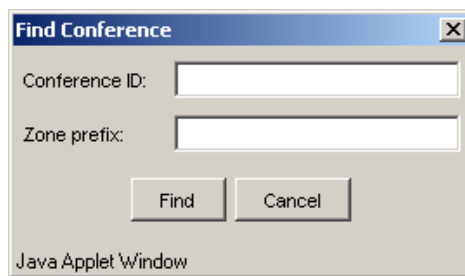
- **MCU**—IP address of the MCU on the which the conference is being hosted. Click on the link to view the element manager of the MCU (Administrator).
- **Conference ID**—Conference ID number. Click on the link to view the conference manager of the MCU (Conference Control).
- **Layout**—Video layout configuration of the conference.
- **Camera**—Indicates whether video is enabled for the conference.
- **Speaker**—Indicates whether audio is enabled for the conference.
- **Data**—Indicates whether data support is enabled for the conference.
- **Total Participants**—Number of current participants.
- **Local Participants**—Number of local participants on this MCU.

## Conferences Tab

- Reserved Participants—Number of reserved participants.
- Video Bit Rate—Maximum bit rate for the conference.
- Zone—Zone in which the conference is taking place.

### FINDING A CONFERENCE

Click the **Find** icon  above the table to display the **Find Conference** dialog box, which enables you to locate a particular conference in the table. Enter the conference ID or the zone prefix and click **Find**. The row in the table matching your search criteria is highlighted.



**Figure 6-3** Find Conference Dialog Box

---

**Note** You can use the [\*] wildcard when searching for conferences.

---

### ACCESSING THE MCU

You can access the element manager of the MCU (Administrator) by clicking the **MCU** link in the left-hand column of each table row.

You can access the MCU Conference Control interface using the link in the **Conference ID** column. This enables you to manage and take control of the conference. For more information about using the RADVISION MCU, see the *RADVISION MCU User Guide*.

# 7

## SETTINGS VIEW

---

### WHAT'S IN THIS CHAPTER

This chapter covers the basic principles for using the Settings view, and includes the following:

- Settings Interface
- Users Tab
- Alert Recipients Tab
- Traps Tab
- Alarms Tab
- Network Subsets Tab
- Logs Tab
- Element Logs Tab
- Element Access Tab
- Endpoint Management Tab
- Auto-detect Tab
- Cisco MCM Tab

### SETTINGS INTERFACE

The Settings interface includes the following tabs:

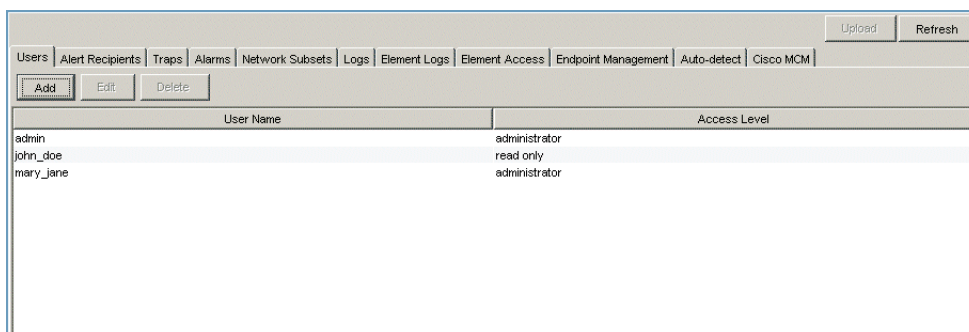
- **Users**  
Enables you to add new Video Management System (VMS) Network Manager users, as well as modify and remove existing users.
- **Alert Recipients**  
Enables you to add new alert recipients, as well as modify and remove existing alert recipients.
- **Traps**  
Enables you to automatically update the elements to either enable or disable sending traps.
- **Alarms**  
Enables you view and sort alarms generated by network elements. Allows you to customize alarm severity levels displayed per user profile, enable and disable alarms and create events for alarms to display in the [Events](#) table.
- **Network Subsets**  
Enables you to define subsets of the network according to zones and element types used to outline **Local user** profile network access capabilities.
- **Logs**  
Enables you to define the Video Management System (VMS) Network Manager log files and view the logs directory.
- **Element Logs**  
Enables you to define the element log files.
- **Element Access**  
Enables you to define the default access information for each element type.
- **Endpoint Management**  
Enables you to configure the default communication port and access settings for common endpoint types recognized by the Video Management System (VMS) Network Manager.
- **Auto-detect**  
Enables you to define when auto-detect should be performed to search the network for elements and add them to the Video Management System (VMS) Network Manager database.

- **Cisco MCM**

Enables you to configure the Video Management System (VMS) Network Manager to open a communication port with the Cisco MCM using the GKTMP TCP-based management protocol.

## USERS TAB

The **Users** tab enables you to create, modify or remove Video Management System (VMS) Network Manager user profiles, as well as define the access level for Video Management System (VMS) Network Manager user.



The screenshot shows a web interface for the 'Users Tab'. At the top, there are navigation tabs: 'Users', 'Alert Recipients', 'Traps', 'Alarms', 'Network Subsets', 'Logs', 'Element Logs', 'Element Access', 'Endpoint Management', 'Auto-detect', and 'Cisco MCM'. Below the tabs are buttons for 'Add', 'Edit', and 'Delete'. In the top right corner, there are 'Upload' and 'Refresh' buttons. The main content area is a table with two columns: 'User Name' and 'Access Level'.

User Name	Access Level
admin	administrator
john_doe	read only
mary_jane	administrator

**Figure 7-1** Users Tab

## ABOUT USER ACCESS

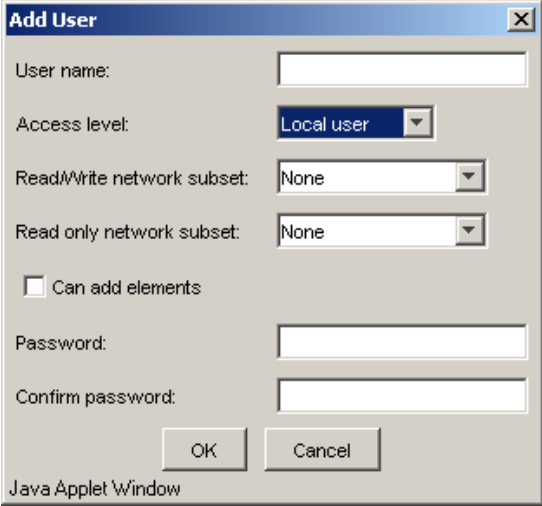
The Video Management System (VMS) Network Manager supports three types of network users:

- **Administrator**  
Full read/write access to all managed elements and zones on the network.
- **Read only**  
Read Only access to all elements and zones on the network.
- **Local user**  
Restricted access to managed elements and zones on the network. This user profile is defined with specific read/write and read only access according to zones, elements and criteria for network subsets configured in the [Network Subsets tab](#).

## ADDING USERS

Click **New** to display the **Add User** dialog box, which enables you to add new users and define user access rights. Add a new Video Management System (VMS) Network Manager user by typing a user name and password in the relevant fields and select the appropriate user access level.

**Local users** can also be configured with read/write access and read only access permissions according to zones and criteria for network subsets defined in the [Network Subsets tab](#). You can also indicate whether a local user may freely add new elements to the Video Management System (VMS) Network Manager database throughout all network zones and subsets.



**Figure 7-2** Add User Dialog Box

## MODIFYING USERS

Select a user from the displayed list and click **Edit** to display the **Edit User** dialog box. Modify the fields, as required. For more information, see the [Adding Users](#) section.

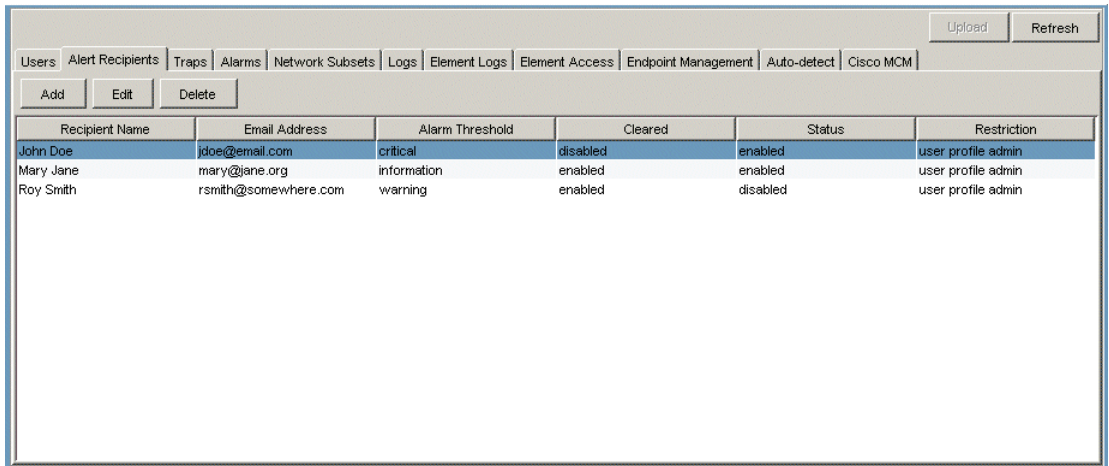
---

**Note** You can remove a user from the database by selecting the user from the list and then clicking **Delete**.

---

## ALERT RECIPIENTS TAB

The **Alert Recipients** tab enables you to create, modify or remove alert recipients. This includes defining the name and e-mail address of the recipient, the severity level of the alerts that will be sent to alert recipients and the user access profile of the recipients.



Recipient Name	Email Address	Alarm Threshold	Cleared	Status	Restriction
John Doe	jdoe@email.com	critical	disabled	enabled	user profile admin
Mary Jane	mary@jane.org	information	enabled	enabled	user profile admin
Roy Smith	rsmith@somewhere.com	warning	enabled	disabled	user profile admin

**Figure 7-3** Alert Recipients Tab

You should note the following:

- Local users only receive notifications about the alerts on the network subsets for which the local user has been defined as a recipient.
- The alarm level for which you configure an alert recipient to receive notifications is based on the alarm level definitions defined by that user.

---

**Note** The **Restriction** column indicates the user profile of the alert recipient according to user access profile settings configured in the [Users](#) tab.

---

## MAIL SERVER SETTINGS

You can modify the mail server through which alert messages are sent by e-mail using the iVIEW Manager Server Configuration utility. For more information, see [Appendix A](#).

---

**Note** To send email alerts outside of your mail domain to an external address, your mail server should be configured to allow mail relay. An alternative method is to forward the email from a local address to the desired external address.

---

## ADDING ALERT RECIPIENTS

Click **Add** to display the **Add Alert Recipient** dialog box, which enables you to add new alert recipients. Type the name and e-mail of the alert recipient. Select a user profile (Administrator, Read only, Local user) and select the minimum severity level of the alerts that will be sent (Warning, Minor, Major, Critical). Click **Notify on alarms clearing** to enable you to receive an error report via the e-mail, when the alarms have been cleared.

Select whether to include a custom subject line in the e-mail and enter a string for the custom subject line. You may also indicate whether to include in the custom subject line details of the elements reported in the alerts. Select **Enable alert** to activate the recipient.

---

### Note

1. In the **Edit Alert Recipients** dialog box, when you configure the **Minimum Severity** tab to **Critical** (for example), you will receive an e-mail notification for alarms that were configured only as **critical** by the user, that is selected in the **User Profile Field**.
  2. When you select a **Local User** (controls only the subset of the network) in the **User Profile** field, this alert recipient (i.e. the defined e-mail address) will receive notifications only for alarms that belong to elements that are part of this network subset. If you select an **Administrator** or **Read only** user, then you will receive notification on all the alarms.
-

**Add Alert Recipient**

Recipient name: admin2

Email address: a2@a.com

Select user profile: admin

Restrict to: All Network Subsets

Minimum severity: Information

Notify on alarms clearing

Use custom subject line  Include element info

Custom subject line

Enable alert

OK Cancel

Java Applet Window

**Figure 7-4** Add Alert Recipient Dialog Box

## MODIFYING ALERT RECIPIENTS

Select an alert recipient from the displayed list and click **Edit** to display the **Edit Alert Recipient** dialog box. Modify the fields, as required. For more information, see the [Adding Alert Recipients](#) on page 98.

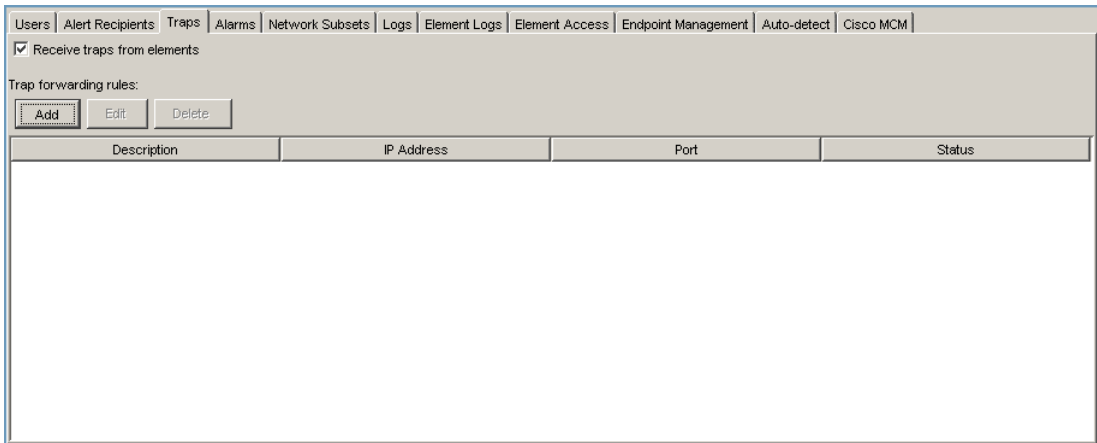
---

**Note** You can remove an alert recipient from the database by selecting the recipient and then clicking **Delete**.

---

## TRAPS TAB

The **Traps** tab enables you to define whether or not the Video Management System (VMS) Network Manager server receives SNMP traps such as alarms and events and allows you forward the traps to addresses specified in the trap forwarding rules. Select the **Receive traps from elements** checkbox to configure the managed elements to send SNMP traps to the Video Management System (VMS) Network Manager.



The screenshot shows the 'Traps' tab interface. At the top, there is a navigation bar with tabs: Users, Alert Recipients, Traps, Alarms, Network Subsets, Logs, Element Logs, Element Access, Endpoint Management, Auto-detect, and Cisco MCM. Below the navigation bar, there is a checkbox labeled 'Receive traps from elements' which is checked. Underneath, there is a section titled 'Trap forwarding rules:' with three buttons: 'Add', 'Edit', and 'Delete'. Below the buttons is a table with the following columns: Description, IP Address, Port, and Status. The table is currently empty.

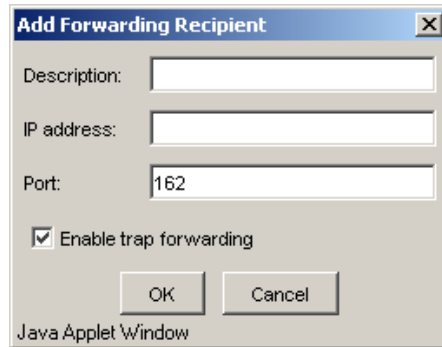
**Figure 7-5** Traps Tab

The **Traps** tab displays the following information:

- Description
- IP Address
- Port
- Status

## ADDING A TRAP FORWARDING RULE

Click **Add** to display the **Add Forwarding Recipient** dialog box, which enables you to define forwarding rules in which you specify an IP address and port number to which traps received from elements are forwarded. Click **OK** to add the new rule to the Video Management System (VMS) Network Manager database.



The screenshot shows a dialog box titled "Add Forwarding Recipient" with a close button in the top right corner. The dialog contains three text input fields: "Description" (empty), "IP address" (empty), and "Port" (containing the value "162"). Below these fields is a checked checkbox labeled "Enable trap forwarding". At the bottom of the dialog are two buttons: "OK" and "Cancel". The text "Java Applet Window" is visible at the bottom left of the dialog.

**Figure 7-6** Add Forwarding Recipient Dialog Box

---

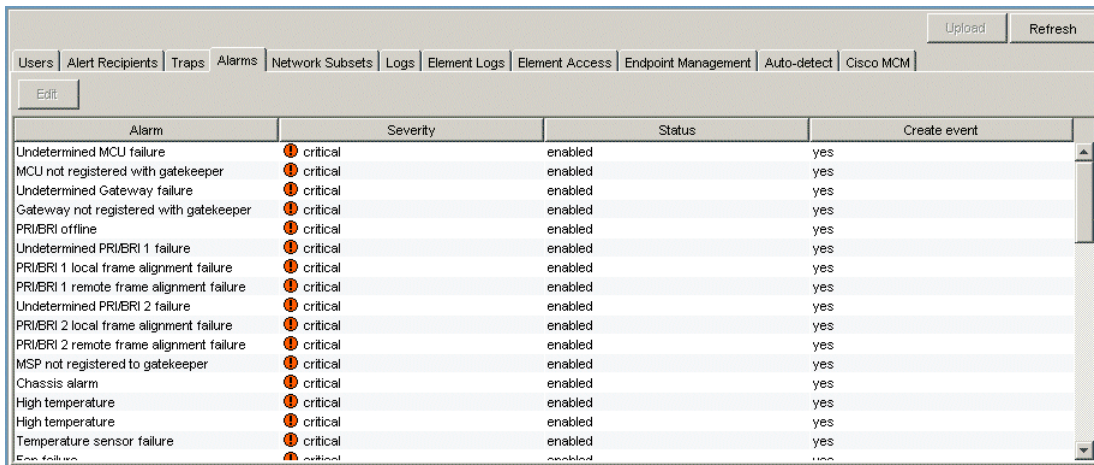
**Note** You can modify and delete existing trap forwarding rules using the **Edit** and **Delete** buttons.

---

## Alarms Tab

### ALARMS TAB

The **Alarms** tab enables you view and sort alarms generated by the elements in the network according to alarm status, alarm message, date and time or element. You can change the severity level displayed for each alarm according to the level defined by the current user, enable and disable alarms and create events for alarms to display in the [Events](#) tab.



Alarm	Severity	Status	Create event
Undetermined MCU failure	critical	enabled	yes
MCU not registered with gatekeeper	critical	enabled	yes
Undetermined Gateway failure	critical	enabled	yes
Gateway not registered with gatekeeper	critical	enabled	yes
PRIVRI offline	critical	enabled	yes
Undetermined PRIVRI 1 failure	critical	enabled	yes
PRIVRI 1 local frame alignment failure	critical	enabled	yes
PRIVRI 1 remote frame alignment failure	critical	enabled	yes
Undetermined PRIVRI 2 failure	critical	enabled	yes
PRIVRI 2 local frame alignment failure	critical	enabled	yes
PRIVRI 2 remote frame alignment failure	critical	enabled	yes
MSP not registered to gatekeeper	critical	enabled	yes
Chassis alarm	critical	enabled	yes
High temperature	critical	enabled	yes
High temperature	critical	enabled	yes
Temperature sensor failure	critical	enabled	yes
...	...	...	...

**Figure 7-7** Alarms Tab

The **Alarms** tab displays the following information:

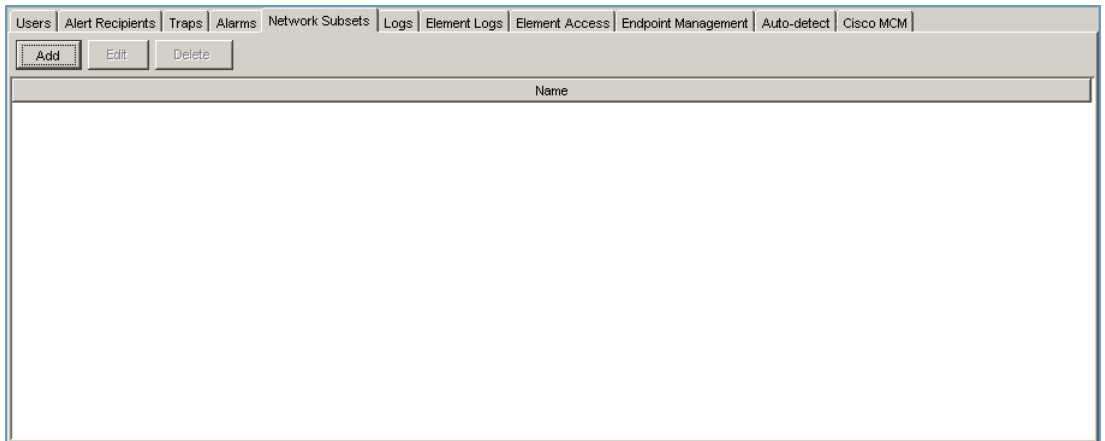
- Alarm
- Severity
- Status
- Create Event

### MODIFYING AN ALARM

Select an alarm and click **Edit** to display the **Edit Alarm Properties** dialog box which allows you to modify the alarm severity level assignment for each alarm, enable or disable the alarm and create an event which is displayed in the [Events](#) tab.

## NETWORK SUBSETS TAB

The **Network Subsets** tab enables you to define subsets of the network according to zones and element types using include and exclude criteria for use with **Local user** access level profiles.



**Figure 7-8** Network Subsets Tab

### ADDING A NETWORK SUBSET

Click **Add** to display the **Add Network Subset** dialog box for creating network subsets which you use to define areas of the network based on existing network zones and element types for use in **Local user** profiles. The **Add Network Subset** dialog box displays lists of include and exclude criteria for the network subset which contain details about the zone, child zone and element types specified in the criteria configuration. For more information about specifying criteria, see [Adding a Criteria](#) on page 104.

---

**Note** A subset contains all elements which match at least one *Include* criterion but do not match any *Exclude* criterion.

---

For more information about user profiles, see [About User Access](#) on page 95.

---

**Note** You can modify and delete existing network subsets using the **Edit** and **Delete** buttons.

---

## Network Subsets Tab

Zone	Child Zones	Element Type	Add
			Edit
			Delete

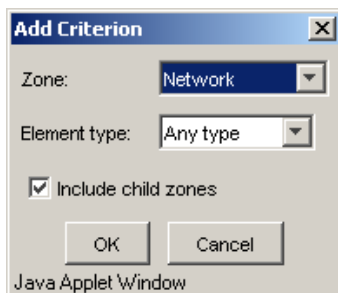
Zone	Child Zones	Element Type	Add
			Edit
			Delete

**Figure 7-9** Add Network Subsets Dialog Box

### ADDING A CRITERIA

Click **Add** in the **Include criteria** or **Exclude criteria** areas of the **Add Network Subset** dialog box to display the **Add Criterion** dialog box for creating include or exclude criteria for network management access using the current network subset.

The **Add Criterion** dialog box displays drop-down lists for selecting a network zone and element type and a checkbox to indicate whether child zones of the specified zone are contained in the criterion. Click **OK** to add the criterion to the relevant list in the **Add Network Subset** dialog box.



**Figure 7-10** Add Criteria Dialog Box

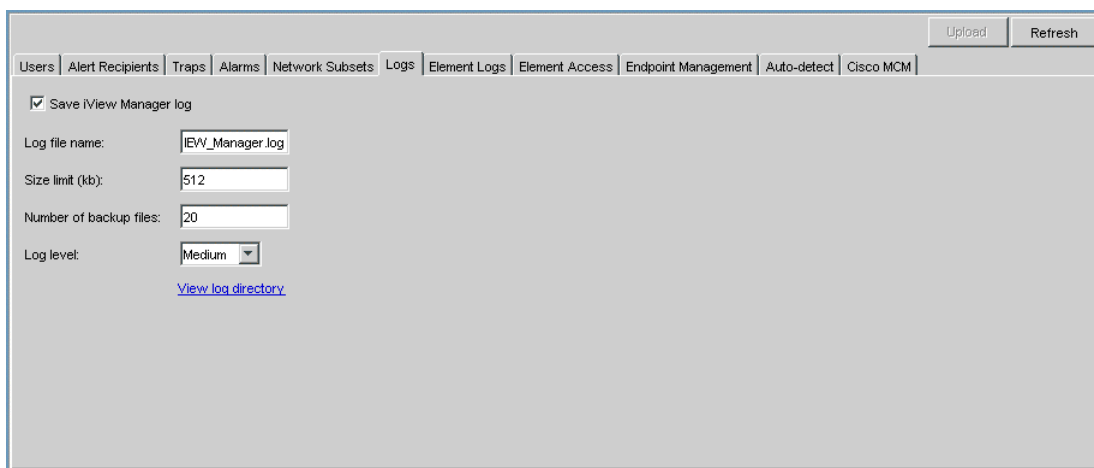
---

**Note** You can modify and delete existing criteria using the **Edit** and **Delete** buttons.

---

## LOGS TAB

The **Logs** tab enables you to keep a log of operations performed in the Video Management System (VMS) Network Manager. You can define the log file name, the maximum file size, the number of backup files to maintain and the level of detail to be included. In addition, you can click the link to view the log directory.

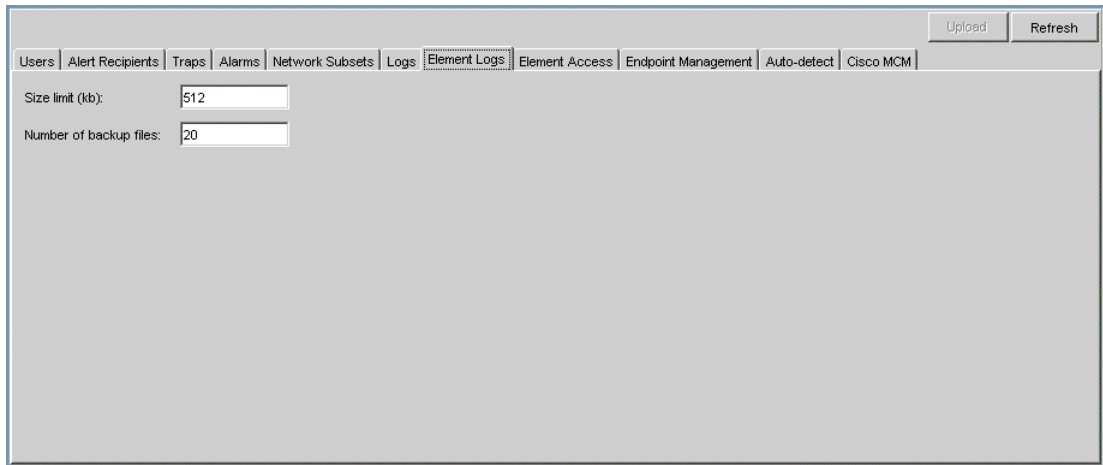


**Figure 7-11** Logs Tab

## Element Logs Tab

### ELEMENT LOGS TAB

The **Element Logs** tab enables the Video Management System (VMS) Network Manager to locally save log files for those elements, such as MCU elements and Gateways, that do not maintain a log of their own. You can define the maximum size of each log file, as well as the number of backup files to maintain.



The screenshot shows the 'Element Logs' tab selected in a navigation menu. The menu includes: Users, Alert Recipients, Traps, Alarms, Network Subsets, Logs, Element Logs (selected), Element Access, Endpoint Management, Auto-detect, and Cisco MCM. In the main content area, there are two input fields: 'Size limit (kb):' with a value of 512, and 'Number of backup files:' with a value of 20. At the top right of the content area are 'Upload' and 'Refresh' buttons.

**Figure 7-12** Element Logs Tab

### ELEMENT ACCESS TAB

The **Element Access** tab enables you to define the default access definitions for each element type in the network. Default element access definitions are used by Video Management System (VMS) Network Manager to access elements which use standard settings in order to perform element monitoring and configuration.

---

**Note** You can override the default element access settings in the **Access** tab for each element. For more information, see [Access Tab](#) on page 26.

---

**Figure 7-13** Element Access Tab

You can define access rights by selecting the element type from the **Element type** drop-down list, and then define access information, including read and write communities, user name and the password (Telnet user name, password and password enable for Cisco MCM), HTTP communication port and Telnet password. Click **Upload** to save the information to the Video Management System (VMS) Network Manager database.

Certain elements using parameters other than the default settings for the element type may be edited by selecting the element in the Network Tree view and modifying the element **Access** tab accordingly. For more information, see the [Network Tree View](#) chapter.

---

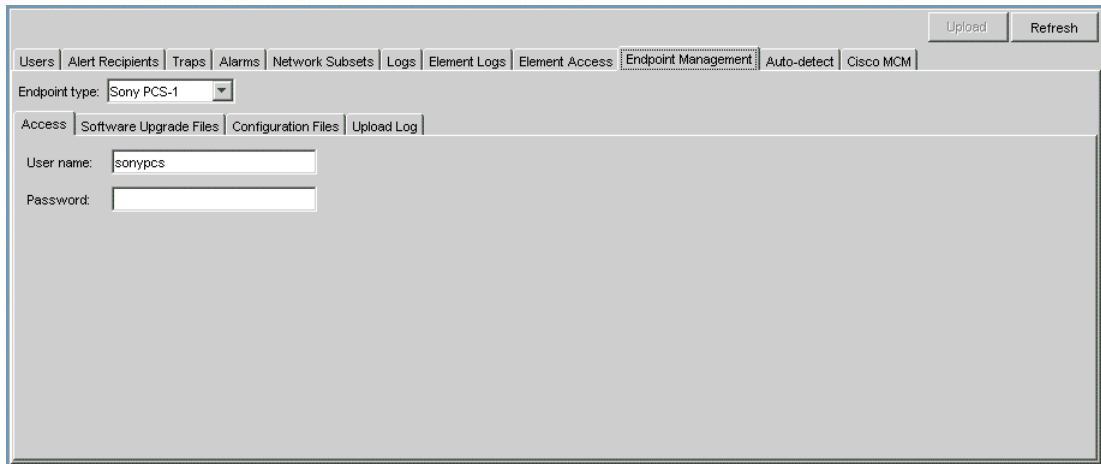
**Note** You can view SNMP Community names by selecting the **View SNMP Community names** option in the **View** menu, when the option is already enabled using the [Configuration Utility](#).

---

## Endpoint Management Tab

### ENDPOINT MANAGEMENT TAB

The **Access** sub-tab of the **Endpoint Management** tab enables you to configure the default communication port and access settings for common endpoint types recognized by the Video Management System (VMS) Network Manager.



The screenshot shows the 'Endpoint Management' tab selected in the VMS Network Manager interface. The 'Access' sub-tab is active, displaying a form for configuring access settings. The 'Endpoint type' is set to 'Sony PCS-1'. The 'User name' field contains 'sonypcs' and the 'Password' field is empty. The interface includes a navigation bar with tabs for 'Users', 'Alert Recipients', 'Traps', 'Alarms', 'Network Subsets', 'Logs', 'Element Logs', 'Element Access', 'Endpoint Management', 'Auto-detect', and 'Cisco MCM'. There are 'Upload' and 'Refresh' buttons in the top right corner.

**Figure 7-14** Endpoint Management Tab: Access

---

**Note** The default values configured in the **Access** tab may be overridden when configuring a single endpoint using the **Endpoints** tab in the **Network Tree** view. For more information, see [Additional Endpoints Tab](#) on page 52.

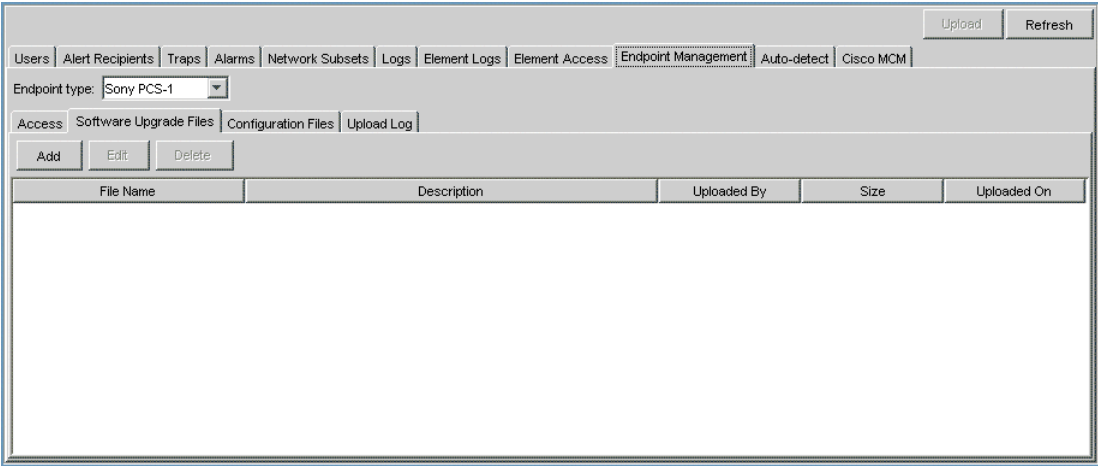
---

When you select a Sony endpoint that supports a software upgrade (PCS-1, PCS-11, PCS-G70, PCS TL-50) or an update configuration (all of these + PCS-1600) from the **Endpoint type** drop-down list, the following additional sub-tabs are available:

- [Software Upgrade Files](#)
- [Configuration Files](#)
- [Upload Log](#)

**SOFTWARE UPGRADE FILES**

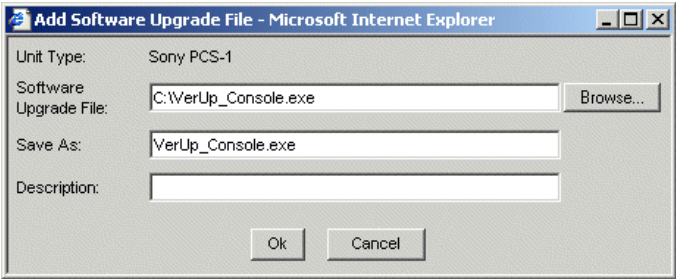
The **Software Upgrade Files** tab enables management of software upgrade files received from a third party distributor.



**Figure 7-15** Endpoint Management Tab: Software Upgrade Files

**ADDING A SOFTWARE UPGRADE FILE**

In the **Software Upgrade Files** tab, click **Add** to add a software upgrade file received from a third party distributor to the Video Management System (VMS) Network Manager database. The **Add Software Upgrade File** dialog box displays.



**Figure 7-16** Add Software Upgrade File Dialog Box

The **Add Software Upgrade File** dialog box includes the following options:

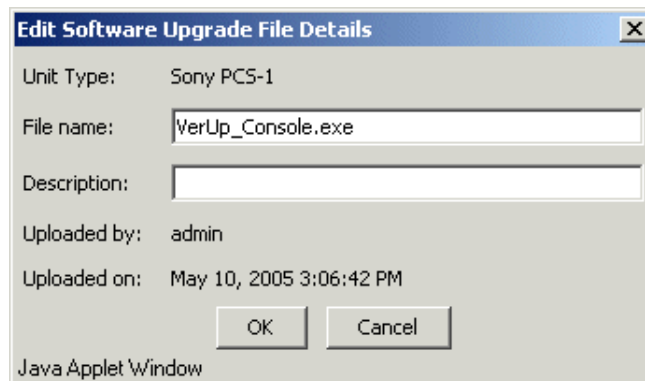
- Unit Type—Displays the endpoint type.
- Software Upgrade File—Type the full path of the software upgrade file to be added to the Video Management System (VMS) Network Manager database, or use the **Browse** button to navigate to the file location.
- Save As—Type the name of the file to be saved in the Video Management System (VMS) Network Manager database.
- Description—Type a description of the file.

Click **OK** to save the file in the Video Management System (VMS) Network Manager database.

Click **Cancel** to cancel the operation.

### MODIFYING A SOFTWARE UPGRADE FILE

Select the required software upgrade files from the **Software Upgrade Files** tab, and click **Edit** to modify the name and description of the selected files. The **Edit Software Upgrade File Details** dialog box displays.



**Figure 7-17** Edit Software Upgrade File Details Dialog Box

The **Edit Software File Details** dialog box includes the following options:

- Unit Type—Displays the name of the endpoint type.
- File name— Type the file name.
- Description—Type a description of the file.
- Uploaded by—Displays the name of the user who added the file to the Video Management System (VMS) Network Manager database.

- **Uploaded on**—Displays the time and date at which the file was added to the Video Management System (VMS) Network Manager database.

Click **OK** to save the changes in the Video Management System (VMS) Network Manager database.

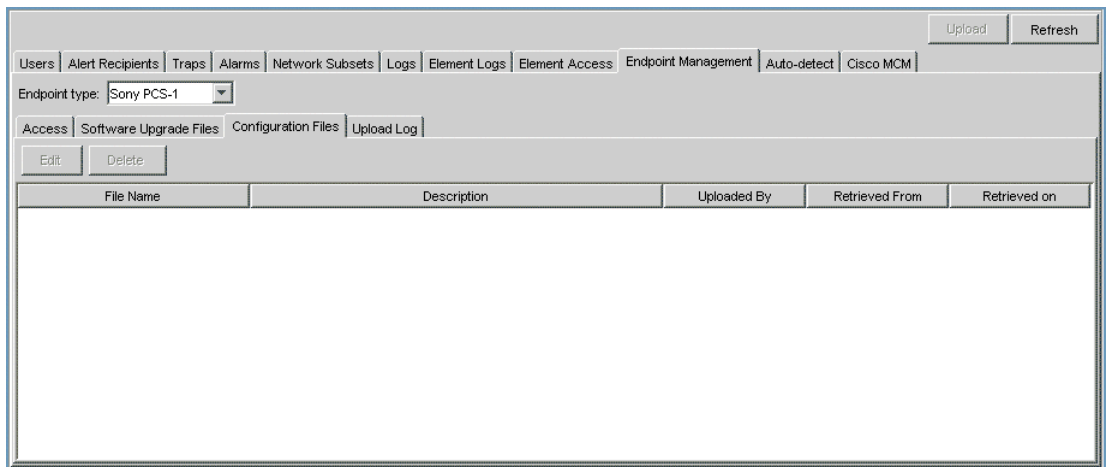
Click **Cancel** to cancel the operation.

#### DELETING A SOFTWARE UPGRADE FILE

Select the required software upgrade files from the **Software Upgrade Files** tab, and click **Delete** to remove the selected files from the Video Management System (VMS) Network Manager database.

#### CONFIGURATION FILES

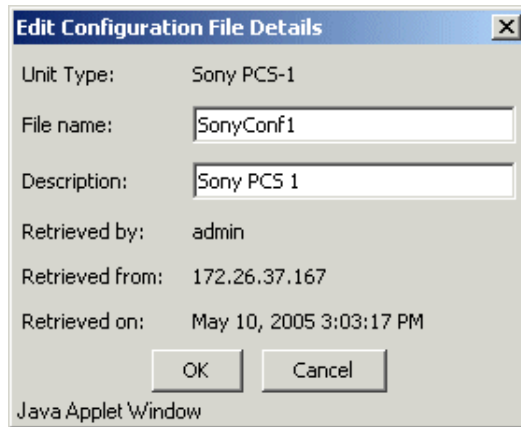
The **Configuration Files** tab displays the configuration files previously retrieved from endpoints and saved in the Video Management System (VMS) Network Manager database. For more information on the retrieving configuration information, see [Retrieving Configuration Parameters](#) on page 57.



**Figure 7-18** Endpoint Management Tab: Configuration Files

#### MODIFYING A CONFIGURATION FILE

Select the required endpoint configuration files from the **Configuration Files** tab, and click **Edit** to modify the name and description of the selected files. The **Edit Configuration File Details** dialog box displays.



**Figure 7-19** *Edit Configuration File Details Dialog Box*

The **Edit Configuration Dialog File** dialog box includes the following options:

- Unit Type—Displays the endpoint type.
- File name—Type the file name.
- Description—Type a description of the file.
- Retrieved by—Displays the name of the user who retrieved the file from the Video Management System (VMS) Network Manager database.
- Retrieved from—Displays the IP address of the endpoint from which the configuration parameters were retrieved.
- Retrieved on—Displays the time and date at which the file was retrieved.

## UPLOAD LOG

The **Upload Log** tab displays a history of endpoint update attempts.

Upload Type	File	Target IP	Time Submitted	Status	Next Retry	Retries
software	VerUpDos2.exe	172.27.37.157	10:08:55 05/04/2005	completed		
configuration	VerUpDos2.exe	172.20.27.45	10:06:57 05/04/2005	failed	10:58:33 05/04/2005	1 / 3
configuration	VerUpDos2.exe	172.20.27.45	10:05:43 05/04/2005	in progress		
configuration	fdgdfg	172.27.37.157	11:30:41 03/03/2005	completed		

**Figure 7-20** Endpoint Management Tab: Upload Log

The **Upload Log** tab displays the following information:

- Upload Type—The type of upload operation—**configuration** or **software upgrade**.
- File—The name of the configuration or software upgrade file.
- Target IP—The target endpoint IP address.
- Time Submitted—The time and date at which the initial upload attempt began.
- Status—The status of the upload operation—pending (before the first attempt), in progress, completed or failed.
- Next Retry—The time of the next attempt (in case the previous attempt failed).
- Retries—x/y where x is the number of failing update/upgrade attempts already performed and y is the total number of attempts that will be performed in case of failures.

Click **Delete** to delete the selected log records.

Click **Retry** to attempt to run the update.

## AUTO-DETECT TAB

The **Auto-detect** tab enables you to define policies for running the auto-detect mechanism to discover new elements.

Type	Description	Status
ECS/DCS/MSP	Windows 2000/XP	enabled
viaIP/INVISION	GW/MCU public	enabled

**Figure 7-21** Auto-detect Tab

The **Auto-detect** tab includes a checkbox which you can select to run auto-detect automatically whenever the server is restarted. In addition, you can run auto-detect at regular intervals by selecting the **Run autodetect every (hrs)** checkbox and then selecting the time interval from the drop-down list.

The **Auto-detect** tab includes a checkbox for selecting whether the Auto-detect routine uses the default element access information defined in the [Element Access](#) tab. You can also define additional access settings for element types with access settings which are different from the default settings. You can enable or disable each of the additional element access settings. This provides additional control for determining on which types of elements the auto-detect routine performs a search.

---

**Warning** Elements manually deleted from the Video Management System (VMS) Network Manager database are not detected when running subsequent auto-detect routines. Deleted elements must be manually added to the Video Management System (VMS) Network Manager database.

---

## ADDING AUTO-DETECT ACCESS INFORMATION

Click **Add** to display the **Add Auto-detect Access Information** dialog box, which enables you to add element type access information. Select the unit type in the drop-down list, enter a description and SNMP read community, SNMP write community, user name and password details. The SNMP read community is the only mandatory field to be filled. Select **Enable** to activate the access information setting.

**Figure 7-22** Add Auto-detect Access Information Dialog Box

---

**Warning** The access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element in order to retrieve the information from the element. If these fields are not configured correctly, the required information cannot be displayed.

---



---

**Note** You can view SNMP Community names by selecting the **View SNMP Community names** option in the **View** menu, when the option is already enabled using the [Configuration Utility](#).

---

## MODIFYING AUTO-DETECT ACCESS INFORMATION

Select an Auto-detect access information setting from the displayed list and click **Edit** to display the **Edit Auto-detect Access Information** dialog box. Modify the fields, as required. For more information, see the [Adding Auto-detect Access Information](#) section.

---

**Note** You can remove an Auto-detect access information setting from the database by selecting the access type and then clicking **Delete**.

---

## CISCO MCM TAB

The **Cisco MCM** tab enables you to configure the Video Management System (VMS) Network Manager to get calls and registration information from the Cisco MCM and allows you to modify the communication port number.



The screenshot shows a web-based configuration interface for the Cisco MCM tab. At the top right, there are 'Upload' and 'Refresh' buttons. Below them is a navigation menu with tabs for 'Users', 'Alert Recipients', 'Traps', 'Alarms', 'Network Subsets', 'Logs', 'Element Logs', 'Element Access', 'Endpoint Management', 'Auto-detect', and 'Cisco MCM'. The 'Cisco MCM' tab is currently selected. The main content area contains a checkbox labeled 'Automatically open port for MCM GKTMP' which is checked. Below this checkbox is a text input field labeled 'GKTMP port:' with the value '20000' entered.

**Figure 7-23** Cisco MCM Tab

---

**Note** If the GKTMP port is not opened either by the Video Management System (VMS) Network Manager or the Cisco MCM, information is updated less frequently.

---

You configure the Cisco MCM by selecting **Automatically open port for MCM GKTMP** to enable communication with the Video Management System (VMS) Network Manager via the MCM GKTMP TCP-based management

protocol. The default port is *20000* and automatically displays in the **GKTMP port** box which may also be set with an alternative value according to the settings on your MCM.



# 8

## FINDING AND MANAGING ELEMENTS

---

### WHAT'S IN THIS CHAPTER

This chapter covers the basic principles for finding and managing elements in the Video Management System (VMS) Network Manager, and includes the following:

- [Performing Auto-detect](#)
- [Adding Elements Manually](#)
- [Creating Custom Views](#)

### PERFORMING AUTO-DETECT

Auto-detect enables you to search the network for elements and add them to the Video Management System (VMS) Network Manager database. Auto-detect is performed by broadcasting requests to all SNMP communities defined in the Video Management System (VMS) Network Manager to RADVISION elements. Once these elements respond to the requests, the Video Management System (VMS) Network Manager can query the elements directly for full configuration and status details.

The auto-detect method of discovery may not find all the elements located behind equipment such as routers. Therefore, the Video Management System (VMS) Network Manager interface enables you to complete the database by adding elements manually.

---

**Note** Elements manually deleted from the Video Management System (VMS) Network Manager database are not detected in subsequent auto-detect procedures. These elements must be manually added to the Video Management System (VMS) Network Manager database. For more information, see [Adding Elements Manually](#).

---

---


**Warning** In order for auto-detect to work, the access field definitions for SNMP communities and Telnet must correspond with the settings configured in the selected element.

---

In the **Auto-detect** tab of the **Settings** view, you can configure the Video Management System (VMS) Network Manager to run auto-detect automatically whenever the server is restarted, or to run at set intervals. You can also initiate auto-detect manually at any time. For more information, see the [Settings View](#) chapter.



### To perform auto-detect

- ③ Click the **Auto-detect elements** icon  in any network view,  
OR  
Select **Auto-detect elements** from the **Tools** menu.  
The Video Management System (VMS) Network Manager interface is updated accordingly.

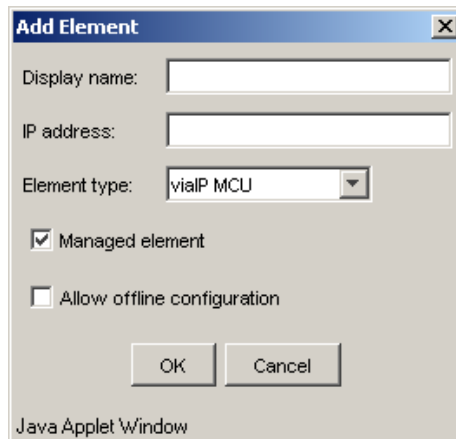
---

**Note** The auto-detect procedure may take some time, depending on the size of the network.

---

### ADDING ELEMENTS MANUALLY


The network views (**Network Tree**, **Network Table**, **Network Map**) enable you to add elements manually to the Video Management System (VMS) Network Manager database. When adding elements, you can define whether or not the Video Management System (VMS) Network Manager should manage the new element after it is defined. You can also set the new element to allow offline configuration. The Video Management System (VMS) Network Manager retains the configuration settings and updates the element when the element is online.



**Figure 8-1** Add Element Dialog Box



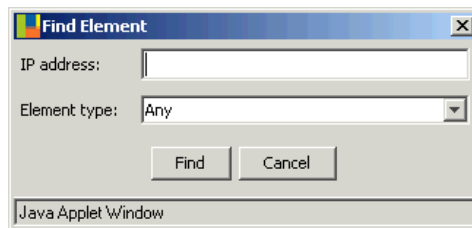
#### To add elements manually

1. Select the location in the Network Tree or Network Map view where the new element should be added.
2. Select **New | New element** from the **Edit** menu,  
–or–  
Click the **Add element** icon .
- The **Add Element** dialog box is displayed.
3. Type the element name and IP address in the fields provided.
4. Select the element type from the **Element type** drop-down list.
5. Select **Managed element** to enable the Video Management System (VMS) Network Manager manage the element.

6. Select **Allow offline configuration** to allow offline configuration of the element.
7. Click **OK**.

## FINDING ELEMENTS


The Video Management System (VMS) Network Manager interface enables you to search for specific elements in the database according to the IP address or element type.



**Figure 8-2** Find Element Dialog Box



### To find elements

1. Select **Find | Find element** from the **Edit** menu,  
 –or–  
 Click the **Find element** icon  from the Network Tree, Network Table or Network Map view.  
 The **Find Element** dialog box is displayed.
2. Define the search criteria for the element, as follows:
  - Type the IP address of the element in the **IP address** field to search for the element according to the IP address.
  - Select the element type from the **Element type** drop-down list to search for the element according to type.

## Adding Elements Manually

### 3. Click **Find**.

The required element is highlighted in the Network Tree, Network Table or Network Map view.

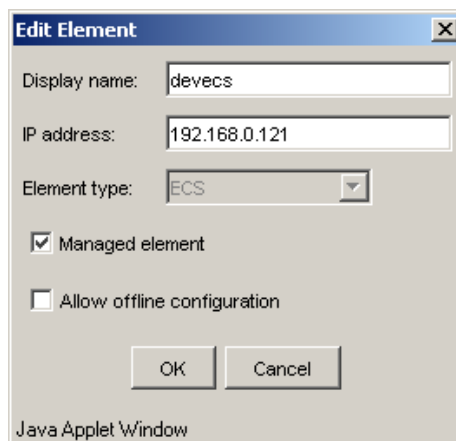
---

**Note** You can cancel pending offline configuration settings by right-clicking an offline element in the **Network Tree View** and selecting **Clear Offline Updates**. The element configurations settings which existed before the offline modifications, are restored.

---

## MODIFYING ELEMENTS


The Video Management System (VMS) Network Manager interface enables you to edit existing elements. You can change the name and IP address of an existing element, change the setting in the **Managed element** checkbox and set the element as configurable offline.



**Figure 8-3** Edit Element Dialog Box



### To edit elements

1. Select the element to edit in one of the network views.
2. Select **Edit | Modify | Modify element**,  
–or–  
Click the **Edit element** icon ,  
–or–  
Right click the element and then select **Edit element**.  
The **Edit Element** dialog box is displayed.
3. Modify the relevant fields. For more information, see [Adding Elements Manually](#) on page 122.

---

**Note** The element type cannot be modified.


---

4. Click **OK**.

## DELETING ELEMENTS

The Video Management System (VMS) Network Manager enables you to delete existing elements from the database.


---

**Warning** Deleted elements are not added to the Video Management System (VMS) Network Manager database in any subsequent auto-detect operations. You can only add a deleted element manually either using the **New element** option in the **Edit** menu, selecting the **Add element** icon  in the Network Views or by connecting to a deleted element that is inferred.

---



### To delete elements

1. Select the element to delete from one of the network views.
2. Select **Delete | Delete element** from the **Edit** menu,  
–or–  
Click the **Delete element** icon ,  
–or–  
Right click the element and then select **Delete element**.  
A confirmation window is displayed.

3. Click **Yes**. The selected element is removed from the database and the network views are updated accordingly.

---

**Note** A menu containing options for adding, editing and deleting elements and disabling pending offline configuration is available by right-clicking on the element in the **Network Tree View**.

---

## CREATING CUSTOM VIEWS

From the Network Tree view, you can add custom views to create your own tree structures according to criteria you define, such as the physical location or other customer-specific criteria. You can add folders and elements to the custom views and organize them as needed.



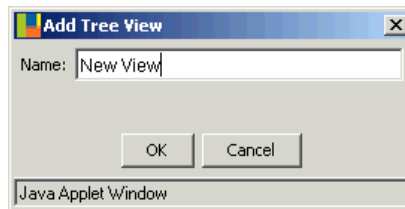
### To create custom views

1. Right click a tab in the Network Tree view (above the tree) and select **Add tree view**,

–or–

Select **New | New tree view** from the **Edit** menu.

The **Add Tree View** dialog box is displayed.



**Figure 8-4** Add Tree View Dialog Box

2. Type the name of the new tree view in the **Name** field.
3. Click **OK** to create the new tree view.  
The new tree view is added to the Network Tree view. By default, the new tree view includes a **Network** root directory and an **Unassigned** folder. The **Unassigned** folder contains all the elements in the network organized by type.
4. Create folders for organizing the elements in the tree view by right clicking the location in the tree where each folder should be located, and selecting **Add folder**.

5. Drag and drop elements from the **Unassigned** folder to the folders that you created.

---

**Note** You can rename or remove tree views either by from the **Edit** menu or by right-clicking the tree view. You can rename or remove folders by right clicking the folder and selecting the relevant option.

---



# APPENDIX A

## CONFIGURATION UTILITY

---

### WHAT'S IN THIS APPENDIX

This appendix provides a description of the Video Management System (VMS) Network Manager Server Configuration utility and includes the following:

- [VMS Manager Server Configuration Utility](#)
- [Utility Tabs](#)

### VMS MANAGER SERVER CONFIGURATION UTILITY

The Video Management System (VMS) Network Manager Server Configuration utility can be used after the Video Management System (VMS) Network Manager is installed to configure a mail server for issuing e-mail alerts, configure a web server port, enable security settings and run a check and repair procedure on the Video Management System (VMS) Network Manager database.

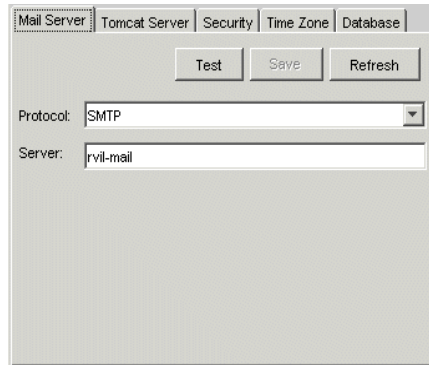
The Video Management System (VMS) Network Manager Server Configuration utility standalone application is installed on the host PC during the Video Management System (VMS) Network Manager setup. Select the Video Management System (VMS) Network Manager Server Configuration utility in the **Start** menu of the Video Management System (VMS) Network Manager directory.

## UTILITY TABS

### ABOUT THE MAIL SERVER TAB

Restart the Video Management System (VMS) Network Manager server after performing any modifications to enable the new settings to take effect.

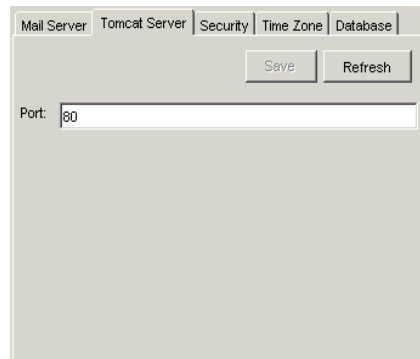
The **Mail Server** tab enables you to configure a mail server to use for issuing e-mail alerts. You can perform a test to ensure the mail server is valid.



**Figure A-1** Mail Server Tab

### ABOUT THE TOMCAT SERVER TAB

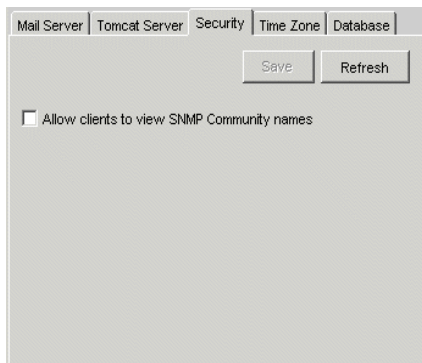
The **Web Server** tab enables you to configure the web server port number on which the Video Management System (VMS) Network Manager runs.



**Figure A-2** Tomcat Server Tab

## ABOUT THE SECURITY TAB

The **Security** tab enables you to specify whether clients can view SNMP community names for elements in locations of the interface where community details are configured and displayed.



**Figure A-3** Security Tab

The following locations display SNMP Community details.

- The **Access tab** of selected elements in the [About the Network Tree View](#).
- The **Element Access** tab in [Settings View](#).
- The **Add Auto-detect Access Information** dialog box and the **Edit Auto-detect Access Information** dialog box selected in the **Auto-detect** tab of the [Settings View](#).



### To view SNMP community names

1. Run the Video Management System (VMS) Network Manager Server Configuration utility and select **Allow clients to view SNMP Community Names** checkbox in the **Security** tab.
2. In the Video Management System (VMS) Network Manager interface, select **View SNMP Community names** in the [View Menu](#) of the Video Management System (VMS) Network Manager interface.

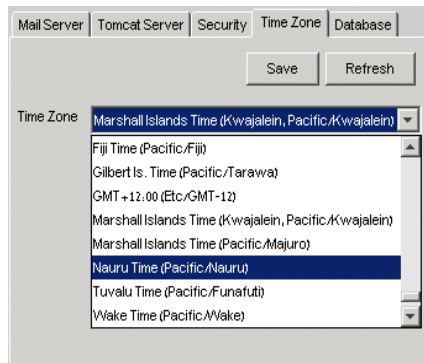
SNMP Community names display in the tabs containing SNMP Community details.

## Utility Tabs

### ABOUT THE TIME ZONE TAB

The **Time Zone** tab allows you to configure the time zone. The value that you configure influences the time that will be displayed in the VMS Log files.

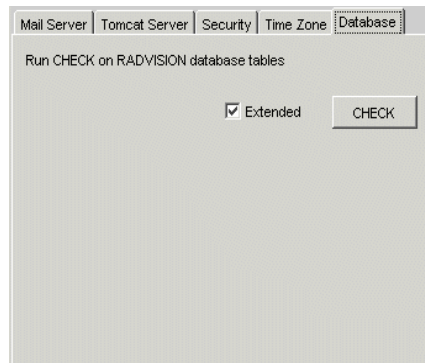
By default the value is set to the VMS server time zone.



**Figure A-4** Time Zone Tab

### ABOUT THE DATABASE TAB

The **Database** tab allows you to perform check and repair procedures on Video Management System (VMS) Network Manager database tables.



**Figure A-5** Database Tab

VMS database tables have two components: data and indexes.

The **CHECK** procedure performs the following:

- Checks for consistency of all indexes.
- Scans data rows to verify deleted links.
- Calculates and verifies key checks for all the data rows.
- The **Extended** procedure performs a complete index check.

If an error is found in a table, you are prompted to confirm repairs to the table. You can confirm each error individually or all errors at the same time.

The repair procedure deletes corrupted data rows and rebuilds all indexes. The extended check procedure rebuilds all indexes row by row which improves scanning speed and compression ratios.



# APPENDIX B

## ECS BANDWIDTH POLICIES

---

### WHAT'S IN THIS CHAPTER

This appendix provides a sample topology with subzones and describes bandwidth configuration for working with ECS version 3.5 elements using Video Management System (VMS) Network Manager and includes the following:

- [Sample Topology with Subzones](#)
- [Subzone Rules](#)
- [Applying Rules](#)
- [Calculating Used Bandwidth](#)
- [Dedicated Rules](#)
- [Default Rules](#)

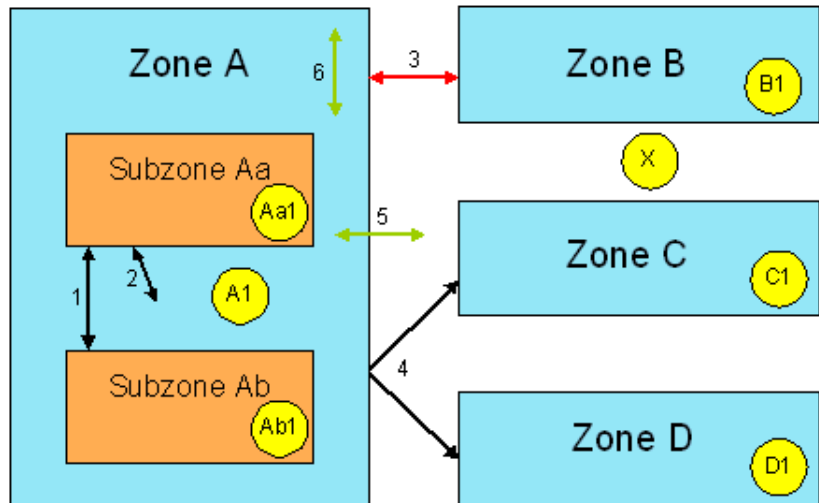
### SAMPLE TOPOLOGY WITH SUBZONES

Figure B-1 shows four Gatekeeper Zones (**A**, **B**, **C** and **D**), two subzones (**Aa** and **Ab**) and seven endpoints (**Aa1**, **Ab1**, **A1**, **B1**, **C1**, **D1** and **X**). [Table B-1](#) on page 137 defines the rules configured for this topology.

- Subzones **Aa** and **Ab** are in Zone A.
- Endpoint **Aa1** is in Subzone Aa.
- Endpoint **Ab1** is in Subzone Ab.
- Endpoint **A1** is in Zone A, but not in any subzone.
- Endpoints **B1**, **C1** and **D1** are in Zones B, C and D respectively.
- Endpoint **X** is not a member of any of the defined Gatekeeper Zones.

The arrows numbered 1 to 6 in the sample topology represent rules. For more information, see [Subzone Rules](#) on page 137.

## Sample Topology with Subzones



**Figure B-1** Sample Subzone Topology

## SUBZONE RULES

This section describes the rules shown in [Figure B-1](#) on page 136.

### SAMPLE RULES

[Table B-1](#) shows the available bandwidth according to the rules configured for an ECS in Zone A of the sample topology in [Figure B-1](#) on page 136.

**Table B-1** *Bandwidth Per Rule*

Rule number	For calls between ...	and between ...	Available bandwidth (Mbps)
1	Subzone Aa	Subzone Ab	5
2	Subzone Aa	Anywhere	10
3	Zone A	Zone B	20
4	Zone A	Zones C and D	20 (dedicated—see <a href="#">Dedicated Rules</a> on page 139)
5	Zone A	Anywhere	25 (default—see <a href="#">Default Rules</a> on page 140)
6	Any subzone	Anywhere	1 (default—see <a href="#">Default Rules</a> on page 140)

**Note** Rule 6 is used for calls between endpoints in different subzones which are not governed by any other defined rule. For example, calls between endpoints A1 and Aa1 in [Figure B-1](#) on page 136.

## Applying Rules

Table B-2 shows which rules are activated by differing call scenarios.

**Table B-2** Rules Used in Sample Call Scenarios

Source endpoint	Destination endpoint	Rules used
Aa1	Ab1	Rules 1 and 2
Aa1	A1	Rule 2
Aa1	B1	Rules 2 and 3
Aa1	C1	Rules 2, 4 and 5
Aa1	D1	Rules 2, 4 and 5
Aa1	X	Rules 2 and 5
A1	B1	Rules 3 and 5
A1	C1	Rule 4
A1	X	Rule 5
Ab1	A1	Rule 6

## APPLYING RULES

This section describes the order in which rules are applied to calls.

### FOR INTER-ZONE CALLS

1. All relevant dedicated rules are applied.
2. If there are no relevant dedicated rules, all relevant non-dedicated rules (including default rules) are applied.
3. Any relevant subzone rules are applied.

### FOR INTER-SUBZONE CALLS

1. All relevant dedicated rules are applied.
2. If there are no relevant dedicated rules, all relevant non-dedicated rules are applied.
3. If there are no relevant dedicated rules and no relevant non-dedicated rules, and the endpoints belong to different subzones, the default subzone rule will apply.

---

**Note** The inter-subzone algorithm is skipped if both endpoints are in the same subzone, or if both endpoints belong to no subzone. Endpoints that are not members of any subzone are considered to be in the same subzone, and are automatically placed in the default subzone. The default subzone rules will then apply to the endpoints.

---

## CALCULATING USED BANDWIDTH

The bandwidth required by a call must be available via each of the rules used by that call. For example, the call between endpoints Aa1 and B1 in [Table B-2](#) uses rules 2 and 3. The bandwidth allowed by each of these rules is as follows, according to [Table B-1](#):

- Rule 2—10 Mbps
- Rule 3—20 Mbps

Assume that the call requires 5 Mbps of bandwidth and that no other calls are currently in progress. When the call connects, 5 Mbps will be used for each of Rules 2 and 3. The available bandwidth will fall to 5 Mbps for Rule 2, and to 15 Mbps for Rule 3.

---

**Warning** A call will fail if there is not enough bandwidth available for any of the rules used by that call. The ECS bandwidth restriction mechanism blocks the call on first rule that does not have enough bandwidth available.

---

## DEDICATED RULES

You can use dedicated rules with, for example, leased lines or for a dedicated network connection between subzones or zones. A dedicated rule (such as Rule 4 in [Table B-1](#)) is a rule which applies to calls between specified endpoints, subzones or zones. For example, in [Table B-1](#), Rule 4 is a dedicated rule between Zone A and Zone C, and between Zone A and Zone D. A call governed by a dedicated rule will not be governed by any non-dedicated rule.

## Default Rules

The bandwidth used a call which activates a dedicated rule is not included in the used bandwidth calculation described in the [Calculating Used Bandwidth](#) section.

A non-dedicated rule can govern any call that is not dedicated.

## DEFAULT RULES

A **default zone rule** (such as Rule 5 in [Table B-1](#)) applies to any inter-zone call that does not match any of the defined dedicated rules.

A **default subzone rule** (such as Rule 6 in [Table B-1](#)) applies to any inter-zone call that does not match any of the defined inter-subzone rules (dedicated or non-dedicated).

# INDEX

---

## A

- Adding Alert Recipients 98
- Adding Auto-detect Access Information 115
- Adding Multipoint Processors 63
- Adding Services 67
- Adding Users 96
- Adding Video Processors 64
- Additional Cisco MCM tabs 68
- Additional DCS tab 79
  - adding MCUs 79
- Additional ECS tabs 31
- Additional Endpoints tab 52
- Additional Gateway tab 67
- Additional MCU tabs 61
- Additional Network tabs 28
- Alarms tab 85
- Alarms view 4
  - Alarms tab 15, 85
  - Events tab 86
- Alert Recipients
  - modifying 99
- Auto-Detect 3, 120

## C

- Centralized Log Management 5
- Children 47
- Cisco MCM
  - configuration 4
- Community access 26
- Conferences and Calls view
  - Calls tab 90
  - Conferences tab 91
- Configuration Utility 129

- Database tab 132
- Mail Server tab 130
- Security tab 131
- Tomcat Server tab 130
- Configuring
  - Cisco MCU 24
  - DCS 24
  - ECS 20
  - Gateway 24
  - MCU 22
  - Terminal managers 5
- Configuring Protocols 61
- Custom views 126

## D

- Defining bandwidth
  - ECS version 3.5 39
  - up to ECS version 3.2 38
- Defining subzones 33

## E

- ECS
  - configuration 4
- ECS hierarchy
  - children 47
  - neighbors 50
  - parent 45
- Element configuration 4
- Element management 11, 82, 84
- Element Managers
  - configuration 5
- Elements
  - adding 122
  - deleting 125
  - editing 124

- finding 123
- Endpoint Management tab 108
- Events tab 86
- Events view
  - Events tab 16

## F

- Features vii
- Filtering Traps 87
- Finding a conference 18, 92
- Finding Elements 123

## G

- Gateway
  - configuration 4
- Global Services tab 29

## H

- Hierarchy tab 28

## L

- Logs
  - ECS 25
  - Gateway 26
  - MCM 26
  - MCU 25

## M

- MCM
  - Bandwidth Rules 74
  - command 77
  - debug flags 76
  - local zones 69
  - Prefixes 72
  - remote zones 70
- MCU
  - configuration 4
- MCU access 92
- Modifying Auto-detect Access Information 116

- Modifying users 96
- MVP 62

## N

- Neighbors 50
- Network Map
  - navigating 84
- Network Map view 83
- Network Status 2
- Network Table view 81
- Network Tree tabs 12
- Network Tree view 8, 10
  - Access tab 26
  - Additional Cisco MCM tabs 68
  - Additional DCS tab 79
  - Additional ECS tabs 31
  - Additional Endpoints tab 52
  - Additional Gateway tab 67
  - Additional MCU tabs 61
  - Additional Network tabs 28
  - Calls tab 19
  - Conferences tab 17
  - Configure tab 20
  - Elements tab 14
  - Hierarchy tab 28
  - Logs tab 25
  - Monitor Tab 12
  - Services tab 32
- Network Views 5

## P

- Parent 45

## R

- Registering MPs 62
- Registration
  - MCU 79
- Requirements
  - system 2

## S

- Services 66

- ECS 32
- Gateway 67
- MCU 66
- viewing 10, 12
- Settings view 94
  - Alarms tab 102
  - Alert Recipients tab 97
  - Auto-Detect tab 114
  - Cisco MCM tab 116, 117
  - Element Access tab 106
  - Element Logs tab 106
  - Endpoint Management tab 108
  - Logs tab 105
  - Network Subsets tab 103
  - Traps tab 100
  - Users tab 95
- Software Upgrade Files 109
- Subzone rules 135, 137
  - applying rules 138
  - calculating used bandwidth 139
  - dedicated rules 139
  - defaults 140
  - sample 137

## Z

- Zone management 8

## U

- Upgrading Sony endpoints 60
- User Access 95

## V

- Viewing MCUs 79
- Viewing conferences 2
- Viewing events 4
- Views
  - Custom 126
  - Network Map 83
  - Network Table 81
  - Network Tree 8
  - Settings 94
- VMS Network Manager
  - overview 1, 2
- VPS 64

