Dialogic® IP Media Server Release 2.5.0

Installation and Operations Guide

April 2009 64-0436-01

www.dialogic.com

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses**

may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.

Dialogic, Dialogic Pro, Brooktrout, Diva, Cantata, SnowShore, Eicon, Eicon Networks, NMS Communications, NMS (stylized), Eiconcard, SIPcontrol, Diva ISDN, TruFax, Exnet, EXS, SwitchKit, N20, Making Innovation Thrive, Connecting to Growth, Video is the New Voice, Fusion, Vision, PacketMedia, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation or its subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Hardware Limited Warranty

Warranty for Hardware Products: Dialogic Corporation or its subsidiary that originally sold the hardware product to you ("Dialogic") warrants to the original purchaser ("Purchaser") of this hardware product ("Product"), that at the time of delivery the Product supplied hereunder will be free from defects in material and workmanship. This warranty is for the standard period for such Product set out on Dialogic's website at http://www.dialogic.com/warranties at the date of purchase, provided the Product remains unmodified, is operated under normal and proper conditions in accordance with its published specifications and documentation, and the system is not opened by unauthorized personnel. The warranty is also void if the defect has resulted from accident, misuse, abuse or misapplication. Any Product which becomes defective during the warranty period and is returned by Purchaser to Dialogic's Authorized Service Center shipping prepaid with a Return Material Authorization (RMA) number (which must be obtained from Dialogic before any return) within thirty (30) days after discovery of the defect, with a written description of the defect, will be repaired or replaced at Dialogic's option. Dialogic will not accept C.O.D. shipments. Dialogic reserves the right to refuse to repair or replace any Product which shows signs of abuse, misuse, neglect or has been altered in any way, including but not limited to Products which have been (i) used in environments which exceed operating tolerances such as supplied voltages and signals or (ii) stored under improper temperature or humidity conditions or (iii) used with equipment, software or interfacing not furnished by Dialogic or (iv) improperly packaged or shipped or (v) harmed by Purchaser or its agents' fault or negligence or (vi) repaired or modified without Dialogic's prior written consent . Purchaser must exercise proper electrostatic discharge (ESD) precautions and pack the Product and the other returned diagnostic information **in the original Dialogic packaging, including the antistatic bag/container and an ESD foam-filled cardboard box. Purchaser may void the warranty if the Product is improperly packaged or shipped**. Dialogic will bear the cost to return the repaired or replaced Product to the location specified on the Return Material Authorization (RMA) form by a method it chooses. If the Purchaser desires a specific form of conveyance, the Purchaser must bear the cost of shipment. All risk of loss shall be with the Purchaser during any and all shipments of the Product. Duties and import fees are the responsibility of the Purchaser.

Additional Exclusions: Dialogic will have no obligation to make repairs or replacements to the Product due to causes beyond the control of Dialogic, including, but not limited to, power or air conditioning failure, acts of God, improper interface with other units, or malfunction of any equipment or software used with the Dialogic Product(s). If Dialogic is requested and agrees to make repairs or replacements necessitated by any such causes, Purchaser will pay for such service or replacement at Dialogic's then prevailing rates.

No Other Warranties: DIALOGIC DISCLAIMS AND PURCHASER WAIVES ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY AGAINST LATENT DEFECTS, WITH RESPECT TO ANY DIALOGIC PRODUCT.

No Liability for Damages: IN NO EVENT SHALL DIALOGIC OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, INTERRUPTION OF ACTIVITIES, LOSS OF INFORMATION OR OTHER PECUNIARY LOSS AND DIRECT OR INDIRECT, CONSEQUENTIAL, INCIDENTAL, ECONOMIC OR PUNITIVE DAMAGES) ARISING OUT OF THE USE OF OR INABILITY TO USE ANY DIALOGIC PRODUCT.

Limitation of Liability: DIALOGIC'S MAXIMUM CUMULATIVE LIABILITY SHALL BE LIMITED TO THE AMOUNTS ACTUALLY PAID BY PURCHASER TO DIALOGIC FOR THE SPECIFIC PRODUCT BEING THE OBJECT OF THE CLAIM. PURCHASER RELEASES DIALOGIC FROM ALL AMOUNTS IN EXCESS OF THE LIMITATION. PURCHASER ACKNOWLEDGES THAT THIS CONDITION IS ESSENTIAL AND THAT DIALOGIC WOULD NOT SUPPLY TO PURCHASER IF IT WERE NOT INCLUDED. THIS WARRANTY EXPRESSLY DOES NOT APPLY TO ANYONE OTHER THAN PURCHASER.

Contents

List of Figures

List of Tables

About this Publication

The Dialogic® IP Media Server is a standards-based SIP and VoiceXML server that performs a wide variety of media processing functions.

This media sever also provides a cost-effective and scalable IP media option, as it can power a broad range of voice and video services for next generation wireline, wireless, and broadband services.

This section describes this manual and the contents of the manual set and consists of the following sections:

- Using this Publication
- Contacting Dialogic Technical Services and Support

Using this Publication

Audience and Purpose

This manual is for network or system administrators responsible for installing and configuring the Dialogic® IP Media Server.

Organization and Content

Chapter 1, “Introduction”, provides an overview of the structure and operation of the Dialogic® IP Media Server.

Chapter 2, “Installing the Media Server”, explains how to install and configure the IP Media Server.

Chapter 3, “Using the Web User Interface (Web UI)”, explains how to use the Web User Interface.

Chapter 4, “Configuring the Dialogic® IP Media Server”, describes procedures for configuring the IP Media Server for operation.

Chapter 5, “Operations, Administration, and Maintenance”, describes procedures for operating, administering, and maintaining the IP Media Server.

Appendix A, “Compliance and Standards Information”, describes the IP Media Server’s compliance with standards.

Appendix B, “Troubleshooting”, provides troubleshooting procedures for the IP Media Server.

Appendix C, “Required Red Hat Enterprise Linux Packages” lists the software packages that are required for the IP Media Server.

Dialogic® IP Media Server Documentation Set

The Dialogic® IP Media Server is documented in the following publications:

- The *Installation and Operations Guide* provides instructions for configuring, administering, and maintaining the IP Media Server.
- The *Application Developer's Guide* provides information for application developers who choose to use the IP Media Server to deploy network announcements, conferences, and Interactive Voice Response (IVR) in a voice over IP (VoIP) environment.
- *Installing Red Hat Enterprise Linux 4.0 for the IP Media Server* describes how to install and configure Red Hat Enterprise Linux 4 if you are installing the licensed software version of the IP Media Server.
- *Installing Red Hat Enterprise Linux 5.0 for the IP Media Server* describes how to install and configure Red Hat Enterprise Linux 4 if you are installing the licensed software version of the IP Media Server.
- The *License Activation Guide* describes how to activate the license for your Dialogic® IP Media Server.
- *Upgrading from Release 2.4.0 to 2.5.0 on Red Hat Enterprise Linux ES Platform* provides information and instructions for upgrading from IP Media Server Release 2.4.0 to IP Media Server Release 2.5.0 on platforms running Red Hat Enterprise Linux ES Platform. It also includes instructions for downgrading from 2.5.0 to 2.4.0 in the event that you need to restore your previous configuration.

Printed and Electronic Document Formats

The documentation package for the IP Media Server contains a printed copy of Release Notes and a CD including electronic versions of both the IP Media Server manuals, and Release Notes in PDF format. The PDF files require the Adobe Acrobat reader, a free download from www.adobe.com.

Document Conventions

Notes, Cautions, and Warnings

Notes contain tips and information of general interest, for example:

Cautions and warnings appear when appropriate throughout the manual.

Cautions alert you to situations that can make system administration less effective or can compromise system performance or security. For example:

Before changing the configuration of a running system, always back up the current configuration using the System→Config Backups command.

Warnings alert you to situations that could cause physical harm to an operator, or damage to the IP Media Server. For example:

If an interface is deactivated, all traffic on that interface will be dropped.

Links in PDF

Hypertext links in the PDF version of this manual use non-serif font. You can click on a cross reference to move to the information it references.

Index entries and Table of Contents listings are also clickable links in the PDF format. After you jump to a link, use the Back button on the Acrobat Reader toolbar to return to your prior location.

Contacting Dialogic Technical Services and Support

For more information, contact Dialogic Technical Services and Support at:

http://www.dialogic.com/support/

When reporting an issue to Technical Services and Support, please make sure you provide the following information:

- Full description of the issue.
- Version of the IP Media Server software you are using.
- IP Media Server log files.
- Whether the issue is reproducible; the steps that you took.

Please note that the latest software update and release notes are available from Dialogic support page.

Ordering Licenses

In order to purchase Dialogic software products, you must have a license to use these products. For directions on how to acquire licenses, see the Dialogic® IP Media Server *License Activation Guide*.

1 - Introduction

This chapter provides an overview of the Dialogic® IP Media Server (which is referred to in this document as the “IP Media Server” or “Media Server” or IPMS” or “MS”).

This chapter includes the following sections:

- Overview of the IP Media Server
- Supported Applications

Overview of the IP Media Server

The Dialogic® IP Media Server is capable of handling processing tasks associated with next generation voice, video, and data applications. The IP Media Server processes, manages, and delivers media resources for IP-based services when one or more third-party application servers, softswitches, or telephony applications provide direction to do so.

The IP Media Server is capable of handling media in various forms. Streaming media, such as real-time voice, most often takes the form of Real Time Protocol (RTP) streams encapsulated in UDP/IP packets. Other media, such as recorded announcement files, are stored locally or on remote servers and retrieved using the Network File System (NFS) or HTTP protocol.

Figure 1 illustrates the role of the Dialogic® IP Media Server in a network and how it communicates with other network resources and devices.

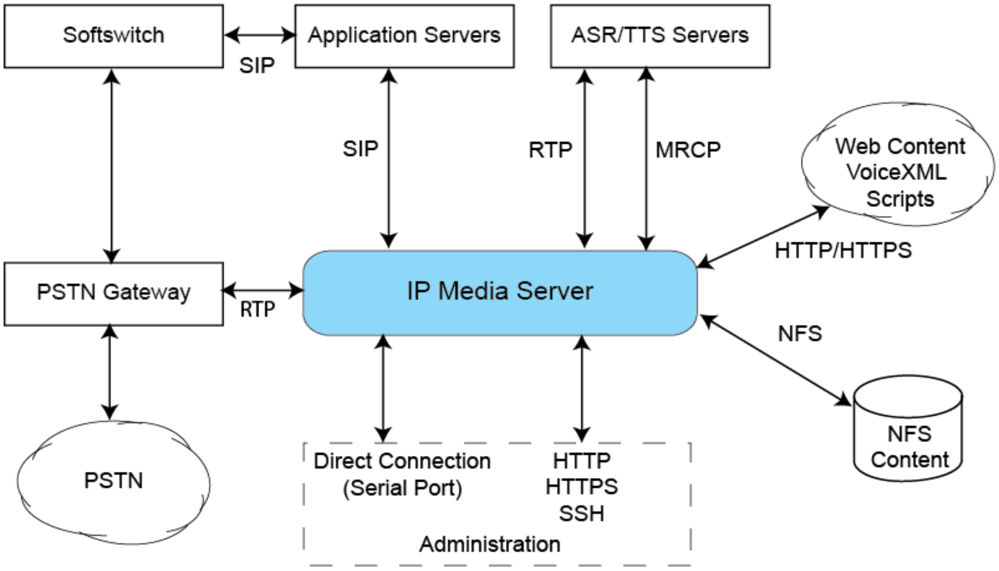


Figure 1. The IP Media Server in a Network

IP Media Server Components

The IP Media Server consists of several stand-alone processes and integrations with standard Linux applications such as Apache. Figure 2 illustrates these major components.

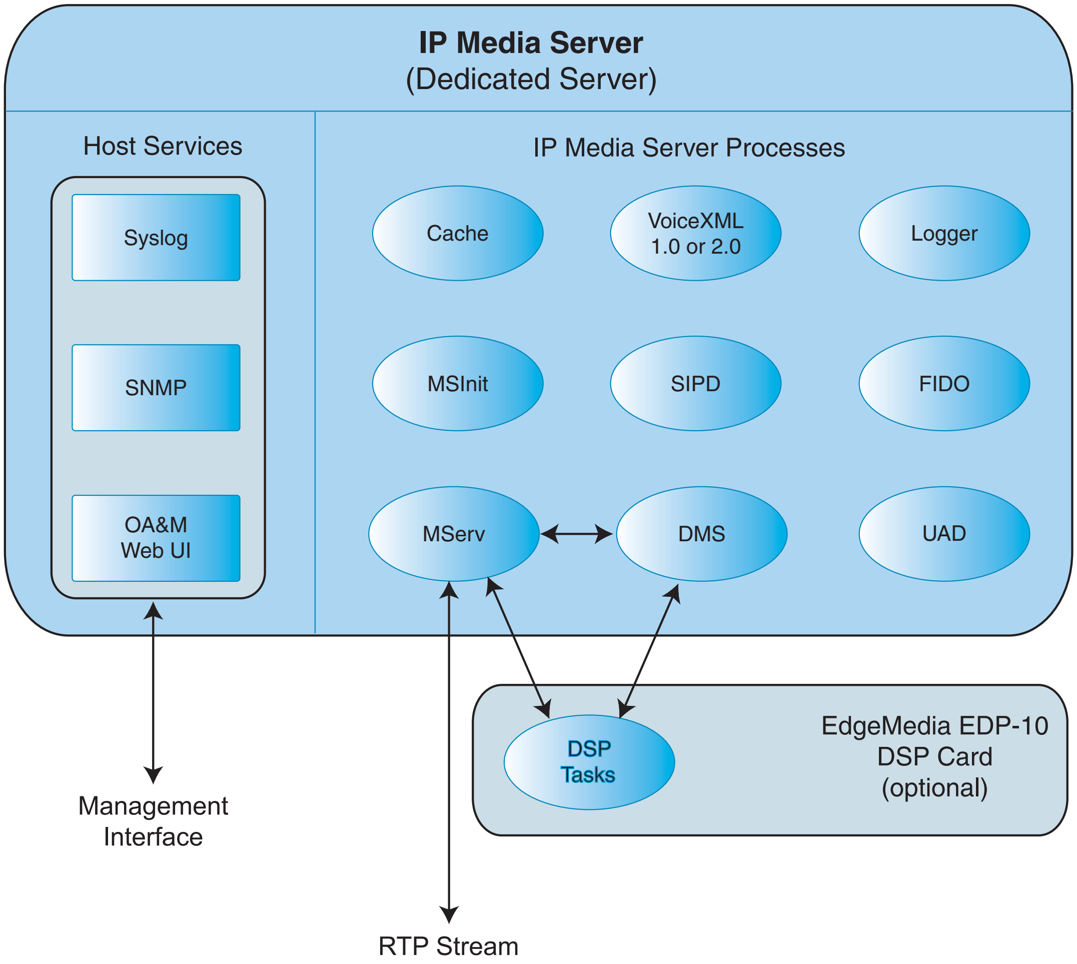


Figure 2. IP Media Server Components

The IP Media Server components are described in the following sections.

DMS

DMS (DSP Management Service) manages requests from MServ for DSP resources when the optional DSP processor is available. The EdgeMedia EDP-10 DSP card is required for processing advanced codes such as AMR.

FIDO

FIDO (Fetcher of Internet Domain Objects) is an HTTP/HTTPS client used to retrieve prompts and VoiceXML scripts and to post recordings and VoiceXML results.

Cache

The cache component is an HTTP caching proxy server used by other processes that retrieve content using the HTTP and HTTPS protocols.

MRCP

MRCP is the component responsible for ASR and TTS communication with a Nuance MRCP server. MRCP is responsible for managing MRCP IPMS licenses.

MServ

The MServ process is responsible for all RTP processing and the handling of audio and video media (e.g., conference mixing, playing prompts, etc.).

MSInit

This component tracks and logs initialization of other IP Media Server components.

MSProvider

This process handles licensing services on the IP Media Server.

SIPD

SIPD processes SIP requests received by the IP Media Server.

SNMPDaemon

The SNMPDaemon process handles SNMP traps and activities on the IP Media Server.

UAD

The User Agent Daemon (UAD) generates outbound SIP requests and is used in conjunction with the VoiceXML <transfer> tag.

VXML 1.0 and VXML 2.0

The IP Media Server provides VoiceXML 1.0, and VoiceXML 2.0, compliant browsers. VoiceXML browsers interpret and execute VoiceXML scripts generated by applications.

When VXML 1.0 is enabled on the IP Media Server, the VXMLD process runs. When VXML 2.0 is enabled on the IP Media Server, multiple processes are invoked.

IP Media Server Components and Related Logs

Table 1 lists components that run on the IP Media Server, and the log file(s) associated with each component. The information contained in the logs is useful to troubleshooting issues that may be encountered during application development and deployment. Tracing a call through the logs also can help one to become familiar with the detailed operation of the IP Media Server. All of the logs are stored in the directory `/var/snowshore/logs`.

Table 1. IP Media Server Components and Related Logs

IP Media Server Components	Related Log Files
Cache	cache_access.log
DMS	dms.log
Email to Fax	email_to_fax.log
FIDO	fido.log
HTTP	cache.log
MServ	mserv.log
MRCP	MrcpClientLibrary.log
MSInit	msinit.log
MSProvider	msprovider.log
Recoveryd (VXML 1.0)	recoveryd.log
SIPD	sipd.log
SNMPDaemon	snmpdaemon.log
SR140	sr140app.log
Syslog	messages.log
UAD	uad.log
VXML 1.0	vxmld.log
VXML 2.0	vxml2d.log
Web UI	audit.log
Clear Text Accounting	accounting.log
Encrypted Log	msaccounting.log

Supported Applications

The Dialogic® IP Media Server supports the various application services including the following:

- Network Announcements
- Conferencing
- IVR
- VoiceXML

SIP Implementation

All application services are implemented through the Session Initiation Protocol (SIP) protocol and optional XML-based directives. The SIP Request-URI indicates the service to receive a request.

Service Indicator

The Dialogic® IP Media Server takes advantage of the fact that the SIP standard has a ‘user’ component on the left-hand side of the Uniform Resource Identifier (URI) and that the IP Media Server does not have ‘users’.

The Dialogic® IP Media Server employs the user address portion of the Request-URI as a service indicator, which can take any of the values listed in Table 2.

If no service indicator appears in the SIP message, the default application is VoiceXML (the `dialog` service indicator). This default application can be changed through the web interface by selecting the MEDIA SERVER > SIP menu and setting the Default Application under the SIP Parameters section. The default version of VXML is 2.0. This is configured by selecting the MEDIA SERVER > VOICEXML menu.

Table 2. Application Service Indicators

Service	Service Indicator	Example[a]
Announcements	annc	`INVITE sip:`**annc**`@MS_IP; play=(etc.) SIP/2.0`
Conferencing	conf	`INVITE sip:`**conf**`=confid@MS_IP SIP/2.0`
IVR	ivr	`INFO sip:`**ivr**`@MS_IP SIP/2.0`
VoiceXML	dialog	`INVITE sip:`**dialog**`@MS_IP; voicexml=http://path/ filename.vxml SIP/2.0`

[a] The Service Indicators are shown in bold text in the Example column of this table.

Media Content and Processing by Applications

For all services, the IP Media Server generates RTP voice packets encoded as G.711 (a-law and μ-law), G.726, G.729, or AMR-NB.

Note: RTP encoding is established through SDP negotiation of the media description (which is done using the attribute 'm=').

The announcement and IVR services can retrieve and play files with content encoded in the following formats:

Table 3. Supported Announcement and IVR File Encodings

Service	Encoded Format	File Format
announcement and IVR services	G.711	*.ulaw, *.alaw, *.au, and *.wav
announcement and IVR services	MSGSM	*.msgsm or *.ms_gsm

Table 3. Supported Announcement and IVR File Encodings (Continued)

Service	Encoded Format	File Format
IVR service	G.711 a-law or µ-law MSGSM	*.au, *.wav
Video	H.263, H.263+, H.264	*.3gp, *.3gpp, *.wav
All services	Convert to RTP stream encoded as G.711 a-law or µ-law	Retrieve an audio file encoded as G.711a-law or µ-law or MSGSM

All services can retrieve an audio file encoded as G.711a-law or µ-law or MSGSM and convert it to an RTP stream encoded as either G.711 a-law or µ-law.

Note: Audio data format and content encoding are specified in the file header and through the prompt encoding parameter in the MSCML interface. If the file format is unknown or unspecified, the IP Media Server assumes headerless µ-law.

The announcement and IVR services can retrieve audio files anywhere they are accessible by the IP Media Server. Files can be in either the file://// scheme retrieved by NFS or the http:// scheme retrieved by HTTP (version 1.0 or version 1.1).

NFS mount points are automounted.

2 - Installing the Media Server

The Dialogic® IP Media Server is distributed in two forms:

- An integrated server, including a hardware platform and preinstalled IP Media Server software.
- A software-only release for installation on an existing hardware platform.

This chapter explains how to install and configure the IP Media Server and includes the following sections:

- Installing the Integrated IP Media Server
- Installing the Integrated IP Media Server
- Installing IP Media Server Software
- Configuring a Management Interface

Note: The Dialogic® IP Media Server is suitable for use as a dedicated telephony media server. Other software applications installed on the IP Media Server may adversely affect its performance.

Installing the Integrated IP Media Server

This section provides information for installing the integrated IP Media Server. The IP Media Server is also available as a software-only release that can be installed on a wide range of supported hardware platforms. Installing the software-only version is described in *“Installing IP Media Server Software” (page 38)*.

Description

The integrated IP Media Server is delivered as a 1U system based on the Intel TIGW1U chassis with the IP Media Server software already installed. The operating system is Red Hat Enterprise Linux with support for versions ES 4.0 Update 5 and 5.0 Update 1.

Refer to the Intel web site for details about the Intel TIGW1U chassis.

The IP Media Server Release Notes list other supported hardware platforms.

Optional Components

The integrated IP Media Server is available with the following optional component:

◆ EDP-10 The EdgeMedia EDP-10 is a DSP processor card. This card is for processing G.726, G.729, and AMR-NB codecs. This is a factory-installed option, not a field-upgradable option. (The G.726 and G.729 codecs can also be host-based. Refer to *Host-Based Codecs* in the *Application Developer’s Guide*.

Warning: Although your IP Media Server may have open disk drive bays, these must not be upgraded with field-installed drives.

Specifications

The following table provides specifications for the integrated IP Media Server.

Table 4. Integrated IP Media Server Specifications

Processor	Dual Intel Xeon Processors @ 2.8 GHz
Hard Disk	Single 70GB
Ethernet	Two 1Gb Ethernet Ports (eth0, eth1)

Table 4. Integrated IP Media Server Specifications (Continued)

PCI Slot: full-height low-profile	 1 1
Memory	2GB
Power	Single or dual 520W power supplies AC Voltage: 100–127 / 200–240 V~; 6.5 / 3.2A
Weight	~28 / 35 lbs.
Dimensions	Height 1.7", Width 16.93", Depth 26.46" (43 mm x 430 mm x 672 mm)
Temperature: Operating Non-operating	 +50°F to +95°F (+10°C to +35°C) –40°F to +158°F (–40°C to +70°C)
Humidity: Non-operating	90% (non-condensing) @ +30°C
Cooling Requirements	2322 BTU/hour (based on 520W maximum power, 78% power subsystem efficiency, and 98% power factory correction loss)
EDP-10 (Optional)	EdgeMedia DSP card for AMR-NB, G.726 and G.727 Codec Support (LED Indicators: On, Active, Transmit, Receive)

Before Installing the IP Media Server

Preparing the Site

Before you install the IP Media Server, make sure the operating environment meets the physical specifications for humidity and temperature described in Table 4 (page 33).

Choose a location where the IP Media Server and all devices that connect to it can be in close proximity to each other and to an electrical outlet. For more information, see the *Quick Install Guide* that came with your IP Media Server.

Checking the Package Contents

The integrated IP Media Server shipment comes in a single box. Unpack it, verifying that you have received the following items:

- The IP Media Server chassis
- A front bezel (which must be installed)

- A North American AC power cord
  (not NEBS [Network Equipment Building System])
- A documentation package containing Release Notes, a license, and a CD containing electronic versions of the user documentation
- A serial cable kit
- An additional box (below chassis) that contains a bracket kit and installation guide

Tools and Supplies

To install the IP Media Server, you need:

- A Phillips-head screwdriver for mounting the chassis to the rack
- Cables for the RJ45 NIC interfaces
- For the Management Interface configuration, you need either a PC/laptop with a terminal emulation program or a terminal server. Both require use of the included serial cable kit. You can optionally use a keyboard, monitor, or mouse connected directly to the appropriate connectors on the IP Media Server.

Hardware Installation

The integrated version of the IP Media Server is shipped as a user-installable device. It is recommended that the system be powered using a UPS system for reliability and protection from power fluctuations.

Rack Mounting

The integrated version of the IP Media Server can be mounted in any standard rack.The IP Media Server comes with sliding rails and a set of fixed rails for mounting in rack-mount systems. The configuration of your racks may dictate which rails you are able to use. Refer to the installation instructions provided with the rails for more information.

Cabling

Connect all cables to the connectors on the back of the chassis. For the standard Dialogic® IP Media Server , there are two 1Gb Ethernet ports and a serial connector as shown in Figure 3.

Connect the serial port to a terminal server for emergency access to the system or for initial setup.

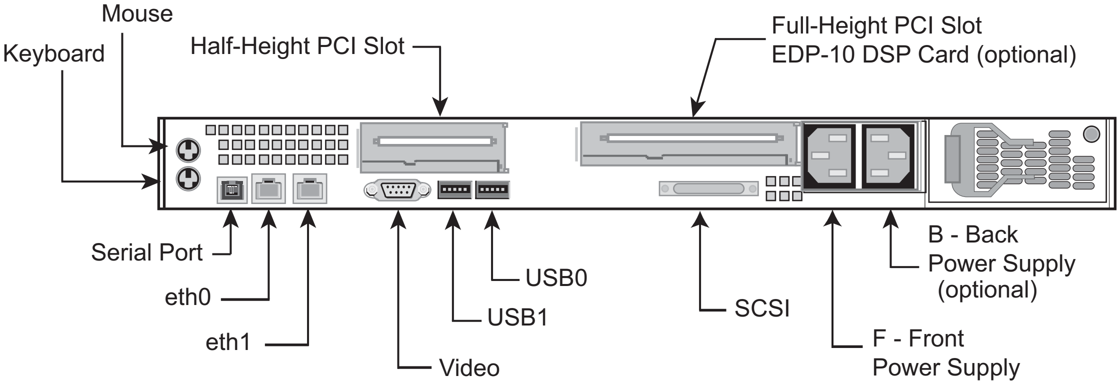


Figure 3. Rear View of the IP Media Server Chassis

Front Panel

The front panel of the integrated IP Media Server is shown below. Each of the front panel features is described in Table 5

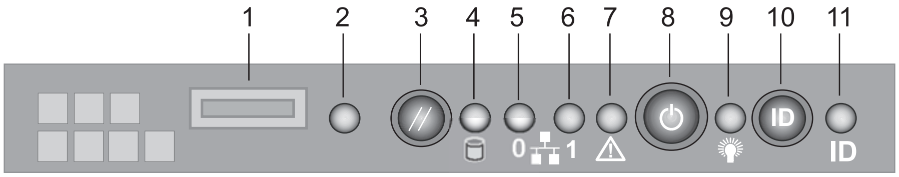


Figure 4. IP Media Server Front Panel

Table 5. Front Panel Features and Functions

Item	Feature	Function
1	USB 2.0 port	Allows you to attach a USB component to the front of the chassis.
2	NMI button	Puts the server in a halt-state for diagnostic purposes.
3	Reset button	Reboots and initializes the system.
4	Hard disk drive activity LED	Random blinking green light indicates hard disk drive activity (SCSI). No light indicates no hard disk drive activity.
5	NIC 0 activity LED	Blinking green light indicates network activity. Continuous green light indicates a link between the system and the network to which it is connected.

Table 5. Front Panel Features and Functions (Continued)

Item	Feature	Function
6	NIC 1 activity LED	Blinking green light indicates network activity. Continuous green light indicates a link between the system and the network to which it is connected.
7	System Status LED	Solid green indicates normal operation. Blinking green indicates degraded performance. Solid amber indicates a critical or non-recoverable condition. Blinking amber indicates a non-critical condition. No light indicates POST is running or the system is off.
8	Power/Sleep button	Toggles the system power on/off. Sleep button for ACPI-compatible operating systems.
9	Power/Sleep LED	Continuous green light indicates the system has power applied to it. Blinking green indicates the system is in S1 sleep state. No light indicates the power is off / is in ACPI S4 or S5 state.
10	System identification button	Illuminates the front panel ID LED and the server board ID LED for 15 seconds.
11	System Identification LED	Solid or blinking blue indicates system identification is active. No light indicates system identification is not activated. **Note:** The server board LED is visible from the rear of the chassis and allows you to locate the server from the rear of a rack of systems.

Installing IP Media Server Software

This section provides instructions for installing the IP Media Server software on a server that will act as a dedicated IP Media Server platform. The server hardware must meet the minimum system requirements defined below.

Operating System Requirements

IP Media Server Release 2.5.0 can be installed on systems running Red Hat Enterprise Linux ES 4.0 Update 5 or ES 5.0 Update 1.

Server Hardware Requirements

The server on which you install the IP Media Server software must meet the minimum requirements listed in Table 6.

Table 6. Minimum Server Hardware Requirements

Item	Requirement
Processor	Two 64-bit Intel Xeon Processors running at no less than 2.8 GHz, 800 MHz front side bus, 2 MB L2 cache
Memory	2 GB ECC DDR-2 SDRAM
Ethernet	Dual 1000baseT Gigabit Ethernet
Disk	At least 30 GB Ultra320 SCSI 10000 RPM hard drive
DSP Card - Optional (Required for G.726, G.729ab, and AMR-NB processing)	EdgeMedia EDP-10 DSP card

⚠ **Note:** The IP Media Server is suitable for use as a dedicated telephony media server. Other software applications installed on the same physical device that is configured as the IP Media Server may adversely affect the performance of the IP Media Server.

Installing the IP Media Server 2.5.0 Software

This section provides instructions for installing the IP Media Server software on a system that has Red Hat Enterprise Linux installed.

Note: For information on installing and configuring Red Hat, see the Red Hat documentation and the Dialogic Technical Note *Installing Red Hat Enterprise Linux 4.0 for the Dialogic® IP Media Server* and *Installing Red Hat Enterprise Linux 5.0 for the Dialogic® IP Media Server .*

⚠ **Note:** Before installing the IP Media Server software on the Red Hat operating system, you must disable SELinux. This is done automatically by the kickstart script in the Dialogic Technical Note *Red Hat 4.0 and MS 2.5* and *Red Hat 5.0 and MS 2.5*. You can also disable SELinux by editing the file `/etc/sysconfig/selinux` by changing the selinux line to `SELINUX=disabled` and rebooting the system.

After installing Red Hat Enterprise Linux on your system, insert the IP Media Server CD-ROM (IP Media Server software only for Red Hat ES 4.0 CD or for Red Hat Server 5.0 CD) into the drive.

1 Mount the CD-ROM on your system:

```
mount  /dev/hda  /media/cdrom
```

Note: This command may vary depending on the device names in your system.

2 Make a temporary installation directory on your system:

```
mkdir /tmp/install_1
```

3 Copy the contents of the CD-ROM to your temporary installation directory:

```
cp /media/cdrom/* /tmp/install_1
```

4 Change directory to install_1:

```
cd /tmp/install_1
```

5 Unzip the tar.gz file:

```
gunzip –d SNOW*.gz
```

6 Untar the compressed tar file:

```
tar –xvf SNOW*.tar
```

7 Install the Snowshore RPMs:

```
rpm –ivh SNOW*.rpm
```

8 Run the ms_install script:

```
./ms_install
```

A series of messages appears on the system monitor as the script installs the IP Media Server software.

9 When the installation script ends, unmount the CD drive:

```
unmount /media/cdrom
```

10 Remove the temporary installation directory:

```
cd /tmp
rm –rf /tmp/install_1
```

11 Reboot the system (this should take approximately 5 minutes):

```
reboot
```

Refer to “Configuring a Management Interface” (page 41) for information about configuring a management interface on the IP Media Server. You use the management interface to configure and administer the system.

Running the G2Check Utility to Check the Installation

The IP Media Server CD-ROM contains the G2Check utility that you can run to ensure that the Media Server Installation was successful.

1 Copy the G2Check utility to the install_1 directory.

2 Run the G2Check utility:

```
root@snow-sip snowshore]# perl G2Check
```

3 Respond to the prompts.

4 When the utility is done, it prints the results to STDOUT and the details to G2Install.log.

Configuring a Management Interface

The system is configured by default to run DHCP on the Ethernet interfaces (eth0, eth1, and optional eth2). If you use DHCP to set the IP address of an interface and you know the IP address, then you can use the Web User Interface (Web UI) immediately.

If you do not know the IP address configured on the system, or to set an IP address for the first time, access the system with a monitor and keyboard or over the serial port. Connect to the serial port using any standard terminal interface.

The serial port on the IP Media Server is configured as:

- Rate: autosense 9600 baud (press enter several times to autosense)
- Bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

Logging In

When a connection to the IP Media Server is established, the login prompt appears. The IP Media Server is delivered with a single Administrator access level user defined in the system. The login prompt appears as follows:

{hostname} login:

Use “admin” as the user name to log in through the serial port or through the console.

Navigating through the Web User Interface

Use the keyboard to navigate through the interface. The navigation keys are:

Table 7. Navigation Keys

Navigation Key	Description
Tab, up and down arrows	Navigate through the fields in the display.
Right arrow	Select an option.
Enter	To apply, cancel, or reboot.
H	To access help.

➢ To view the interface configuration:

- Select the Interface Configuration command.

➢ To change the IP address of an interface:

1. Select the interface to be configured.
2. Tab or mouse over to the IP address field.
3. Enter an IP address.
4. Enter network mask.
5. Note the IP address and apply the change.

Note: Specify an IP address for each interface.

The next page displayed is the original page you saw when you logged in.

◆ Tab to the **REBOOT** option and press **ENTER**.

The host reboots and the interface comes up with the specified address.

All further configuration is done through the Web User Interface.

The Web User Interface arrives configured to use HTTP. If HTTPS is preferred, you can install a security certificate and key on the system using the Web User Interface. You can also install a certificate and key using the command options provided over the serial port or monitor/keyboard. Refer to “Managing Certificates” (page 137) for information on how to install a certificate.

License Activation

Note: License activation applies only to IP Media Servers running Red Hat Enterprise Linux Server operating systems.

The IP Media Server has limited functionality unless you activate licenses. The primary method of activation is interactive through use of the Web. To activate your license, you must have the following:

- Access to the license key from the License Certificate or via an email from Dialogic.
- Access to the IP Media Server Web User Interface to obtain your Node ID.
- Access to the Dialogic Web site from a system with a Web browser and Internet access.
- Access to a local FTP or NFS server.

For detailed information and instructions on activating the license, refer to the *License Activation Guide*.

3 - Using the Web User Interface (Web UI)

This chapter explains how to use the Web User Interface (Web UI). It includes the following sections:

- Overview
- Navigating the Web User Interface (UI)

Overview

The Dialogic® IP Media Server is configured using a standard Web browser. Internet Explorer 6.0 or Netscape 7 or higher is recommended.

Web UI Access Levels

The IP Media Server supports two access levels:

- Administrator—Can change the configuration of the system and execute administrative tasks.
- Operator—Can monitor the system, but cannot change configurations or execute administrative tasks.

Commands that are only available to Administrators are noted as such. All other commands are usable by both operators and administrators.

Note: You must be an Administrator to configure the system.

These two levels and the privileges associated with each are described in detail in Chapter 5, “Operations, Administration, and Maintenance”. The IP Media Server comes with a default Administrator user account. The user name and password of this account are:

User Name: admin

Password: <blank>

User names and passwords are case sensitive.

⚠ **Note:** You should immediately change your password after initial login; see “Changing Administrator Password” (page 131).

Logging In

To open the Web User Interface:

1 Start your Web browser.

2 Enter the fully qualified domain name or IP address (for either eth0 or eth1) of the system in the address field of your browser; for example:

```
https://<your IP address>
```

This displays the Login page.

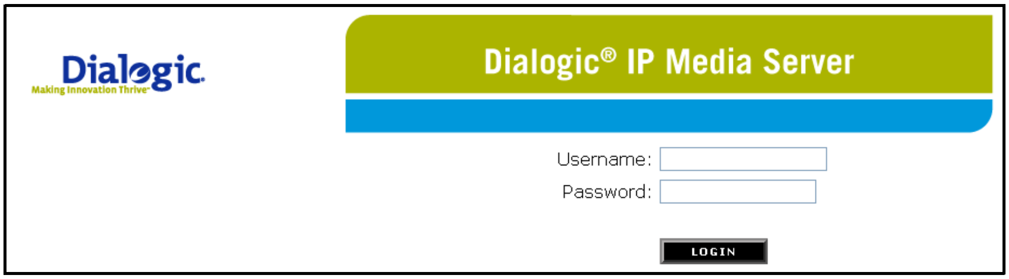
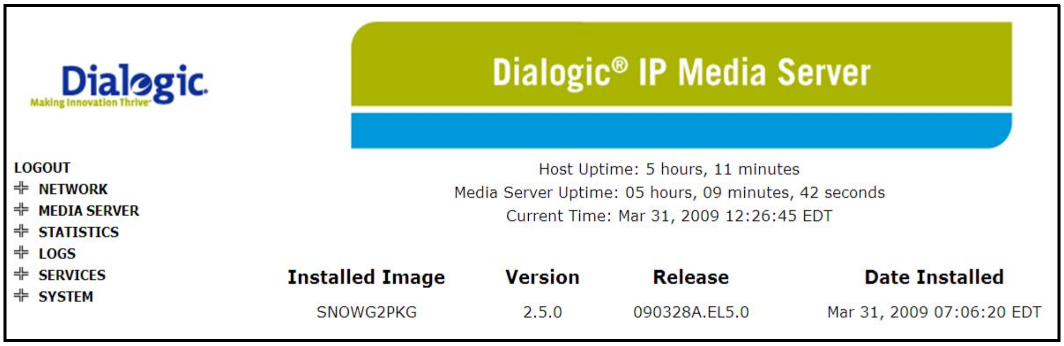


Figure 5. Login page

3 To log in, enter your user name and password, then click LOGIN. This displays the Web UI home page.

Web UI Home Page



Host Uptime: 5 hours, 11 minutes
Media Server Uptime: 05 hours, 09 minutes, 42 seconds
Current Time: Mar 31, 2009 12:26:45 EDT

Installed Image	Version	Release	Date Installed
SNOWG2PKG	2.5.0	090328A.EL5.0	Mar 31, 2009 07:06:20 EDT

Figure 6. Web UI: Home Page

The Web UI page has three sections:

- The page title at the top.
- A menu frame to the left for navigation.
- A display frame to the right for viewing and changing data.

The display frame of the home page contains the following information about the IP Media Server you have logged into:

Item	Description
Host Uptime	How long the IP Media Server host has been running.
Media Server Uptime	How long the IP Media Server software has been running.
Current Time	The current time.

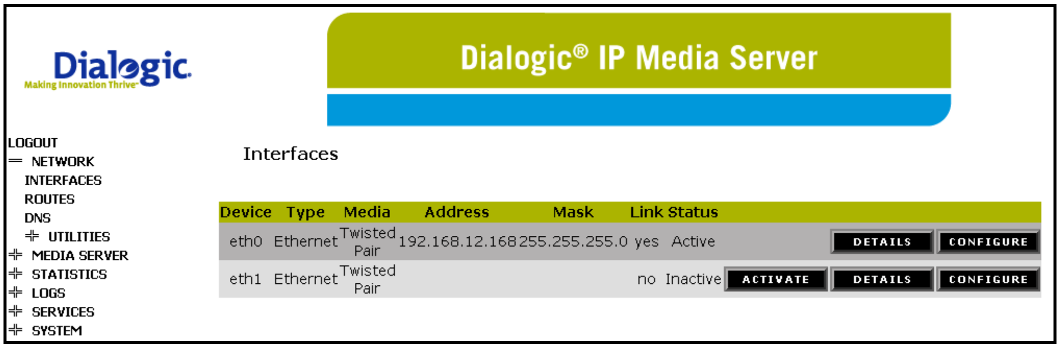
Item	Description
Installed Images	Information about the IP Media Server VXML interpreter images: ◆ Image name ◆ Image version ◆ Image release number ◆ Date Installed

Navigating the Web User Interface (UI)

This section describes how to use the Web UI to view and change data and perform commands. Under the page title, the Web UI has a menu frame for navigation and a display frame for viewing and changing data.

The left hand frame contains a hierarchical menu system. If a menu item has submenus, a “+” sign appears to the left of the menu text. To expand a menu item with a “+” sign to its left and display the submenus, select the menu item. If the menu item is expanded, a “-” sign appears beside the expanded menu name. If neither a “+” or “-” sign appears to the left of the menu text, the item is a command. Select the menu item to execute the command.

The display frame shows the results for the first item in the expanded menu set, as in the example in Figure 7.



Interfaces

Device	Type	Media	Address	Mask	Link Status				
eth0	Ethernet	Twisted Pair	192.168.12.168	255.255.255.0	yes	Active		DETAILS	CONFIGURE
eth1	Ethernet	Twisted Pair			no	Inactive	ACTIVATE	DETAILS	CONFIGURE

Figure 7. Menu and Display Frames in the Web User Interface

Examples are:

- The LOGOUT menu item is a command. Select LOGOUT to log out.
- The NETWORK menu has been expanded in Figure 7. The NETWORK menu contains the INTERFACES command and a sub menu for UTILITIES. The sub menu UTILITIES contains further commands. When the NETWORK menu item is expanded, the INTERFACES command is executed automatically, and displays the data for the interfaces in the display frame.

At any time, you can select another menu item in the left hand frame. This action leaves the current command and goes to the one selected. Many of the displays also have a BACK button located in the display area. To return to the previous display, click this button. You can also use the browser forward and back arrows.

Note: To return to the previous menu, click Back.

4 - Configuring the Dialogic® IP Media Server

This chapter describes procedures for configuring the IP Media Server for operation, and includes the following sections:

- Configuration Checklist
- Network Configuration
- Configuring SIP and SDP
- Configuring VoiceXML
- Configuring Fax
- Halt Active Calls
- Shutdown Calls

The Ethernet interfaces and routing table in the IP Media Server must be configured to enable the operation of the IP Media Server. The IP Media Server requires an interface to be designated for RTP traffic and one for SIP traffic. When IP addresses, routes and designated interfaces for SIP and RTP have been established, the IP Media Server is ready to be brought up in its default configuration and to process calls.

Configuration Checklist

⚠ **Note:** Before changing the configuration of a running system, always back up the current configuration using the SYSTEM→CONFIG FILES→CREATE BACKUP command.

The following checklist summarizes the minimum configuration steps required to get the IP Media Server up and running.

1. Configure the Network Interfaces (Network→Interfaces: Configure button):
   - Assign IP addresses.
   - Select an interface to be used for RTP traffic.
   - Select an interface to be used as the SIP contact address.
   - Add routes to the interfaces (Network and Routes).
2. Check the IP Media Server default parameter settings:
   - Check SIP and SDP settings (Media Server→SIP).
   - Check VoiceXML settings (Media Server→VoiceXML).
3. Reboot the host to ensure all configuration changes take effect:
   - System→Reboot Host
4. Test the interfaces:
   - From another system, ping the IP address of each interface.
   - From the IP Media Server, use the Network→Utilities→Ping command to verify that the IP Media Server can access the network.

After these configuration steps have been done, the IP Media Server can accept calls.

The following sections give details on all of the IP Media Server configuration menus and commands.

System Files Updated

Dialogic recommends using the Web UI (administrator access level) to configure the IP Media Server. The following system files are updated during configuration.

- `/etc/hosts` (snow-sip and snow-rtp get added)
- `/etc/resolve.conf` (DNS servers)
- `/etc/ntp.conf` and `/etc/ntp/step-tickers` (NTP servers)
- `/etc/sysconfig/network-scripts/ifcfg-eth(x)` (interface configuration settings)

If you create routes on the Media Server:

- `/etc/sysconfig/network-scripts/route-eth(x)`
- `/opt/snowshore/etc/snmp.conf` and `/etc/snmp/snmp.conf` (snmp)

You can manually update these files, but be careful because if you manually update a parameter and later change the parameter using the Web UI, you can create a conflict.

Network Configuration

The NETWORK menu provides commands for configuring and activating the Ethernet interfaces on the IP Media Server and for configuring routing and DNS information.

Overview of IP Media Server Ethernet Interfaces

The IP Media Server has two Ethernet interfaces by default, eth0 and eth1.

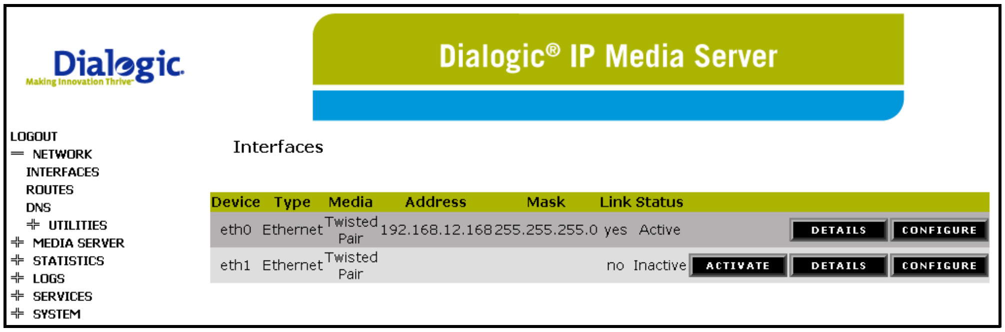
- eth0 is typically connected to a DHCP server and acquires its address via DHCP. This port is used for management and configuration access via the Web UI.
- eth1 is typically configured with a static address dedicated to SIP and RTP traffic.

Configuring Interfaces

There are two default interfaces on the IP Media Server, eth0 and eth1. To configure an interface:

1 Select INTERFACES.

The Interfaces page appears:



Interfaces

Device	Type	Media	Address	Mask	Link	Status
eth0	Ethernet	Twisted Pair	192.168.12.168	255.255.255.0	yes	Active
eth1	Ethernet	Twisted Pair			no	Inactive

Figure 8. Interfaces Page

The Interfaces page shows the following information:

Item	Description
Device	Device name
Type	Type of the interface: Ethernet
Media	Type of media: normally twisted pair
Address	Current IP address of the IP Media Server host
Mask	Network mask associated with this interface

Item	Description
Link	Whether the interface is linked
Status	Status of the interface. The status can be: ◆ Active - the interface is up and running. ◆ Inactive - the interface is not running.

The Interfaces page also enables you to perform several actions on each interface:

- Change its status (toggle between Active and Inactive)
- View detailed information about it
- Configure it

Changing the Status of an Interface

Note: Only Administrators can change the status of an interface.

Each interface except eth0 has a DEACTIVATE or ACTIVATE button next to it, which enables you to change its status.

- To activate an inactive interface, click ACTIVATE.

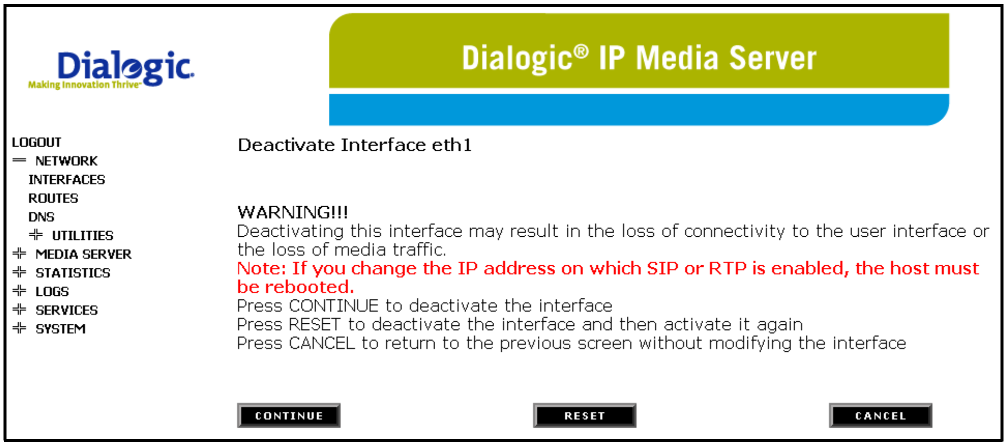
  The interface comes up with the configuration stored in the configuration file.

- To deactivate an active interface, click DEACTIVATE.

  This action stops all traffic using that interface.

  Note: You cannot deactivate the interface eth0, because there must always be an interface available for the Web User Interface.

  When you click DEACTIVATE, a warning page appears.



Deactivate Interface eth1

WARNING!!!
Deactivating this interface may result in the loss of connectivity to the user interface or the loss of media traffic.
Note: If you change the IP address on which SIP or RTP is enabled, the host must be rebooted.
Press CONTINUE to deactivate the interface
Press RESET to deactivate the interface and then activate it again
Press CANCEL to return to the previous screen without modifying the interface

Figure 9. WARNING: Options on DEACTIVATE Interface Command

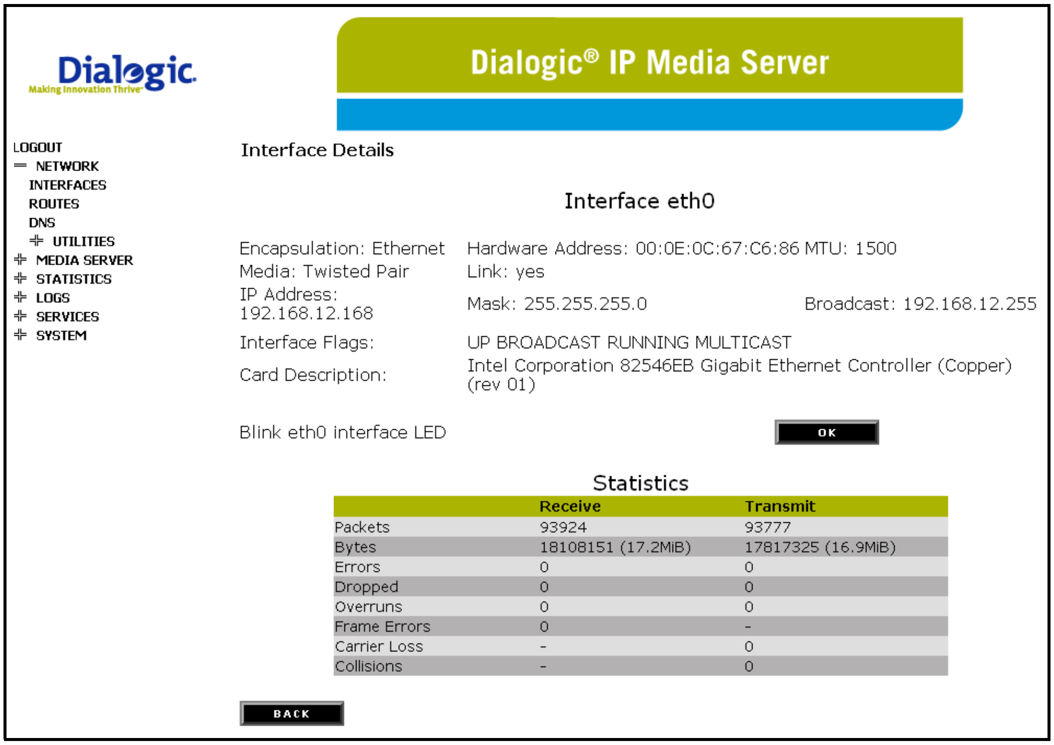
You have three options:

- CONTINUE with the deactivation.
- RESET the interface (take it down and bring it back up immediately).
- CANCEL the deactivation.

If you deactivate an interface, all traffic on that interface is dropped.

Interface Details

The DETAILS button for an interface displays the Interface Details page (Figure 10), which displays information about the running configuration of the interface and interface statistics.



Interface Details

Interface eth0

Encapsulation: Ethernet
Hardware Address: 00:0E:0C:67:C6:86 MTU: 1500
Media: Twisted Pair
Link: yes
IP Address: 192.168.12.168
Mask: 255.255.255.0
Broadcast: 192.168.12.255
Interface Flags: UP BROADCAST RUNNING MULTICAST
Card Description: Intel Corporation 82546EB Gigabit Ethernet Controller (Copper) (rev 01)

Blink eth0 interface LED

Statistics

	Receive	Transmit
Packets	93924	93777
Bytes	18108151 (17.2MiB)	17817325 (16.9MiB)
Errors	0	0
Dropped	0	0
Overruns	0	0
Frame Errors	0	-
Carrier Loss	-	0
Collisions	-	0

Figure 10. Interface Details Page

The configuration includes the following information:

Table 8. Interface Configuration

Item	Description
Encapsulation	Type of network connection (such as Ethernet).
Hardware Address	MAC address of the IP Media Server host.

Table 8. Interface Configuration (Continued)

Item	Description
MTU	Maximum Transmission Unit, the largest physical packet size, measured in bytes, that a network can carry. Ethernet has a fixed MTU of 1500 bytes.
Media	Type of media: normally twisted pair.
Link	Whether the interface is linked.
IP Address	Current IP address of the IP Media Server host.
Mask	Network mask associated with this interface.
Broadcast	Default route.
Interface Flags	Linux flags showing the current status of the interface.
Card Description	Type of hardware card for the interface.

Below the configuration parameters is a button Blink eth0 interface LED. Clicking this button lights the system LED (front and back) on the IP Media Server, so that you can identify it in a rack of equipment.

The interface statistics include statistics for all packets received at or sent from the host through the selected interface, including the numbers of the following:

- Packets
- Bytes
- Errors
- Dropped packets
- Overruns
- Frame errors
- Carrier losses
- Collisions

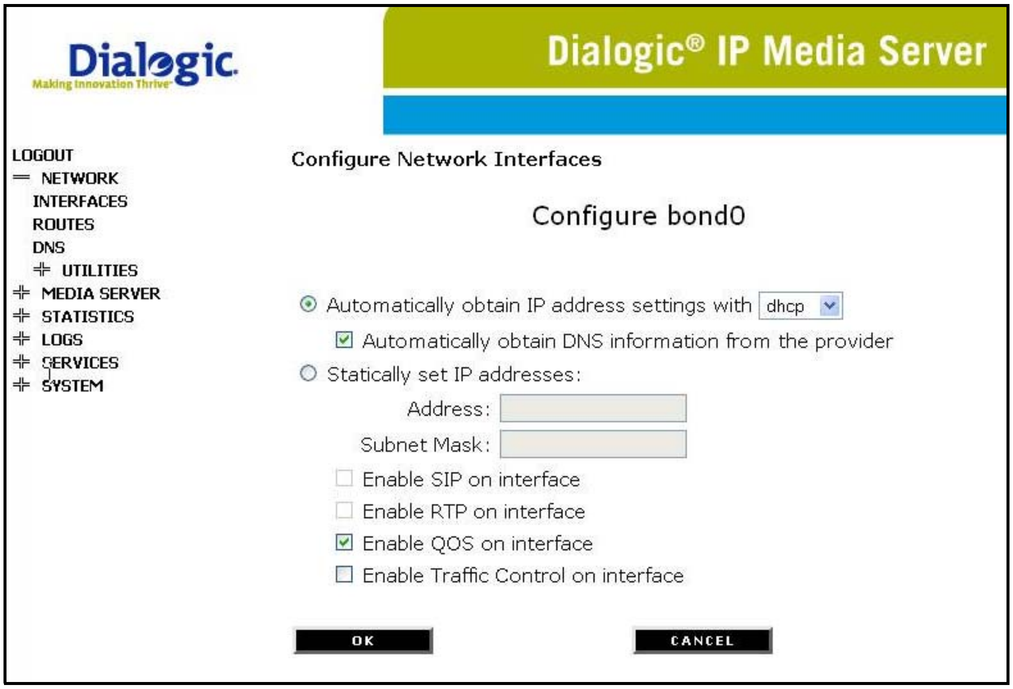
Interface Configuration

Note: Only Administrators can configure interfaces. All users can view the configuration.

To configure an interface:

Note: If you configure a bonded interface, such as bond1, to enable/disable STP and RTP on the interface, the settings apply only to the bonded interface. They do not change any existing settings on the physical interfaces that are combined in the bonded interface.

1 Click CONFIGURE for the interface you want to configure to display the Configure Network Interfaces page for that interface.



Configure Network Interfaces

Configure bond0

● Automatically obtain IP address settings with dhcp

☑ Automatically obtain DNS information from the provider

○ Statically set IP addresses:

Address:

Subnet Mask:

□ Enable SIP on interface

□ Enable RTP on interface

☑ Enable QOS on interface

□ Enable Traffic Control on interface

Figure 11. Configure Network Interfaces Page

When the Configure Network Interfaces page appears, it shows the current information stored in the configuration file. For an active interface, this information can be different from the running configuration shown in the Interfaces display.

The IP Media Server can be configured to use a particular interface for RTP traffic and for the SIP contact address. Only interfaces configured with static IP addresses can be enabled for RTP and SIP. If DHCP is used to set the address for an interface, that interface cannot be enabled for RTP and SIP.

If no interface has been enabled for RTP and SIP, the system tries to use the interface associated with the local host name. If a host name has not been assigned, this attempt fails and the IP Media Server cannot accept calls.

Note: A typical configuration uses DHCP to set the address for eth0 to be used for the Web UI. The second Ethernet interface, eth1, should have a static IP address and be used for RTP and SIP traffic.

2 To store the changes made, click OK. To cancel the changes, click CANCEL.

Accepting the configuration change updates the configuration file, but does not change the running configuration of an active interface:

- When you go back and display the interfaces, the running configuration is shown.
- When you return to the Configure page, the stored configuration is shown.

3 To apply a configuration change to an interface, reboot the IP Media Server.

Setting an IP Address for an Interface

Note: Only Administrators can set the IP address of an interface.

By default, the system has DHCP configured on eth0 and eth1. This allows the IP Media Server to automatically receive an IP address from a DHCP server (or from bootp). If the system is automatically obtaining an IP address, it can also obtain other DNS information, such as the network mask and hostname.

Note: If DHCP (or bootp) is used to set the IP address for an interface, you cannot enable that interface for RTP and SIP.

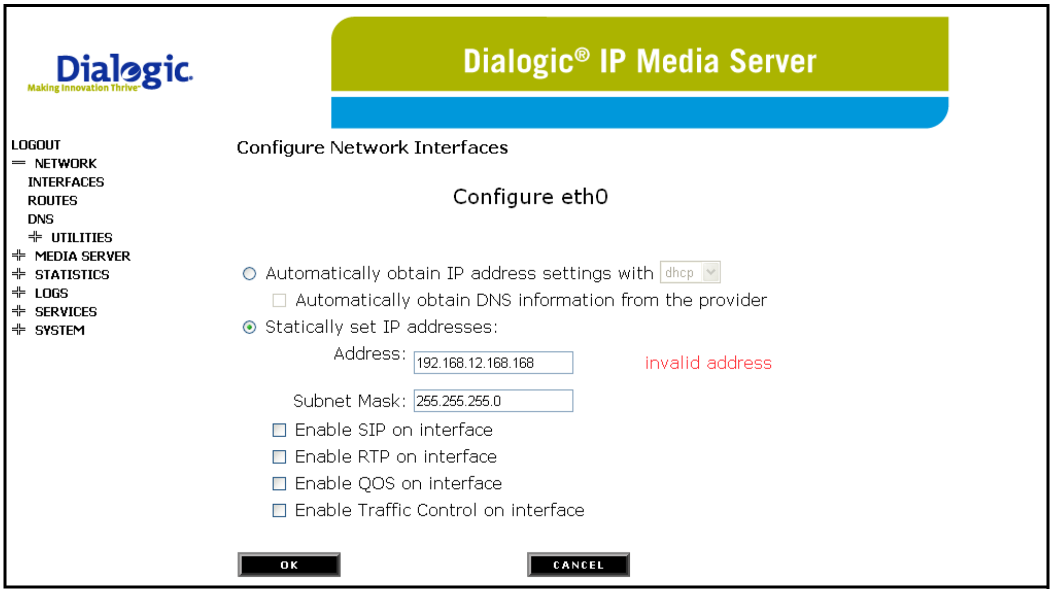
You can also set IP addresses and subnet masks statically. To do this:

1 Select Statically set IP addresses.

2 Enter an IP address and subnet mask in the Configure Network Interfaces page.

The system checks to ensure that the addresses entered are valid. If an invalid address is entered (for example, five octets instead of four), the system flags the error and does not accept the changes. The error appears in red beside the text field that has the violation. For example, in the case of a wrong IP address, the invalid address error appears in red beside the IP textbox.

3 After setting the static IP address, the Web UI will prompt you to reboot. After the reboot, you must then go into the DNS configuration and set the DNS settings since they are no longer receiving the data from DHCP. For more information, see “Configuring DNS” (page 64).



Configure Network Interfaces

Configure eth0

○ Automatically obtain IP address settings with dhcp

□ Automatically obtain DNS information from the provider

● Statically set IP addresses:

Address: 192.168.12.168.168 invalid address

Subnet Mask: 255.255.255.0

□ Enable SIP on interface

□ Enable RTP on interface

□ Enable QOS on interface

□ Enable Traffic Control on interface

Figure 12. Setting IP Address: Error Page

Enabling SIP and RTP on an Interface

You can configure the IP Media Server to use a particular interface for RTP traffic and for the SIP contact address. Only interfaces configured with static IP addresses can be enabled for RTP and SIP. You must enable both SIP and RTP on the same interface. Typically, eth0 is configured with DHCP for the management address, and eth1 is configured with a static address and with SIP and RTP enabled.

Enabling QOS and Traffic Control on an Interface

The IP Media Server supports Differentiated Services (DiffServ) as follows:

If you select Enable QOS on interface, the IP Media Server prioritizes outgoing traffic by injecting a QOS stamp in each UDP and HTTP packet. This way, other network devices know how to prioritize the packet for delivery.

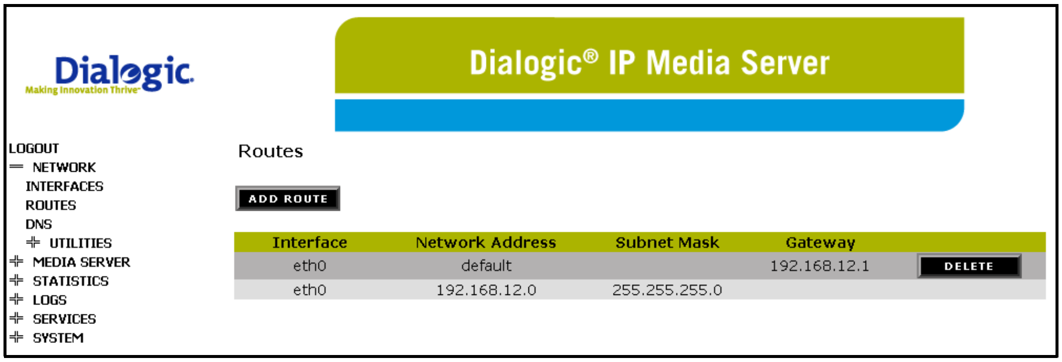
If you select Enable Traffic Control on interface, the IP Media Server filters incoming traffic. Incoming traffic that matches SIP, RTP, RTCP, and HTTP get priority over all other types of incoming traffic.

Note: Traffic Control is a system parameter and enabling/disabling it on an interface applies to all system interfaces.

Configuring Routes

Note: Only Administrators can add and delete routes. All users can display the routes.

The NETWORK→ROUTES menu displays the Routes page containing the routing table for eth0 and eth1.



Interface	Network Address	Subnet Mask	Gateway	
eth0	default		192.168.12.1	DELETE
eth0	192.168.12.0	255.255.255.0		

Figure 13. Routes Page

The routing table displays the following information for each route:

- Interface name
- Network address
- Subnet mask
- Gateway IP address

Routes that have been automatically added to the table are displayed, but they cannot be deleted. Only routes that have been added by users have a DELETE button and can be deleted. For example, in Figure 13, one route was added automatically by the system, and the other two routes were added by a user.

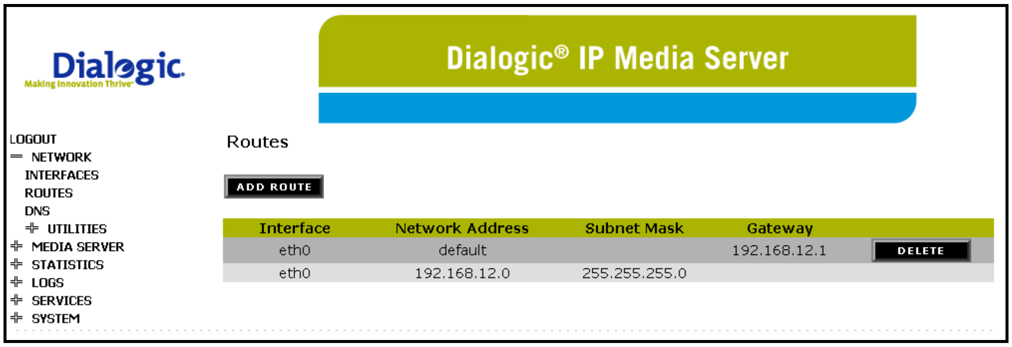
Note: Routes created by DHCP do not persist if the system is rebooted. To make a route persistent, when assigning a static IP address to the primary interface eth0, you must add it statically, even if it already appears in the list on the Routes page.
This is especially important for default routes. If you are accessing the IP Media Server from a different subnet, you must statically create a default route in order to be able to manage the system following a reboot.

Adding Routes

Note: Only Administrators can add routes.

To add a route to the system:

1 Click ADD ROUTE to display the Add Route page.



Interface	Network Address	Subnet Mask	Gateway
eth0	default		192.168.12.1
eth0	192.168.12.0	255.255.255.0	

Figure 14. Add Route Page

2 Select the interface from the drop-down menu.

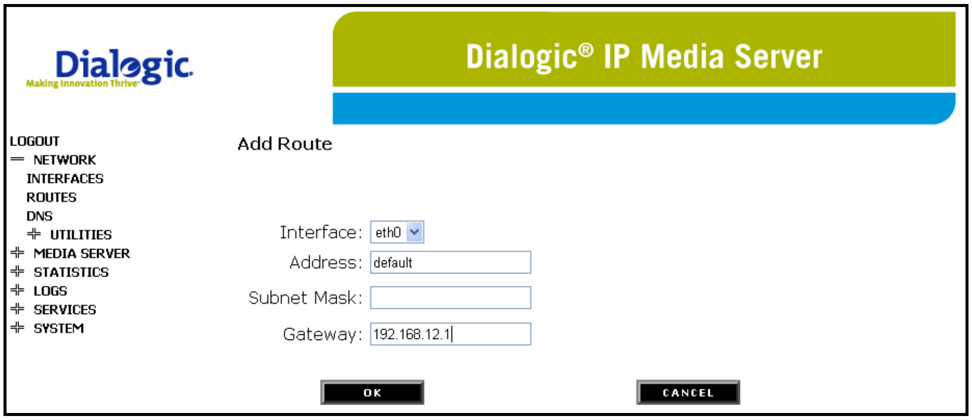
3 Enter the IP address and subnet mask; leave the Gateway field empty.

If this is a default route:

a. Type “default” in the IP address field.

b. Leave the Subnet Mask field empty.

c. Enter a gateway.

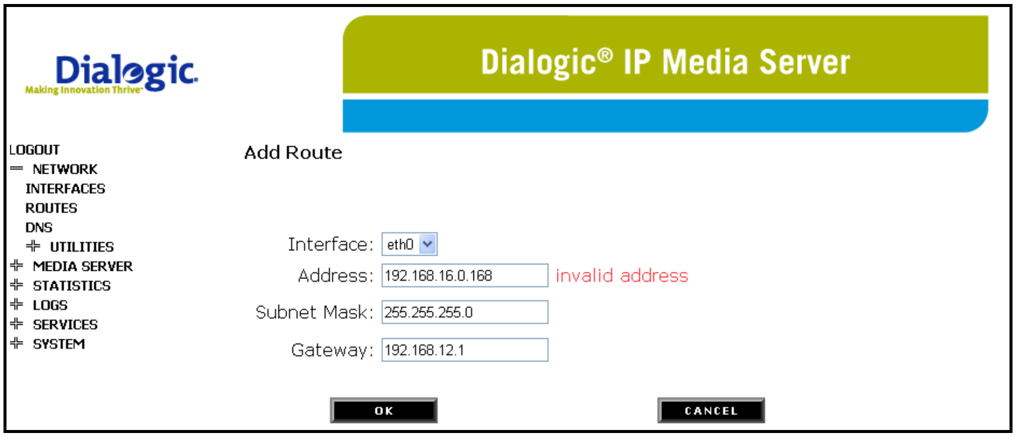


Interface: eth0
Address: default
Subnet Mask:
Gateway: 192.168.12.1

Figure 15. Add Default Route Page

4 If you do not want to add the route, click CANCEL. When you are satisfied that your entries are correct, click OK.

When the OK button is selected, the route entry is checked and added to the current routing table and to the configuration file. If the route entry has an error in it, an error message appears in red next to the text field where the error occurred (for example, Figure 16).



Add Route

Interface: eth0

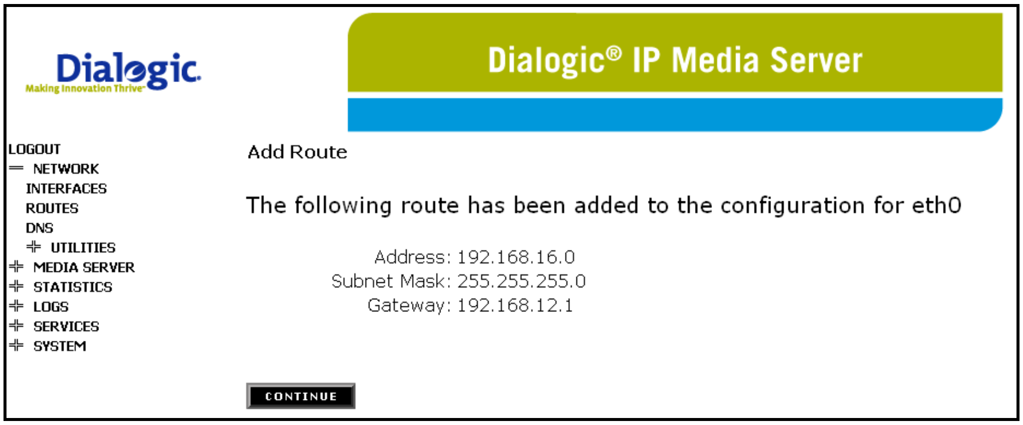
Address: 192.168.16.0.168 invalid address

Subnet Mask: 255.255.255.0

Gateway: 192.168.12.1

Figure 16. Add Route Error Page

A confirmation page is displayed.



Add Route

The following route has been added to the configuration for eth0

Address: 192.168.16.0
Subnet Mask: 255.255.255.0
Gateway: 192.168.12.1

Figure 17. Add Route Confirmation Page

Note: The example in Figure 17 indicates that the gateway specified is not reachable, although the IP address is valid.

5 Click CONTINUE to return to the routing table display.

Note: The system displays results of the route table update immediately after OK is selected.

Deleting Routes

Note: Only Administrators can delete routes. Also, only routes that have been manually added can be deleted.

To delete a route from the system:

1. Click DELETE next to the route that is to be deleted.
2. A confirmation page is displayed:
3. Click OK to delete the route.
4. Click CONTINUE to return to the Routes page.

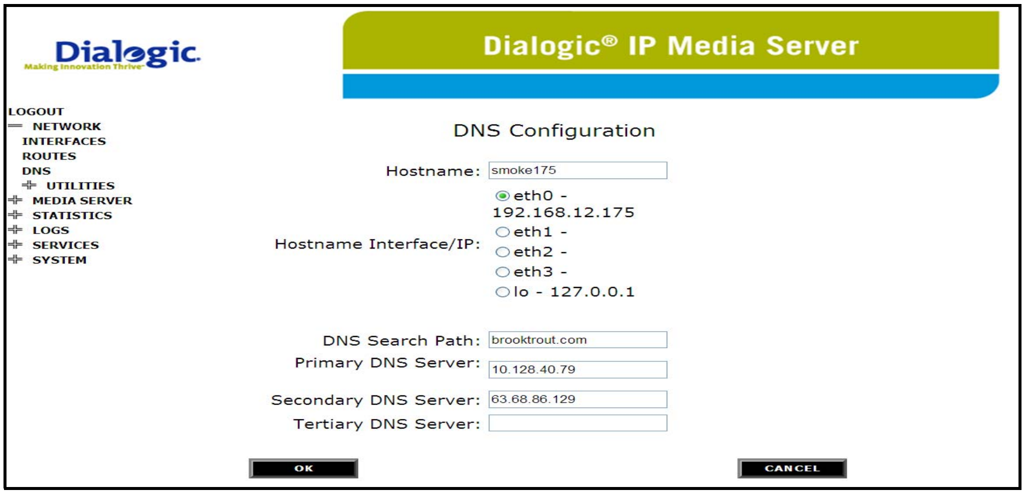
Configuring DNS

Note: Only Administrators can configure DNS. Both Administrators and Operators can display the DNS configuration.

You can configure up to three DNS servers by selecting NETWORK→DNS. The existing configuration appears and can be changed.

To configure DNS:

1 Select Network→DNS→DNS Configuration to display the DNS Configuration page.



DNS Configuration

Hostname: smoke175

Hostname Interface/IP:
● eth0 - 192.168.12.175
○ eth1 -
○ eth2 -
○ eth3 -
○ lo - 127.0.0.1

DNS Search Path: brooktrout.com

Primary DNS Server: 10.128.40.79

Secondary DNS Server: 63.68.86.129

Tertiary DNS Server:

Figure 18. DNS Configuration Page

2 You can change the fields on this screen.

3 To change the Hostname Interface/IP you first erase the Hostname and click OK. Then change the Hostname Interface IP. Click OK and retype the Hostname.

4 Click OK to save the changes. To cancel the changes without writing them to the configuration file, click CANCEL.

Note: The IP Media Server must be reset for these changes to take place.

Network Utilities

Use the Network Utilities to determine if access to the network exists.

Ping Utility

The Ping utility is a standard ICMP ping request. It sends out twelve 64-byte packets to the specified IP address.

To use the Ping Utility:

1 Select Network→Utilities→Ping to display the Network Ping page.

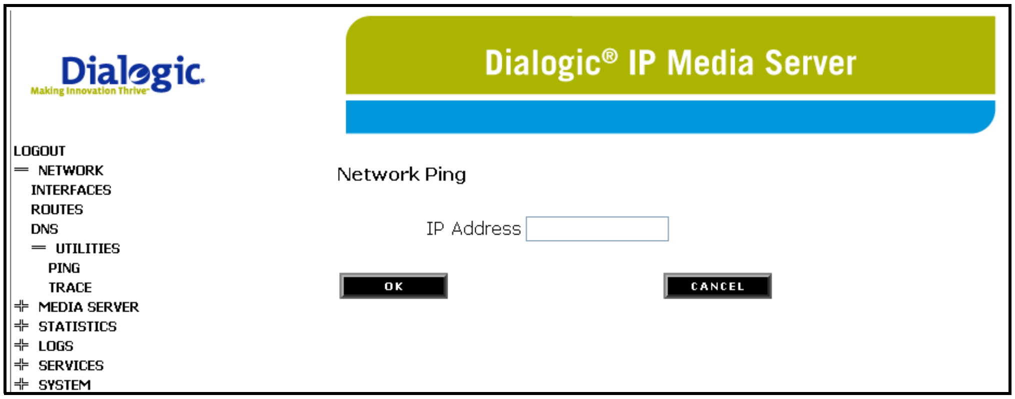
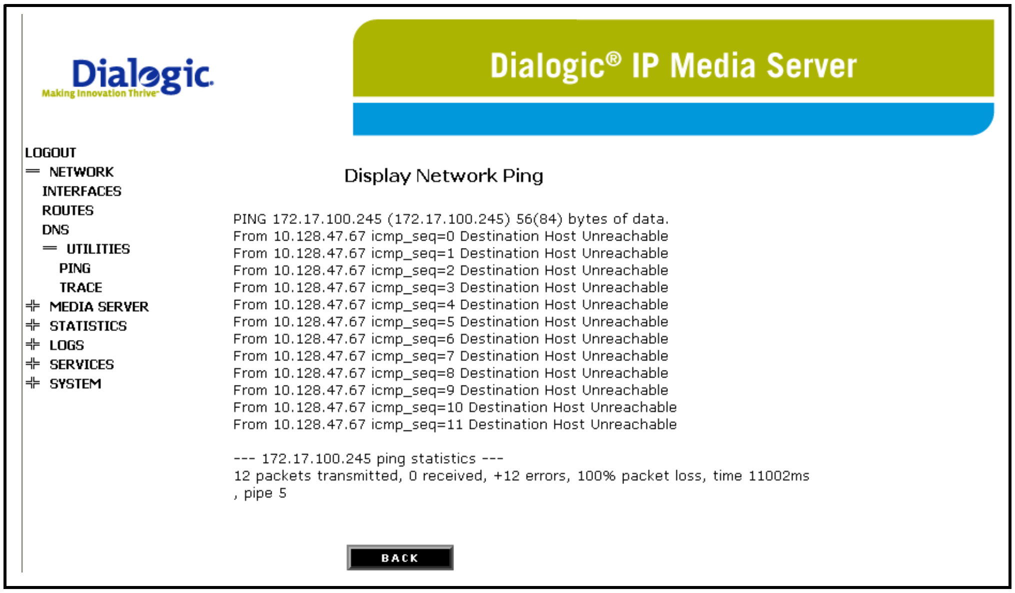


Figure 19. Network Ping Utility Page

2 Enter the IP address you want to test.

3 Click OK.

The Display Network Ping page appears with the results of the ping command.



```
PING 172.17.100.245 (172.17.100.245) 56(84) bytes of data.
From 10.128.47.67 icmp_seq=0 Destination Host Unreachable
From 10.128.47.67 icmp_seq=1 Destination Host Unreachable
From 10.128.47.67 icmp_seq=2 Destination Host Unreachable
From 10.128.47.67 icmp_seq=3 Destination Host Unreachable
From 10.128.47.67 icmp_seq=4 Destination Host Unreachable
From 10.128.47.67 icmp_seq=5 Destination Host Unreachable
From 10.128.47.67 icmp_seq=6 Destination Host Unreachable
From 10.128.47.67 icmp_seq=7 Destination Host Unreachable
From 10.128.47.67 icmp_seq=8 Destination Host Unreachable
From 10.128.47.67 icmp_seq=9 Destination Host Unreachable
From 10.128.47.67 icmp_seq=10 Destination Host Unreachable
From 10.128.47.67 icmp_seq=11 Destination Host Unreachable

--- 172.17.100.245 ping statistics ---
12 packets transmitted, 0 received, +12 errors, 100% packet loss, time 11002ms
, pipe 5
```

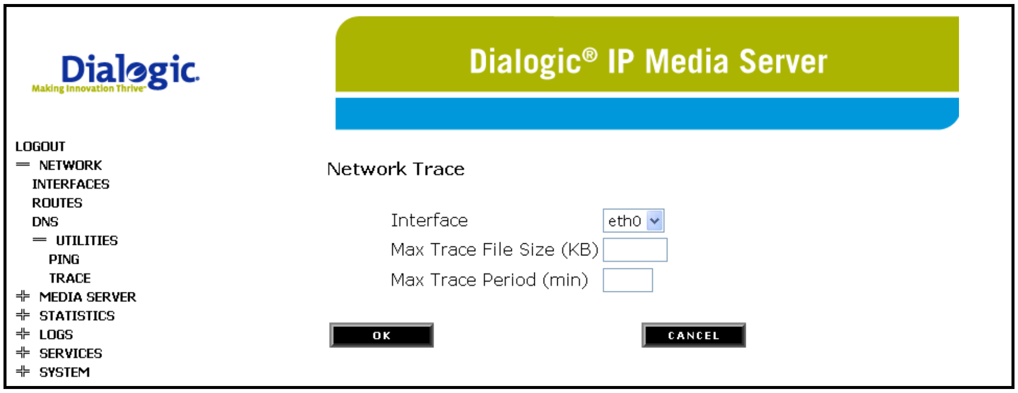
Figure 20. Display Network Ping Page

4 Click BACK to return to the Network Ping page.

Trace Utility

The Trace Utility enables you to capture a network trace of all incoming and outgoing IP traffic. you can access the output from this trace from the LOGS→TRACE page. All of the traces are named by a date/timestamp.

1 Select NETWORK→UTILITIES→TRACE to display the Network Trace page:



Network Trace

Interface eth0

Max Trace File Size (KB)

Max Trace Period (min)

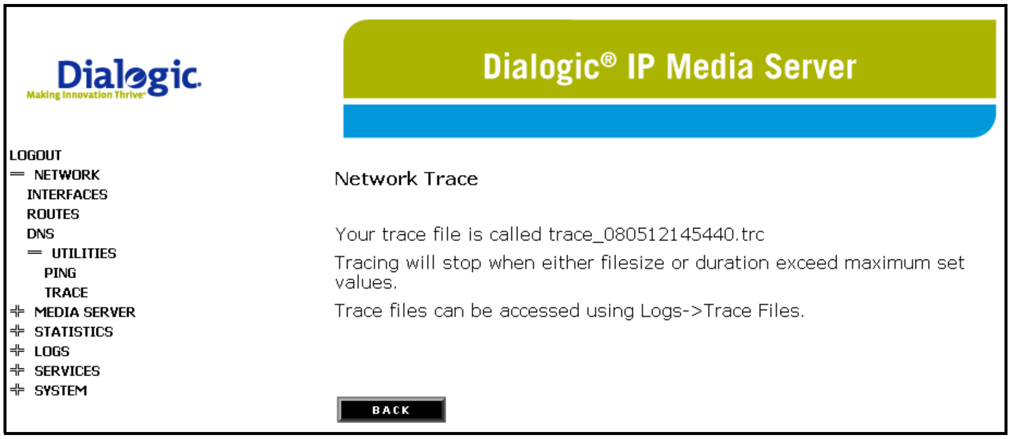
Figure 21. Network Trace Page

2 Enter the Ethernet interface you want to monitor.

3 Enter the maximum trace file size in kilobytes.

4 Enter the maximum trace time period in minutes.

5 Click OK to start the trace. The following page appears, providing status information about the trace:



Network Trace

Your trace file is called trace_080512145440.trc

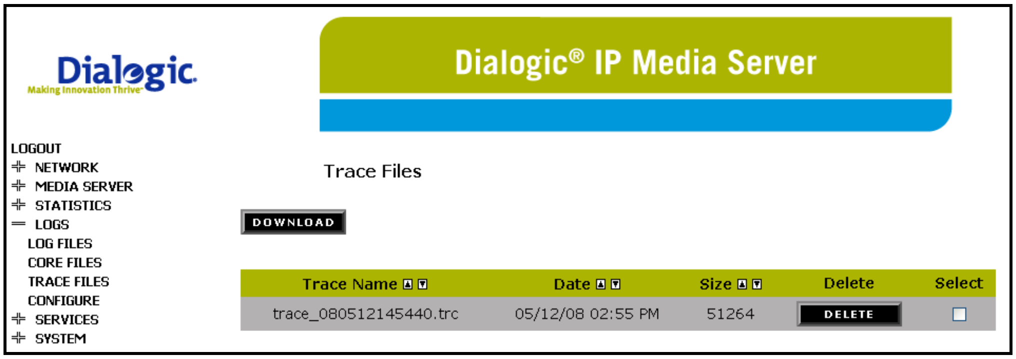
Tracing will stop when either filesize or duration exceed maximum set values.

Trace files can be accessed using Logs->Trace Files.

Figure 22. Network Trace - Status Page

6 Click BACK to return to the Network Trace page.

7 To view a trace file, select the Logs→Trace Files menu to display the Trace Files page:



Trace Files

Trace Name	Date	Size	Delete	Select
trace_080512145440.trc	05/12/08 02:55 PM	51264	DELETE	□

Figure 23. Trace Files Page

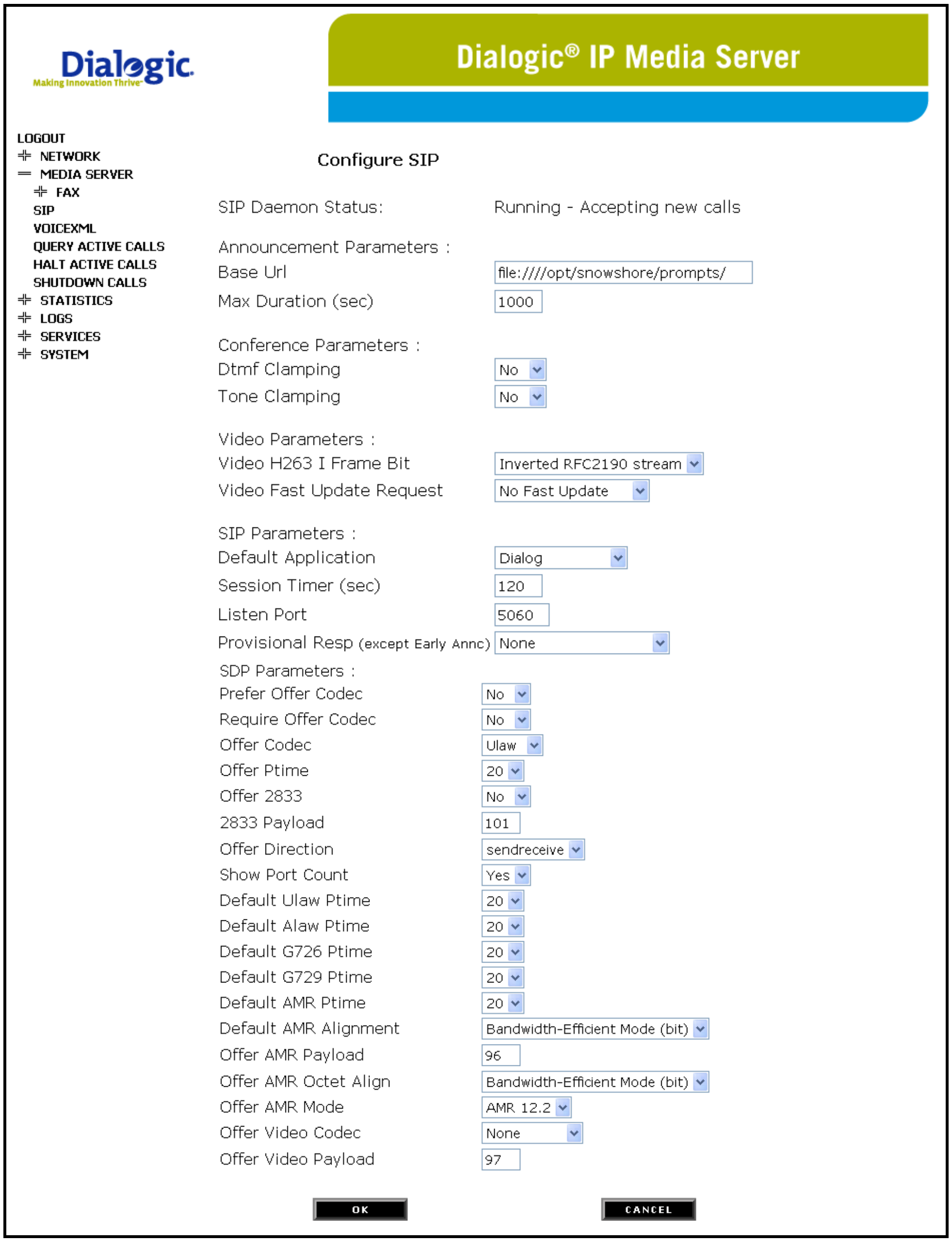
8 To view the trace file, click DOWNLOAD. The trace file is a text file you can view with any network analyzer software.

Configuring SIP and SDP

This section describes the IP Media Server parameters associated with signaling and media services. All user access levels can display the configuration, but only Administrators can change the configuration.

⚠ **The commands in this configuration section manipulate the configuration file. To apply a new configuration, reboot the IP Media Server.**

1 Select the MEDIA SERVER→SIP menu to display the Configure SIP page (Figure 24). This page enables you to configure the SIP and SDP parameters described below.



Configure SIP

SIP Daemon Status: Running - Accepting new calls

Announcement Parameters :
Base Url: file:////opt/snowshore/prompts/
Max Duration (sec): 1000

Conference Parameters :
Dtmf Clamping: No
Tone Clamping: No

Video Parameters :
Video H263 I Frame Bit: Inverted RFC2190 stream
Video Fast Update Request: No Fast Update

SIP Parameters :
Default Application: Dialog
Session Timer (sec): 120
Listen Port: 5060
Provisional Resp (except Early Annc): None

SDP Parameters :
Prefer Offer Codec: No
Require Offer Codec: No
Offer Codec: Ulaw
Offer Ptime: 20
Offer 2833: No
2833 Payload: 101
Offer Direction: sendreceive
Show Port Count: Yes
Default Ulaw Ptime: 20
Default Alaw Ptime: 20
Default G726 Ptime: 20
Default G729 Ptime: 20
Default AMR Ptime: 20
Default AMR Alignment: Bandwidth-Efficient Mode (bit)
Offer AMR Payload: 96
Offer AMR Octet Align: Bandwidth-Efficient Mode (bit)
Offer AMR Mode: AMR 12.2
Offer Video Codec: None
Offer Video Payload: 97

Figure 24. Configure SIP Page

Table 9. Configure SIP Parameters

Parameter	Values	Description
SIP Daemon Status	• SIPD is running; accepting calls. • SIPD is running, but not accepting calls. • SIPD is not running.	Current status of the SIP Daemon (SIPD).

Table 9. Configure SIP Parameters (Continued)

Parameter	Values	Description
Announcement Parameters		

Base URL	<string>	String that is prepended to non-rooted audio URLs. If an INVITE arrives with just a file name, the file name is assumed to be in the location specified in the base URL. For example, if the base URL is:
		`file:////net/IP_of_nfs_server/path_of_file_storage/`
		an invite such as:
		`INVITE sip:annc@172.17.100.157;play=circuit_busy.ulaw`
		rewrites the URL by prepending the Base URL as:
		`file:////net/IP_of_nfs_server/path_of_file_storage/circuit_busy_.ulaw`

Max Duration	- 0 - 1-10000 (Default: 0)	System-wide default announcement duration in seconds to be used if no per-call duration parameter is specified in the SIP URI. This parameter is used for both early and normal media announcements. Once the limit is reached, the IP Media Server terminates the call. A setting of 0 indicates no announcement duration limit.

Table 9. Configure SIP Parameters (Continued)

Parameter	Values	Description
Conference Parameters		
DTMF Clamping	- Yes - No (Default: No)	Simple conferences do not support DTMF clamping. Enhanced conferences use this parameter as the default when each leg is created in a conference. It can be changed later with an INFO with a new value.
Tone Clamping	- Yes - No (Default: No)	Simple conferences do not support tone clamping. Enhanced conferences use this parameter as the default when each leg is created in a conference. It can be changed later with an INFO with a new value.
Video Parameters		
Video H263 I Frame Bit	- Inverted RFC2190 Stream - RFC2190 Stream - Inverted H263 Location - H263 Location	Sets the I-frame bit.
Video Fast Update Request	- No Fast Updates - Media XML Updates	Sets the fast-update request field.
SIP Parameters		
Default Application	- Announcement) - Conference - Dialog - IVR (Default: Dialog)	Application (SIP service) used if the INVITE message does not specify an application.

Table 9. Configure SIP Parameters (Continued)

Parameter	Values	Description
Session Timer	integer: ◆ 0 ◆ 10 - 6000 (Default: 120)	SIP Session Timer interval in seconds. A setting of 0 turns session timers off. The IP Media Server issues a session timer refresh every t/2 seconds, where t is the value set by this command. Setting this timer to a small value can significantly increase the volume of SIP message traffic over the network and can negatively impact overall service delivery and performance.
Listen Port	integer: 1025 - 65535 (Default: 5060)	UDP port used for SIP.
Provisional Response	◆ None ◆ Send 180 (ringing) ◆ Send 183 (progress).	This parameter only applies to dialog, conference, and announce services. The provisional responses sent for these services never contain SDP information. Early announce always sends 183 Session Progress. The 183 sent for early announce is not affected by this value and always contains SDP information. This feature is normally used when interacting with other protocols that require resource reservation (e.g., PacketCable, NCS) when establishing a session.
SDP Parameters		
Prefer Offer Codec	◆ Yes ◆ No (Default: No)	If Yes, the Offer Codec is used as the highest preference codec in the offer. If the Offer codec is not present, another codec can be used.

Table 9. Configure SIP Parameters (Continued)

Parameter	Values	Description
Require Offer Codec	- Yes - No (Default: No)	The policy for the SDP offer. - If Yes, the offer SDP must match the parameters Offer Codec, Offer 2833, 2833 Payload, and Offer Direction. It the offer does not match, the call is rejected. - If No, the standard offer/answer rules are used, taking into account the setting of the Prefer Offer Codec parameter.
Offer Codec	- Ulaw - Alaw - G726 - G729 - AMR (Default: Ulaw)	Codec offered by the IP Media Server in the SDP m= audio line. This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.
Offer Ptime	- 10 - 20 - 30 (Default: 20)	Length of time in milliseconds represented by the media in a packet offered by the IP Media Server in the SDP attribute (a=). This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.
Offer 2833	- Yes - No (Default: Yes)	Whether 2833 is offered.
2833 Payload	integer: 96–127 (Default: 101)	Dynamic payload type to be used when 2833 is offered.
Offer Direction	- sendonly - recvonly - sendrecv (Default:sendrecv)	Direction of the media stream offered by the IP Media Server in the SDP attribute (a=). This setting applies when the inbound initial INVITE does not contain an SDP body, forcing the IP Media Server response to make the initial SDP offer.

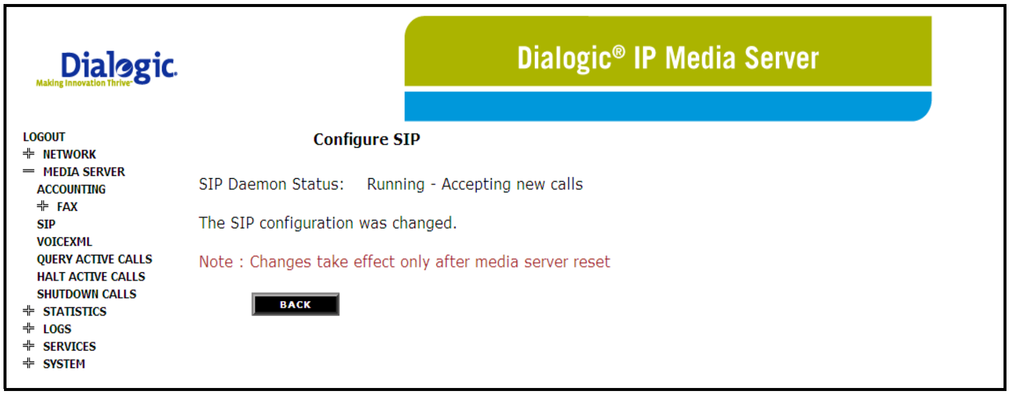
Table 9. Configure SIP Parameters (Continued)

Parameter	Values	Description
Show Port Count	◆ Yes ◆ No (Default: Yes)	Whether "/1" is appended to the port number in the SDP attribute (m=).
Default Ulaw Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default Alaw Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default G726 Ptime	◆ 10 ◆ 20 ◆ 30 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default G729 Ptime	◆ 10 ◆ 20 ◆ 40 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default AMR Ptime	◆ 20 ◆ 40 (Default: 20)	Value to use when the SDP offer is received, but the PTIME attribute is not specified. This value appears in the SDP answer sent by the IP Media Server.
Default AMR Alignment	◆ Bandwidth-Efficient Mode (bit) ◆ Octet-Aligned Mode (byte)	Default alignment mode to be used when INVITE SDP specifies AMR encoding, but does not specify the alignment mode.
Offer AMR Payload	integer: 96–127 (Default: 96)	Dynamic payload type to be used when AMR is offered.
Offer AMR Octet Align	◆ Bandwidth-Efficient Mode (bit) ◆ Octet-Aligned Mode (byte)	Alignment mode to be used when AMR is offered.

Table 9. Configure SIP Parameters (Continued)

Parameter	Values	Description
Offer AMR Mode	• AMR 4.75 • AMR 5.15 • AMR 5.9 • AMR 6.7 • AMR 7.4 • AMR 7.95 • AMR 10.2 • AMR 12.2	Default AMR-NB encoding mode (bit rate).
Offer Video Codec	• None • H263 • H263-1998 • H263-2000 • H264	Default video codec for the IP Media Server.
Offer Video Payload	integer: 96–127 (Default: 97)	Dynamic payload type to be used when video is offered.

When you have made your changes, click OK to confirm them. A confirmation page is displayed (Figure 25). Click BACK to return to the IP Media Server home page.



Configure SIP

SIP Daemon Status: Running - Accepting new calls

The SIP configuration was changed.

Note : Changes take effect only after media server reset

Figure 25. Configure SIP Change Confirmation Page

2 Click CANCEL to return all values to their previous settings and return to the IP Media Server home page.

Note: Your changes to these parameters take effect only after the IP Media Server is rebooted.

Configuring VoiceXML

Use the Media Server→VoiceXML menu to configure VoiceXML support on the IP Media Server. The Configure VoiceXML page (see Figure 26 and Figure 27) appears when you select Media Server→VoiceXML.

VoiceXML Version

The IP Media Server supports two versions of VoiceXML:

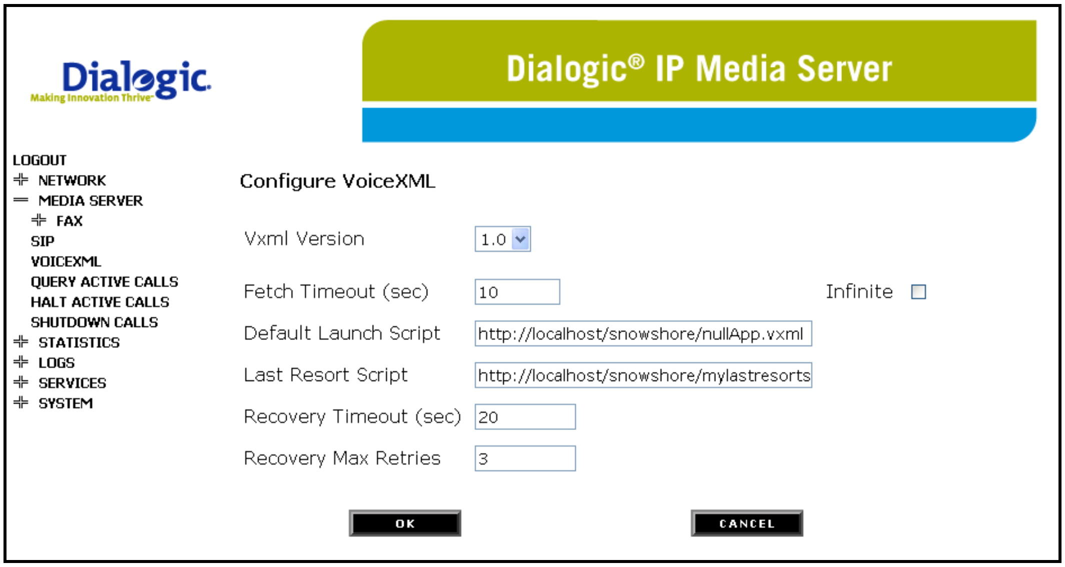
- VoiceXML 1.0
- VoiceXML 2.0 (default browser)

Use the Vxml Version drop-down list box to select the version of VoiceXML that you want to enable on the IP Media Server. The default is VoiceXML version 2.0. The parameters that appear on page depend on which version of VoiceXML you enable.

Each version has its own configuration parameters. The parameters associated with VoiceXML 1.0 and 2.0 configurations are described below.

VoiceXML 1.0 Configuration Parameters

If you select VXML Version 1.0, the Configure VoiceXML page appears as follows:



Configure VoiceXML

Vxml Version: 1.0

Fetch Timeout (sec): 10 Infinite □

Default Launch Script: http://localhost/snowshore/nullApp.vxml

Last Resort Script: http://localhost/snowshore/mylastresorts

Recovery Timeout (sec): 20

Recovery Max Retries: 3

Figure 26. Configure VoiceXML 1.0 Page

Table 10 describes the parameters you can set for VoiceXML Version 1.0.

Table 10. VoiceXML 1.0 Parameters

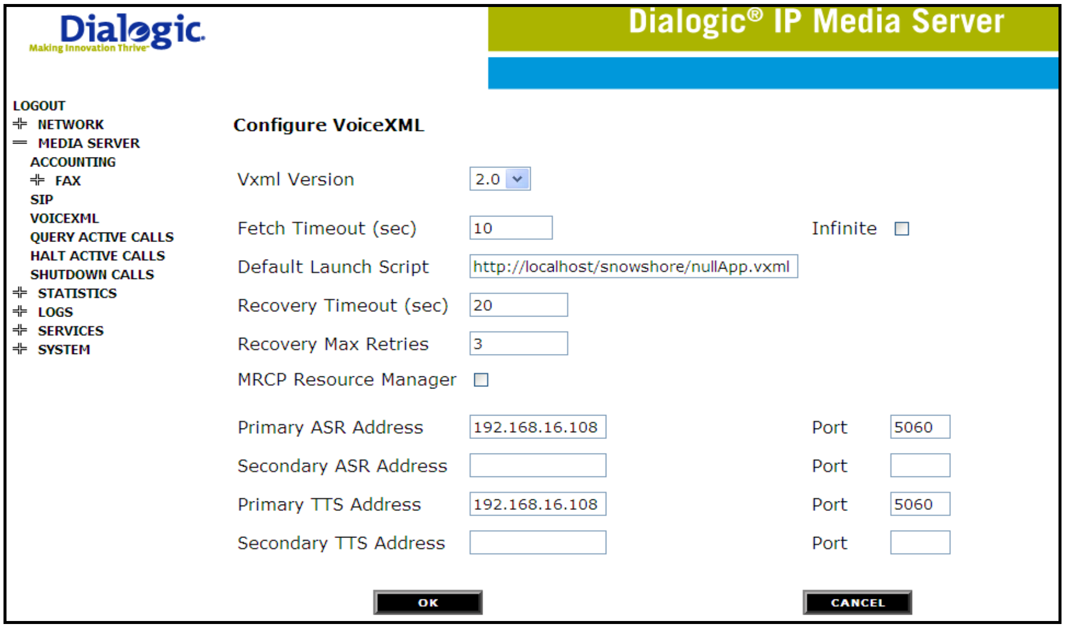
Parameter	Values	Description
Fetch Timeout	integer: 1–65, infinite (Default: 10)	Time (in seconds) the IP Media Server waits when trying to fetch a VoiceXML script from the network. A value of infinite means that a fetch timeout is not applied.
Default Launch Script	<string>	VXML script that is fetched if a dialog request is received and it does not contain a voicexml= parameter. This parameter allows a call to be accepted and for a VoiceXML script to be launched as a result of the initial SIP invite. A Launch Script is required regardless of the browser.
Last Resort Script	<string>	VXML script that is fetched and executed if the VoiceXML browser cannot retrieve the initial VoiceXML script due to a network, server, or other system issue.
Recovery Timeout	integer (Default: 20)	Time (in seconds) after which an attempt to recover media content files will fail. This setting and the Recovery Max Retries setting apply to VXML applications that use the Media Content Recovery extensions in VXML 1.0.

Table 10. VoiceXML 1.0 Parameters

Parameter	Values	Description
Recovery Max Retries	integer (Default: 3)	Number of times to retry the recovery of media content files. If a particular file cannot be delivered within the configured number of retry attempts, a "final failure" state is reached. If this occurs, the recovery daemon writes an error-level log message specifying the file name and associated recovery information. The recovery daemon generates an SNMP trap to inform the operator of this condition.

VoiceXML 2.0 Configuration Parameters

If you select VXML Version 2.0, the Configure VoiceXML page appears as follows:



Configure VoiceXML

Vxml Version	2.0		
Fetch Timeout (sec)	10	Infinite	□
Default Launch Script	http://localhost/snowshore/nullApp.vxml		
Recovery Timeout (sec)	20		
Recovery Max Retries	3		
MRCP Resource Manager	□		
Primary ASR Address	192.168.16.108	Port	5060
Secondary ASR Address		Port	
Primary TTS Address	192.168.16.108	Port	5060
Secondary TTS Address		Port	

Figure 27. Configure VoiceXML 2.0 Page

Table 11 describes the parameters you can set for VoiceXML Version 2.0.

Table 11. VoiceXML 2.0 Parameters

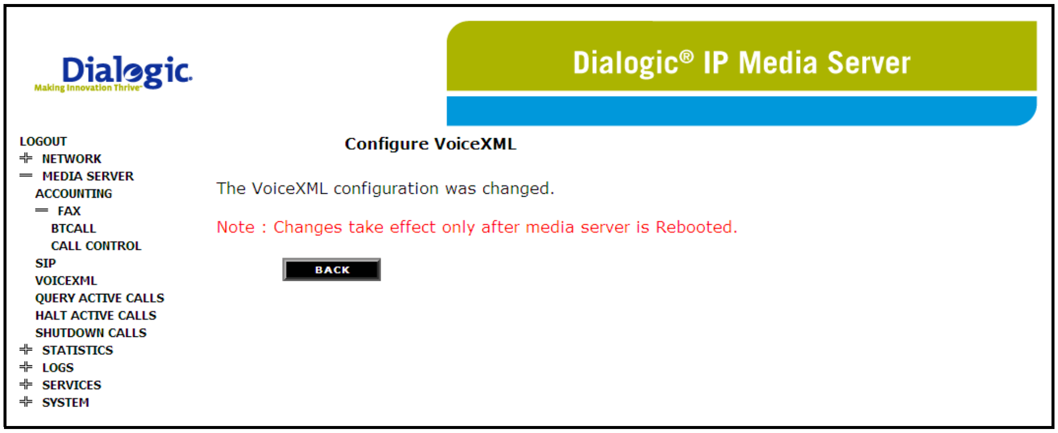
Parameter	Values	Description
Fetch Timeout	integer: 1–65, infinite (Default: 10)	Time (in seconds) the IP Media Server waits when trying to fetch a VoiceXML script from the network. A value of infinite means that a fetch timeout is not applied.
Default Launch Script	<string>	VXML script that is fetched if a dialog request is received and it does not contain a voicexml= parameter. This parameter allows a call to be accepted and for a VoiceXML script to be launched as a result of the initial SIP invite. A Launch Script is required.
Recovery Timeout	integer (Default: 20)	Time (in seconds) after which an attempt to recover media content files will fail. This setting and the Recovery Max Retries setting apply to VXML applications that use the Media Content Recovery extensions.
Recovery Max Retries	integer (Default: 3)	Number of times to retry the recovery of media content files. If a particular file cannot be delivered within the configured number of retry attempts, a "final failure" state is reached. If this occurs, the recovery daemon writes an error-level log message specifying the file name and associated recovery information. The recovery daemon generates an SNMP trap to inform the operator of this condition.
MRCP Resource Manager	Checkbox	Indicates that the Nuance Resource Manager is used to load balance MRCP sessions across multiple MRCP servers.

Table 11. VoiceXML 2.0 Parameters

Parameter	Values	Description
Primary ASR Address	IP Address (associated with a port)	All MRCP sessions will be established against the primary ASR server until the time that it cannot be reached or is out of resources. When this condition is detected, all future MRCP requests go to the secondary server until it enters the same state or the IPMS server is restarted
Secondary ASR Address	IP Address (associated with a port)	The secondary server performs the roll of a “hot standby” ASR server.
Primary TTS Address	IP Address (associated with a port)	All MRCP sessions will be established against the primary TTS server until the time that it cannot be reached or is out of resources. When this condition is detected, all future MRCP requests go to the secondary server until it enters the same state or the IPMS server is restarted.
Secondary TTS Address	IP Address (associated with a port)	The secondary server performs the roll of a “hot” TTS standby
Port	Integer	Indicates the Nuance TCP port that is used to send SIP signaling to establish MRCP sessions. The ports are based on what is configured on the Nuance MRCP server and are outside IP Media Server Control.

Reboot after Changing Parameters

You must reboot the IP Media Server for changes to any of the VoiceXML parameters or settings require to take effect.



Configure VoiceXML

The VoiceXML configuration was changed.

Note : Changes take effect only after media server is Rebooted.

Figure 28. Configure VoiceXML Confirmation Page

Configuring Fax

The fax software in the IP Media Server comes preconfigured. If you want to change any of the default values of the attributes, follow the procedures below to update the following configuration files:

- btcall
- Call Control

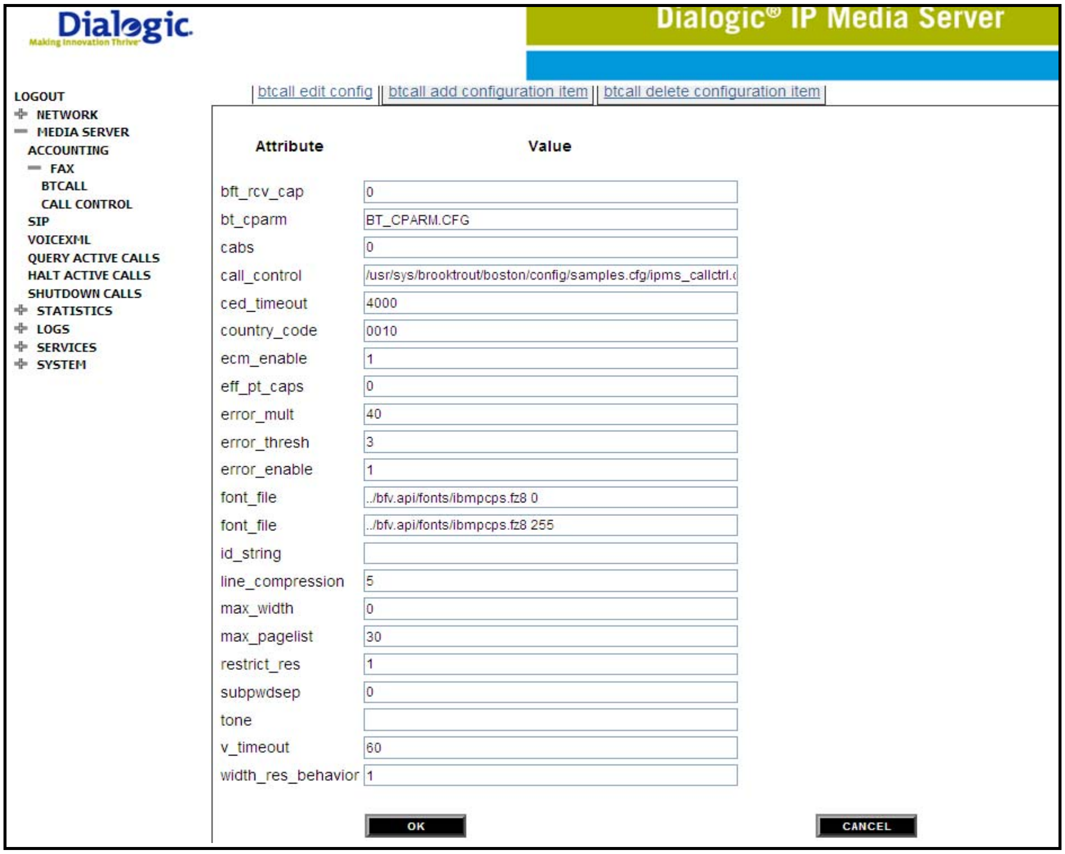
btcall

Follow the procedure below to edit, add, and/or delete attributes for the btcall configuration file.

Editing btcall Attributes

Follow the steps below to edit BTCALL attributes.

1 Select FAX → BTCALL and click the btcall edit config tab. The following screen appears.



Attribute	Value
bft_rcv_cap	0
bt_cparm	BT_CPARM.CFG
cabs	0
call_control	/usr/sys/brooktrout/boston/config/samples.cfg/ipms_callctrl.c
ced_timeout	4000
country_code	0010
ecm_enable	1
eff_pt_caps	0
error_mult	40
error_thresh	3
error_enable	1
font_file	../bfv.api/fonts/ibmpcps.fz8 0
font_file	../bfv.api/fonts/ibmpcps.fz8 255
id_string	
line_compression	5
max_width	0
max_pagelist	30
restrict_res	1
subpwdsep	0
tone	
v_timeout	60
width_res_behavior	1

Figure 29. Edit btcall Configuration

2 Complete the screen as indicated in Table 12 below. Click OK when complete.

Table 12. btcall attributes

Attribute	Values	Description
bft_rcv_cap		Not used
bt_cparm	String Default: BT_CPARM.CFG	Specifies the path and name of the country telephony parameter file to use.
call_control	<User defined>	Specifies the name of the call control configuration file to use.
cabs		Not used
ced_timeout	Country dependent: 4000 (40 sec) in USA	Specifies the length of time, in 10 ms units, to wait for a fax answer tone (CED tone) from a remote fax machine. This parameter can only be set if the host country permits changing the wait_for_ced_high and wait_for_ced_low
country_code	<Hexadecimal> Default: 0010 (USA)	Specifies the international country code with modifiers. Initial digits (up to 3) identify the host country; the last digit supplies a modifier for properties such as the phone system attached to the board. The ccode.h header file contains the available country codes.
ecm_enable	0 - Turns off ECM 1 - Turns on ECM (256-byte frames) (default) 2 - Turns on ECM (64-byte frames)	Turns ECM (error correction mode) on or off. If disabled, MMR fax compression on the line is unavailable. The normal ECM frame size is 256 bytes. You can enable a frame size of 64 bytes, but the channel uses that frame size on transmit only. On receive, it always uses the frame size the transmitter selects.

Attribute	Values	Description
eff_pt_caps	Values are formed by logically ORing together the base values: 0 - Enhanced fax format reception disabled. 1 - JPEG. 2 - Full color mode (JPEG). 4 - Reserved for Huffman tables, do not use. 8 - 12 bits/pel, otherwise 8 bits/pel (JPEG). 10 - No subsampling (JPEG). 20 - Custom illuminant (JPEG). 40 - Custom Gamut (JPEG). 100 - JBIG. 200 - L0 Mode (JBIG).	Specifies the enhanced fax format page types that the channel is permitted to receive. If EFF page reception is enabled, then ECM is automatically enabled for receive faxes regardless of the setting of ecm_enable.
error_mult	<Decimal> Default: 40 (for 5% error rate)	Specifies an error multiplication value used to determine if the error percentage on a received page is too high. The number of errors per page is multiplied by this number and the product is divided by 2. If this result exceeds the number of lines on the page, the error percentage per page is too high and an RTN signal is returned to the transmitting station. The value set for this parameter should normally be less than that of the error_mult_rtp parameter (corresponding to a larger percentage). The RTN threshold takes precedence over the RTP threshold.
error_thresh	<Decimal> Default: 3	Specifies an error threshold value of n (2n for fine resolution) number of consecutive bad G3 lines on a received page. A page with errors in this number of consecutive lines is considered bad, regardless of the results from error_mult. An RTN is returned when a “bad” page occurs.

Attribute	Values	Description
error_enable	0 - Off 1 - On (default)	Turns error detection on (1) or off (0) during fax reception in non-ECM mode.
font_file	<String or Decimal> 0 - 6, 255 Default: ibmpcps.fz8 (no path) and 0	Specifies the name of the file that contains the transmit/convert font for ASCII. An optional font number, indicating the downloadable font to use, can be specified (if no font number is specified, 0 is assumed). The font file must be located in the current directory, or the correct path must be included with its name. The file is opened, and the contents downloaded to the module when BfvLineReset is called using the mill_load_fonts option. Multiple occurrences of font file parameters with different font numbers are permitted in the configuration file. When a font number that is specified for ASCII conversion has not been downloaded, a default font is used. This is font 255. Font 255 may be specified using the font_file keyword. If not, it defaults to ibmpcps.fz8 (no path). When font downloads are done as described above, font 255 is always downloaded regardless of whether other font numbers are listed using this keyword. Some font numbers may be reserved for preloaded fonts.
id_string	<String> Default: 20 spaces	Sets the default ID string (up to 20 characters long) for fax machines. The parameter can be overridden by the BfvFaxSetLocalId function if the host country permits changing the ID string.
line_compression	0 - MH only 1 - MR or MH 5 - MMR, MR, or MH (default)	Specifies the permitted compression types for fax transmission or reception on the phone line. This specification is independent of the file format specified for transmission or reception. If ECM is disabled, then MMR fax compression on the line is unavailable.

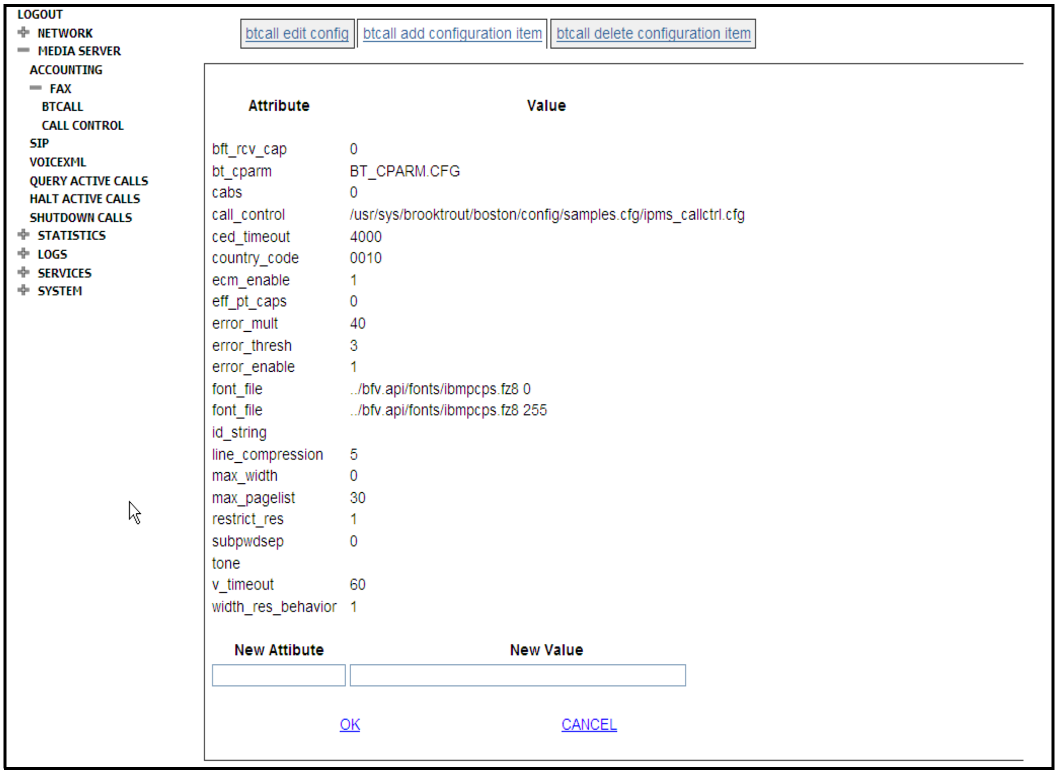
Attribute	Values	Description
max_width	0 - 215 mm A4 1728 Normal resolution pixels. (default) 1 - 255 mm B4 2048 Normal resolution pixels. 2 - 303 mm A3 2432 Normal resolution pixels.	Sets the maximum page width permitted for fax reception.
max_pagelist	<Decimal> Default: 30	Specifies the maximum number of pages allowed for storing results during a call. The last max_pagelist PAGE_RES structures are accessible via the FAX_RES structure if this feature has been enabled.
restrict_res	0 - 200H x 100V (normal) and 100H x 100V (for JPEG only) 1 - 200H x 200V (fine) 2 - 200H x 400V 4 - 300H x 300V 8 - 400H x 400V 10 - 300H x 600V 20 - 400H x 800V 40 - 600H x 600V 80 - 600H x 1200V 100 - 1200H x 1200V	Specifies allowable resolutions for fax reception. Regardless of the value chosen, 200H x 100V (normal) and 100H x 100V (for JPEG only) is always allowed.
subpwdsep	To form values, OR together the following base values: 0 - SUB, PWD, and SEP reception disabled. 1 - SEP reception enabled. 2 - PWD reception enabled. 4 - SUB reception enabled.	Enables reception of the SUB, PWD, and SEP FSK signals. Applications typically use these signals to direct or validate incoming calls.
Tone	Tone	Channel used DTMF tone dialing as the default mode

Attribute	Values	Description
v_timeout	<Decimal> Default: 60	Specifies the maximum time (in seconds) to wait after the last dialed digit for a final call progress result. Use only when you select CALL_PROTOCOL_VOICE mode. This parameter only applies to the use of BfvLineOriginateCall and BfvLineOrigCallDB.
width_res_behavior	<Decimal> Default: 1	Specifies the action taken as a result of page width or resolution mismatches on fax transmission. Does not affect fax reception. Scaling the fax is not available for all combinations of resolution mismatches.

Adding btcall Attributes

Follow the steps below to add new btcall attributes.

1 Select FAX → BTCALL and click the btcall add configuration item tab. The following screen appears.



Attribute	Value
bft_rcv_cap	0
bt_cparm	BT_CPARM.CFG
cabs	0
call_control	/usr/sys/brooktrout/boston/config/samples.cfg/ipms_callctrl.cfg
ced_timeout	4000
country_code	0010
ecm_enable	1
eff_pt_caps	0
error_mult	40
error_thresh	3
error_enable	1
font_file	../bfv.api/fonts/ibmpcps.fz8 0
font_file	../bfv.api/fonts/ibmpcps.fz8 255
id_string	
line_compression	5
max_width	0
max_pagelist	30
restrict_res	1
subpwdsep	0
tone	
v_timeout	60
width_res_behavior	1

New Attibute New Value

Figure 30. Add btcall Configuration Item

2 Enter the attribute in the New Attribute field.

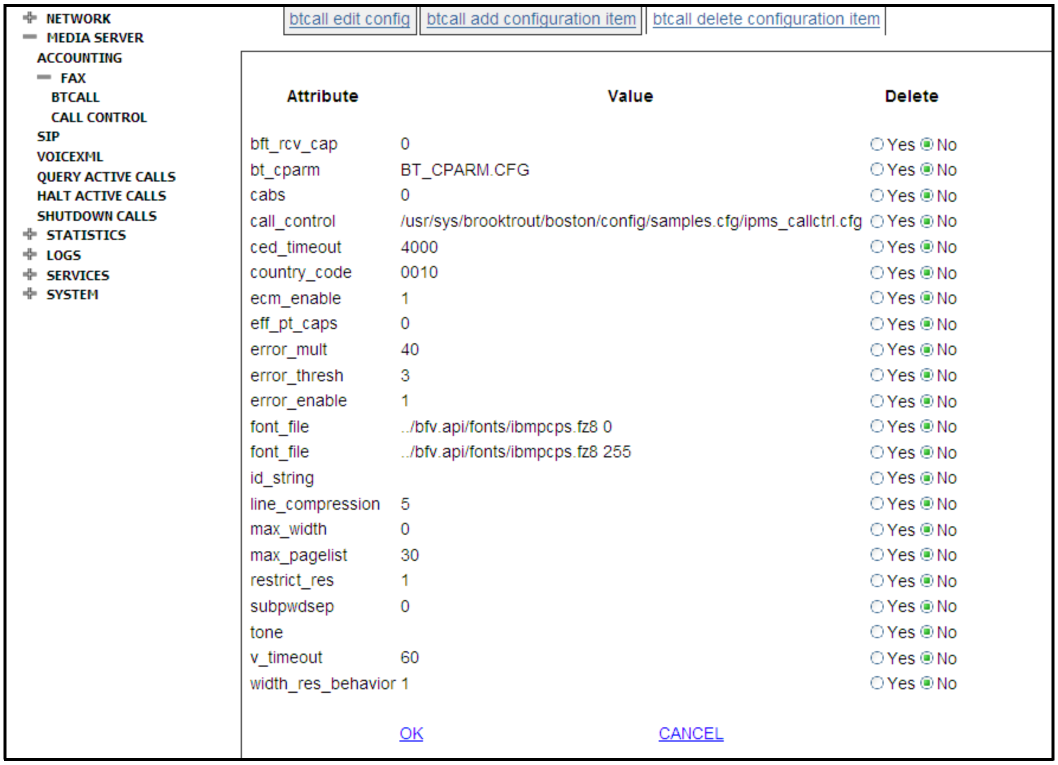
3 Enter the value in the New Value field.

4 Repeat the steps above for additional attributes.

5 Click OK when complete.

Deleting btcall Attributes

1 Select FAX → BTCALL and click the btcall delete configuration tab. The following screen appears.



Attribute	Value	Delete
bft_rcv_cap	0	○Yes ●No
bt_cparm	BT_CPARM.CFG	○Yes ●No
cabs	0	○Yes ●No
call_control	/usr/sys/brooktrout/boston/config/samples.cfg/ipms_callctrl.cfg	○Yes ●No
ced_timeout	4000	○Yes ●No
country_code	0010	○Yes ●No
ecm_enable	1	○Yes ●No
eff_pt_caps	0	○Yes ●No
error_mult	40	○Yes ●No
error_thresh	3	○Yes ●No
error_enable	1	○Yes ●No
font_file	../bfv.api/fonts/ibmpcps.fz8 0	○Yes ●No
font_file	../bfv.api/fonts/ibmpcps.fz8 255	○Yes ●No
id_string		○Yes ●No
line_compression	5	○Yes ●No
max_width	0	○Yes ●No
max_pagelist	30	○Yes ●No
restrict_res	1	○Yes ●No
subpwdsep	0	○Yes ●No
tone		○Yes ●No
v_timeout	60	○Yes ●No
width_res_behavior	1	○Yes ●No

Figure 31. Delete btcall Configuration Item

2 Select Yes next to the attributes that you want to delete.

3 Click OK.

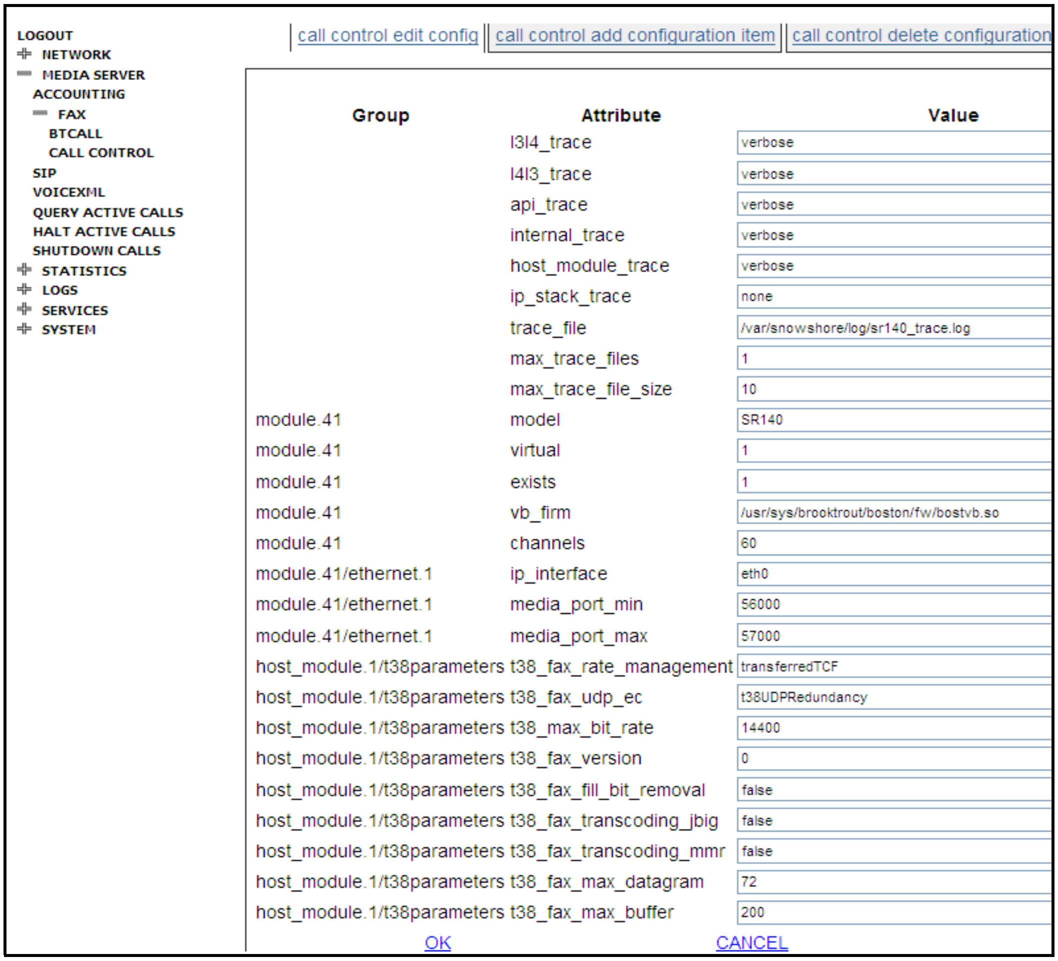
Call Control

Follow the procedures below to edit, add, and/or delete attributes in the Call Control configuration file.

Editing Call Control Attributes

Follow the steps below to edit BTCALL attributes.

1 Select FAX → CALL CONTROL and click the call control edit config tab. The following screen appears.



Group	Attribute	Value
	l3l4_trace	verbose
	l4l3_trace	verbose
	api_trace	verbose
	internal_trace	verbose
	host_module_trace	verbose
	ip_stack_trace	none
	trace_file	/var/snowshore/log/sr140_trace.log
	max_trace_files	1
	max_trace_file_size	10
module.41	model	SR140
module.41	virtual	1
module.41	exists	1
module.41	vb_firm	/usr/sys/brooktrout/boston/fw/bostvb.so
module.41	channels	60
module.41/ethernet.1	ip_interface	eth0
module.41/ethernet.1	media_port_min	56000
module.41/ethernet.1	media_port_max	57000
host_module.1/t38parameters	t38_fax_rate_management	transferredTCF
host_module.1/t38parameters	t38_fax_udp_ec	t38UDPRedundancy
host_module.1/t38parameters	t38_max_bit_rate	14400
host_module.1/t38parameters	t38_fax_version	0
host_module.1/t38parameters	t38_fax_fill_bit_removal	false
host_module.1/t38parameters	t38_fax_transcoding_jbig	false
host_module.1/t38parameters	t38_fax_transcoding_mmr	false
host_module.1/t38parameters	t38_fax_max_datagram	72
host_module.1/t38parameters	t38_fax_max_buffer	200

Figure 32. Edit Call Control Configuration

2 Complete the screen as indicated in Table 13 below. Click OK when complete.

Table 13. Call Control attributes

Attribute	Values	Description
1314_trace	none - Does not perform a trace operation (default value). error - Detects errors and stores them in the specified trace_file. warning - Detects warnings and stores them in the specified trace_file. basic - Stores a simplified trace in the specified trace_file. verbose - Stores a complete trace of operations in the specified trace_file.	Traces BSMI messages between layers 3 and 4.
1413_trace	Same as 1314_trace above.	Traces BSMI messages between layers 4 and 3.
api_trace	Same as 1314_trace above.	Traces call control activity to and from the Bfv API functions.
internal_trace	Same as 1314_trace above.	Traces call control activity in areas not otherwise covered. Dialogic's engineering personnel use this tracing. Application developers are not advised to select this type of tracing.
host_module_trace	Same as 1314_trace above.	Traces call control activity to and from all host modules defined in your call control configuration file.
ip_stack_trace	Same as 1314_trace above.	Traces call control activity to and from all IP stack module libraries defined in your call control configuration file.
trace_file	<user defined>	Turns on tracing and reports results to the filename specified for this parameter.

Attribute	Values	Description
max_trace_files	1 - 999 Default: 1	Specifies the maximum number of trace files for the API to retain on the system’s file system. When set to a value greater than 1, the API appends a sequence number extension to the file name, starting at 1. If the number of created trace files exceeds the value set for this parameter, the API starts deleting files from the lowest numbered trace log until it frees sufficient disk space to store the last created file. To prevent deleting older files, set the maximum number of trace files to a large number.
max_trace_file_size	0 - Sets the trace file to an unlimited size Default: 10	Specifies the maximum size, in megabytes, allowed for the trace file. If the trace of operations reaches this size, tracing loops back to the start of the file and the continued trace starts overwriting the older trace.
model	<user defined>	Indicates a value that identifies the name of a module. The configuration tool uses the value in this parameter as the cached information that identifies the module when in offline mode.
virtual	1	If present in the file, this parameter indicates that the module is a virtual module. When the parameter is absent, configuration applies to a hardware module.
exists	0 - Module does not exist 1 - Module exists	Indicates the state of a module.
vb_firm	Default: No default. Absence of the parameter indicates that the module is not a virtual module.	Indicates that the module is a virtual module and specifies the filename of the shared library that contains the loadable firmware for the virtual module

Attribute	Values	Description
channels	0 - Specifies downloading the firmware to the default value of the number of channels on the module (default). 1 – 1024 - Specifies a value defining the number of channels on the module configured to receive a firmware download.	Specifies the number of channels on either a hardware or virtual module configured to receive a firmware download. When the firmware is downloaded to a module for the first time, the assigned ordinal channel numbers start wherever the assignment left off on the previous module. As the system initializes the modules, this numbering process creates a continuous ordering of the channel assignments across all the modules in the system. On later downloads, each module's ordinals begin at the same location, regardless of any decrease or increase in the channel count of a lower-numbered module. Therefore, if you decrease the channel count for a lower numbered module, the process creates gaps in the channel numbering assignments, possibly affecting your application. If you attempt to increase the channel count above any module's initial channel count, the system ignores the added channels. For the following situations, restart the driver whenever you want to: 1. Get a continuous assignment of channel numbers after decreasing the channel count on any module. 2. Increase the number of channels above a module's initial channel count.

Attribute	Values	Description
IP_interface	<string> Default: <blank>. The virtual module uses the first interface in the PC for sending IP messages.	Specifies the identity of the device on the PC with the IP interface that the virtual module can use for sending IP messages. Note: This parameter only applies to host-based fax applications using a virtual module. Set the value of this parameter to the name of any device in the PC with an IP interface. If you do not provide a value (blank string), the virtual module chooses the first interface in the PC to send its messages.
media_port_min	1024 - 64535 Default: 56000	Specifies the lowest IP port number that the module can use for media transmissions. Set this value to a value 1000 below the value specified for the media_port_max parameter.
media_port_max	2024 - 65535 Default: 57000	Specifies the highest IP port number that the module can use. Set this value to a value 1000 above the value specified for the media_port_min parameter.
t38_fax_rate_management	localTCF - Indicates that the transport uses the local training check frame (TCF) data rate management type (not supported). transferredTCF - Indicates that the transport uses the transferred training check frame (TCF) data rate management type. (Default)	Specifies a value that identifies the data rate management method of the transport.
t38_fax_udp_ec	t38UDPFEC - The transport uses the T.38 user datagram protocol (UDP) forward error correction (FEC) method (not supported). t38UDPRedundancy - The transport uses the T.38 UDP redundancy error correction method. (Default)	Specifies a value that identifies the error correction method of the T.38 fax transport.

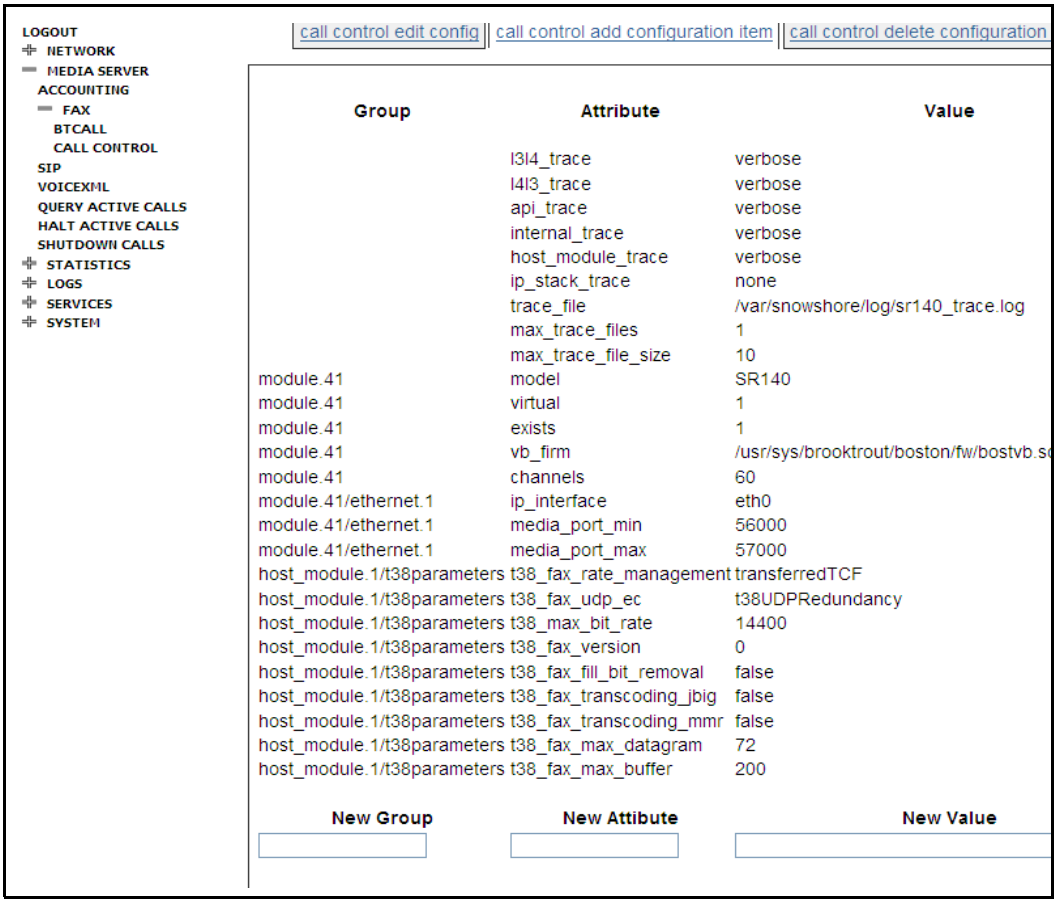
Attribute	Values	Description
T38_max_bit_rate	The following values represent the maximum bit rate that can be negotiated for fax packetization. 2400 4800 7200 9600 12000 14400 - default if T38 Fax Version is 0 or1 16800 19200 21600 24000 26400 28800 31200 33600 - default if T38 Fax Version is 2 or 3	Specifies a value that defines the maximum bit rate for fax packetization onto the network.
t38_fax_version	0, 1, 2, 3 Default: 3	Controls the maximum T.38 ASN.1 version the IP Call Control offers or accepts from a remote party. Versions 0, 1, 2 support a maximum bit rate of 14,400 bps. Version 3 supports V.34 and the following are the possible bit rates: 33,600 (default), 31,200, 28,800, 26,400, 24,000, 21,600, 16,800
t38_fax_fill_bit_removal	FALSE Indicates that the API does not support the capability. TRUE Indicates that the API can remove or insert fill bits.	Specifies whether the API can remove or insert fill bits to reduce the bandwidth of the transport mechanism. Note: This parameter does not affect the normal T.30-level capability to remove or insert fill bits.

Attribute	Values	Description
t38_fax_transcoding_jbig	FALSE - Indicates that the API does not support the capability. (Default) TRUE - Indicates that the API can convert JBIG fax images.	Specifies whether the API can convert to and from JBIG fax images to reduce the bandwidth of the transport mechanism when using a reliable transport (for example, TCP).
t38_fax_transcoding_MMR	FALSE Indicates that the API does not support the capability. (Default) TRUE Indicates that the API can convert MMR compression.	Specifies whether the API can convert to and from MMR fax compression to reduce the bandwidth of the transport mechanism when using a reliable transport (for example, TCP). Note: This parameter does not affect the normal T.30-level capability to use MMR if the two endpoints select MMR as a line compression format.
t38_fax_max_datagram	72	Maximum datagram for receive
t38_fax_max_buffer	200	Maximum fax buffer

Adding Call Control Attributes

Follow the steps below to add new Call Control attributes.

1 Select FAX → CALL CONTROL and click the call control add configuration item tab. The following screen appears.



Group	Attribute	Value
	l3l4_trace	verbose
	l4l3_trace	verbose
	api_trace	verbose
	internal_trace	verbose
	host_module_trace	verbose
	ip_stack_trace	none
	trace_file	/var/snowshore/log/sr140_trace.log
	max_trace_files	1
	max_trace_file_size	10
module.41	model	SR140
module.41	virtual	1
module.41	exists	1
module.41	vb_firm	/usr/sys/brooktrout/boston/fw/bostvb.s
module.41	channels	60
module.41/ethernet.1	ip_interface	eth0
module.41/ethernet.1	media_port_min	56000
module.41/ethernet.1	media_port_max	57000
host_module.1/t38parameters	t38_fax_rate_management	transferredTCF
host_module.1/t38parameters	t38_fax_udp_ec	t38UDPRedundancy
host_module.1/t38parameters	t38_max_bit_rate	14400
host_module.1/t38parameters	t38_fax_version	0
host_module.1/t38parameters	t38_fax_fill_bit_removal	false
host_module.1/t38parameters	t38_fax_transcoding_jbig	false
host_module.1/t38parameters	t38_fax_transcoding_mmr	false
host_module.1/t38parameters	t38_fax_max_datagram	72
host_module.1/t38parameters	t38_fax_max_buffer	200

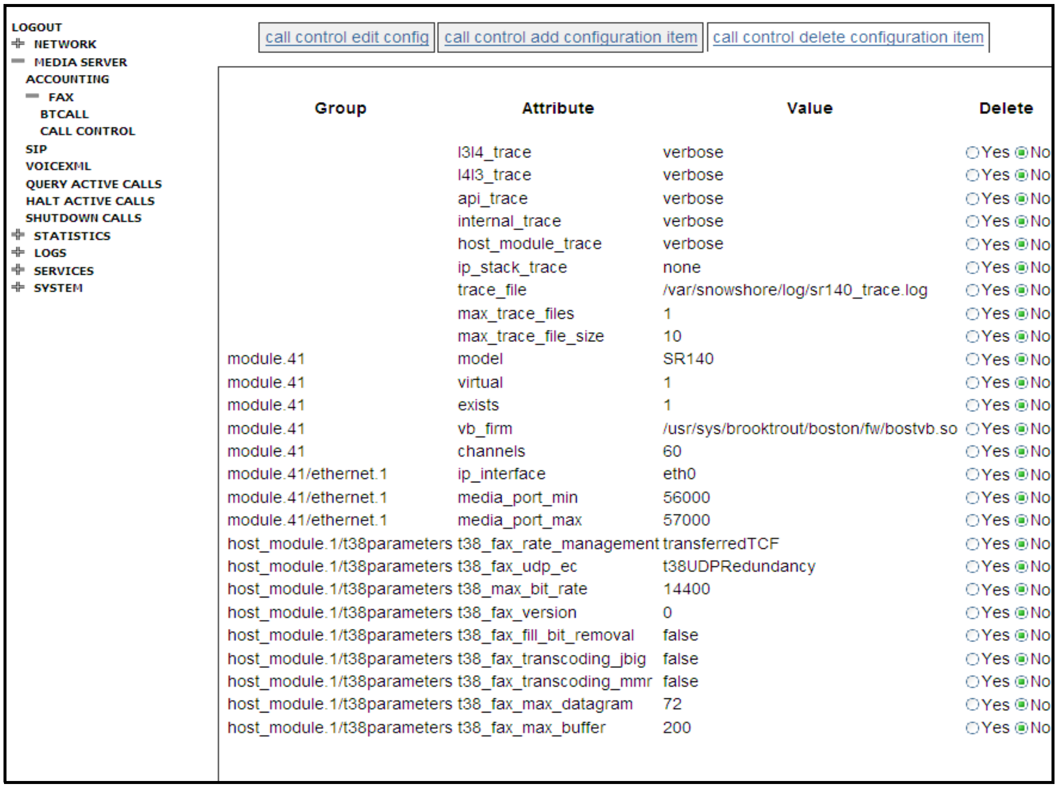
Figure 33. Add Call Control Configuration Item

2 At the bottom of the screen, complete the New Group, New Attribute, and New Value fields and click OK.

3 Repeat the step above until complete.

Deleting Call Control Attributes

1 Select FAX → CALL CONTROL and click the call control delete configuration item tab. The following screen appears.



Group	Attribute	Value	Delete
	l3l4_trace	verbose	○Yes ●No
	l4l3_trace	verbose	○Yes ●No
	api_trace	verbose	○Yes ●No
	internal_trace	verbose	○Yes ●No
	host_module_trace	verbose	○Yes ●No
	ip_stack_trace	none	○Yes ●No
	trace_file	/var/snowshore/log/sr140_trace.log	○Yes ●No
	max_trace_files	1	○Yes ●No
	max_trace_file_size	10	○Yes ●No
module.41	model	SR140	○Yes ●No
module.41	virtual	1	○Yes ●No
module.41	exists	1	○Yes ●No
module.41	vb_firm	/usr/sys/brooktrout/boston/fw/bostvb.so	○Yes ●No
module.41	channels	60	○Yes ●No
module.41/ethernet.1	ip_interface	eth0	○Yes ●No
module.41/ethernet.1	media_port_min	56000	○Yes ●No
module.41/ethernet.1	media_port_max	57000	○Yes ●No
host_module.1/t38parameters	t38_fax_rate_management	transferredTCF	○Yes ●No
host_module.1/t38parameters	t38_fax_udp_ec	t38UDPRedundancy	○Yes ●No
host_module.1/t38parameters	t38_max_bit_rate	14400	○Yes ●No
host_module.1/t38parameters	t38_fax_version	0	○Yes ●No
host_module.1/t38parameters	t38_fax_fill_bit_removal	false	○Yes ●No
host_module.1/t38parameters	t38_fax_transcoding_jbig	false	○Yes ●No
host_module.1/t38parameters	t38_fax_transcoding_mmr	false	○Yes ●No
host_module.1/t38parameters	t38_fax_max_datagram	72	○Yes ●No
host_module.1/t38parameters	t38_fax_max_buffer	200	○Yes ●No

Figure 34. Delete Call Control Configuration Item

2 Select Yes next to the attributes that you want to delete.

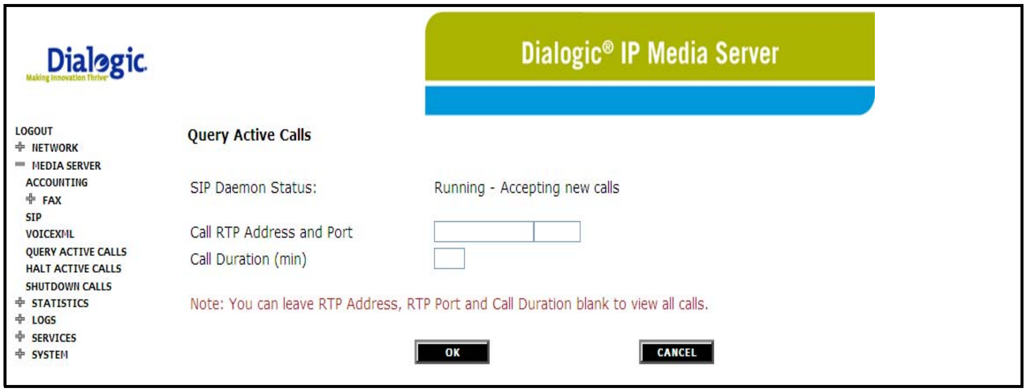
3 Click OK.

Query Active Calls

You can query for currently active calls on the IP Media Server. This enables you to determine if it is safe to change configuration settings.

1 Select MEDIA SERVER→QUERY ACTIVE CALLS from the menu.

The Query Active Calls page is displayed:



Query Active Calls

SIP Daemon Status: Running - Accepting new calls

Call RTP Address and Port

Call Duration (min)

Note: You can leave RTP Address, RTP Port and Call Duration blank to view all calls.

Figure 35. Query Active Calls Page

2 Enter the call RTP address and RTP port.

3 Enter the call duration. The IP Media Server returns all calls that have existed at least as long as the duration value (that is, all calls with times equal to or greater than the specified Duration).

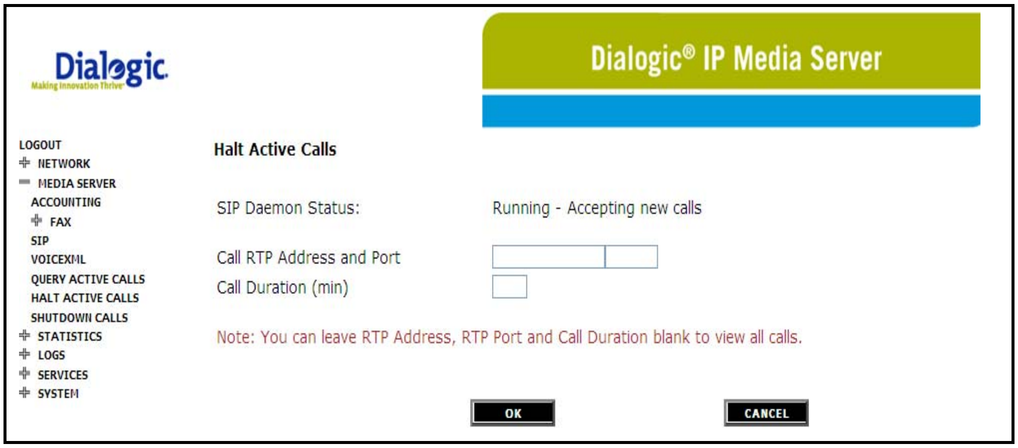
Note: To view all calls, leave the RTP Address, RTP Port, and Call Duration fields blank.

4 Click OK to get the results of the query.

Halt Active Calls

You can selectively stop currently active calls on the IP Media Server at any time. To halt active calls on the IP Media Server:

1 Select MEDIA SERVER→HALT ACTIVE CALLS from the menu to display the Halt Active Calls page:



Halt Active Calls

SIP Daemon Status: Running - Accepting new calls

Call RTP Address and Port

Call Duration (min)

Note: You can leave RTP Address, RTP Port and Call Duration blank to view all calls.

Figure 36. Halt Active Calls Page

2 Enter the call RTP address and RTP port.

3 Enter the call duration.

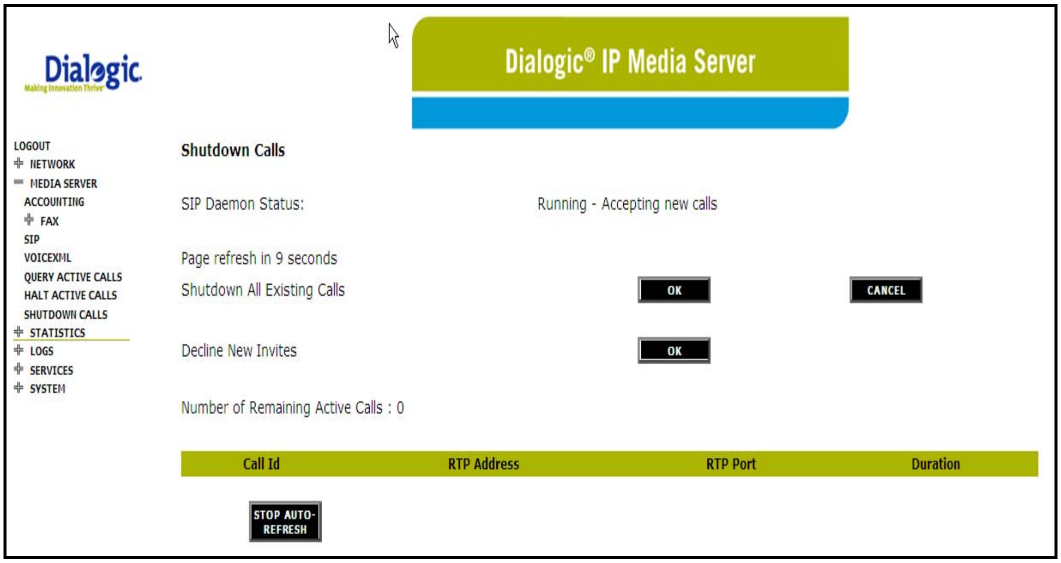
Note: To view all calls, leave the RTP Address, RTP Port, and Call Duration fields blank.

4 Click OK to get the results of the query.

5 Check the Select box for each call you want to halt and click OK to force the halt. The page re-displays, minus the halted calls.

Shutdown Calls

The Shutdown Calls feature blocks incoming call requests to the IP Media Server. This allows an administrator to reboot the server without losing any incoming calls. The Shutdown Calls page also enables an administrator to shutdown all existing calls.



Shutdown Calls

SIP Daemon Status: Running - Accepting new calls

Page refresh in 9 seconds

Shutdown All Existing Calls

Decline New Invites

Number of Remaining Active Calls : 0

Call Id	RTP Address	RTP Port	Duration

Figure 37. Shutdown Calls Page

To block new incoming calls, click OK adjacent to Decline New Invites. This causes the IP Media Server to stop accepting new calls. Active calls are not affected by this setting. After the page is refreshed, the option then changes to Accept New Invites, letting you re-enable the server to accept calls.

This page also enables you to shutdown all active calls.

- To selectively shut down calls, use the Halt Active Calls menu option.
- To shut down all calls, click the OK button adjacent to Shutdown All Existing Calls. The IP Media Server sends SIP BYE requests to terminate any existing calls.

5 - Operations, Administration, and Maintenance

This chapter describes procedures for operating, administering, and maintaining the IP Media Server.

This chapter includes the following sections:

- IP Media Server Statistics
- Logs Menu
- Services Menu
- The Dialogic® IP Media Server Private MIB
- System Menu
- Accounting Mechanism

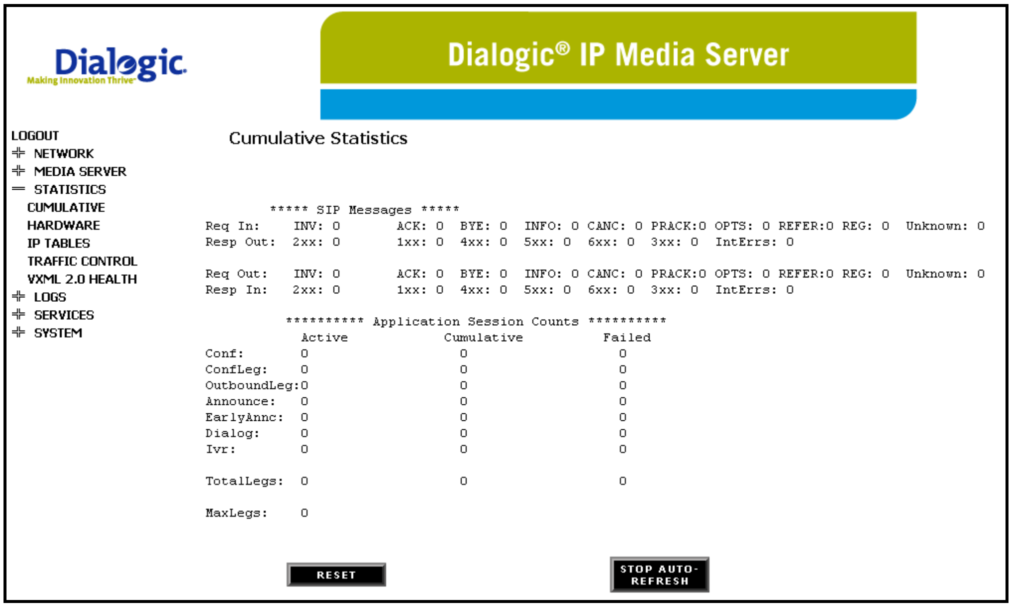
IP Media Server Statistics

The IP Media Server collects statistics associated with SIP messages and call attempts. It also gathers statistics on the server hardware.

Cumulative

To access the SIP message statistics:

1 Select CUMULATIVE. The number of SIP messages received and sent is shown.



Cumulative Statistics

```
         ***** SIP Messages *****
Req In:     INV: 0        ACK: 0  BYE: 0  INFO: 0 CANC: 0 PRACK:0 OPTS: 0 REFER:0 REG: 0  Unknown: 0
Resp Out:   2xx: 0        1xx: 0  4xx: 0  5xx: 0  6xx: 0  3xx: 0  IntErrs: 0

Req Out:    INV: 0        ACK: 0  BYE: 0  INFO: 0 CANC: 0 PRACK:0 OPTS: 0 REFER:0 REG: 0  Unknown: 0
Resp In:    2xx: 0        1xx: 0  4xx: 0  5xx: 0  6xx: 0  3xx: 0  IntErrs: 0

          ********** Application Session Counts **********
            Active              Cumulative           Failed
Conf:       0                   0                    0
ConfLeg:    0                   0                    0
OutboundLeg:0                   0                    0
Announce:   0                   0                    0
EarlyAnnc:  0                   0                    0
Dialog:     0                   0                    0
Ivr:        0                   0                    0

TotalLegs:  0                   0                    0

MaxLegs:    0
```

Figure 38. Cumulative Statistics Page

The IP Media Server also keeps statistics of call attempts for the supported application services. For each application service type, the statistics show:

- Active Calls—The number of currently active calls for each application service type.
- Cumulative Calls—The total number of call attempts for each application service type since the last reset of the statistics.
- Failed Calls—The total number of failed call attempts for each application service type since the last reset of the statistics.

The screen displays the total number of calls (Active, Cumulative, Failed) since the last reset of the statistics. This is shown at the bottom of the statistics screen and is labeled TotalLegs.

Note: The total does not include the Conf row, but does include the ConfLeg row. The Conf number is the number of unique conferences, not the number of calls in the conference.

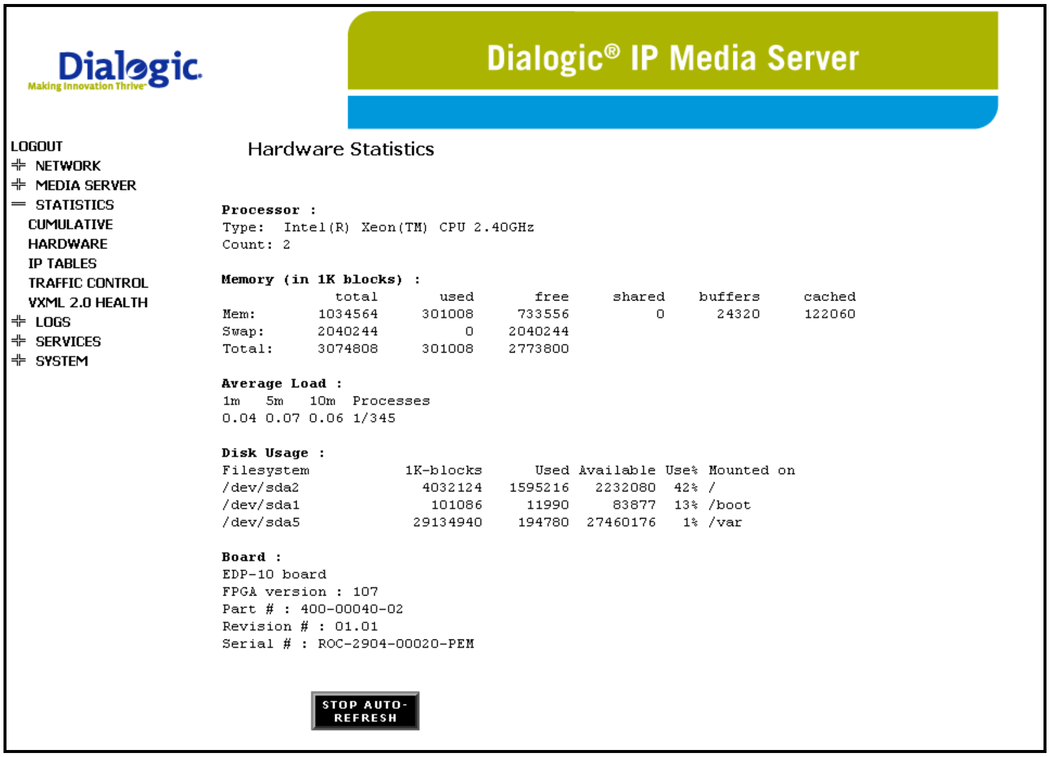
A high-water mark counter is found under the TotalLegs line and is called MaxLegs. This shows the highest number of simultaneously active calls on the IP Media Server since the last reset of the statistics.

2 To set the statistics to 0, click RESET.

Hardware

To access the hardware statistics, select Hardware to display the Hardware Statistics screen. This screen reflects the current status of the IP Media Server hardware. The hardware statistics include processor information, memory, average load of the system, disk usage of the system, and DSP board information, if one is installed.

The only option on this screen is to stop/start the auto refresh. To use this feature, click Stop Auto-Refresh to stop the screen from automatically refreshing. To restart auto-refresh, click Start Auto-Refresh.

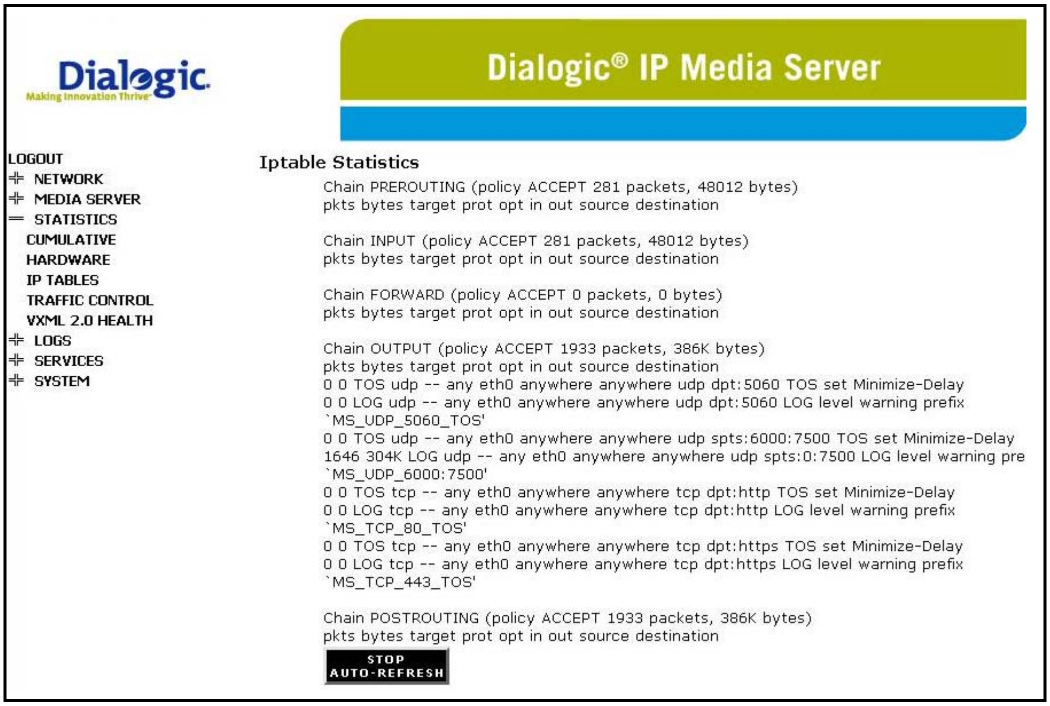


```
Processor :
Type:  Intel(R) Xeon(TM) CPU 2.40GHz
Count: 2

Memory (in 1K blocks) :
             total       used       free     shared    buffers     cached
Mem:       1034564     301008     733556          0      24320     122060
Swap:      2040244          0    2040244
Total:     3074808     301008    2773800

Average Load :
1m   5m   10m  Processes
0.04 0.07 0.06 1/345

Disk Usage :
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda2              4032124   1595216   2232080  42% /
/dev/sda1               101086     11990     83877  13% /boot
/dev/sda5             29134940    194780  27460176   1% /var

Board :
EDP-10 board
FPGA version : 107
Part # : 400-00040-02
Revision # : 01.01
Serial # : ROC-2904-00020-PEM
```

Figure 39. Hardware Statistics Page

IP Tables

The IP TABLES menu displays statistics for the IP Tables as shown in Figure 40. IP Tables are used to tag specific outgoing VoIP traffic.



Iptable Statistics

```
Chain PREROUTING (policy ACCEPT 281 packets, 48012 bytes)
pkts bytes target prot opt in out source destination

Chain INPUT (policy ACCEPT 281 packets, 48012 bytes)
pkts bytes target prot opt in out source destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 1933 packets, 386K bytes)
pkts bytes target prot opt in out source destination
0 0 TOS udp -- any eth0 anywhere anywhere udp dpt:5060 TOS set Minimize-Delay
0 0 LOG udp -- any eth0 anywhere anywhere udp dpt:5060 LOG level warning prefix
`MS_UDP_5060_TOS'
0 0 TOS udp -- any eth0 anywhere anywhere udp spts:6000:7500 TOS set Minimize-Delay
1646 304K LOG udp -- any eth0 anywhere anywhere udp spts:0:7500 LOG level warning pre
`MS_UDP_6000:7500'
0 0 TOS tcp -- any eth0 anywhere anywhere tcp dpt:http TOS set Minimize-Delay
0 0 LOG tcp -- any eth0 anywhere anywhere tcp dpt:http LOG level warning prefix
`MS_TCP_80_TOS'
0 0 TOS tcp -- any eth0 anywhere anywhere tcp dpt:https TOS set Minimize-Delay
0 0 LOG tcp -- any eth0 anywhere anywhere tcp dpt:https LOG level warning prefix
`MS_TCP_443_TOS'

Chain POSTROUTING (policy ACCEPT 1933 packets, 386K bytes)
pkts bytes target prot opt in out source destination
```

Figure 40. IP Table Statistics Page

The following are key points from these statistics:

- The line below indicates to set the TOS (Type of Service) bit for all UDP traffic on eth0 where the destination port is 5060 (SIP) to be Minimum delay.

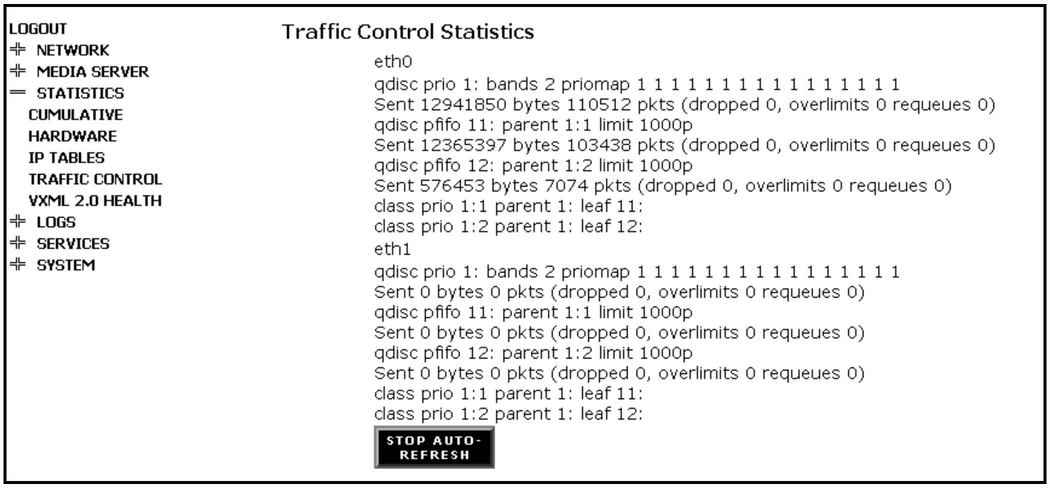
```
0 0 TOS udp -- any eth0 anywhere anywhere udp dpt:5060 TOS set Minimize-Delay
```

- The next line indicates to log this information.

```
0 0 LOG udp -- any eth0 anywhere anywhere udp dpt:5060 LOG level warning prefix
```

Traffic Control

The Traffic Control menu displays statistics for the Traffic Control as shown in Figure 41. Traffic Control application allows the IP Media Server to prioritize incoming traffic.



Traffic Control Statistics

```
eth0
qdisc prio 1: bands 2 priomap 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Sent 12941850 bytes 110512 pkts (dropped 0, overlimits 0 requeues 0)
qdisc pfifo 11: parent 1:1 limit 1000p
Sent 12365397 bytes 103438 pkts (dropped 0, overlimits 0 requeues 0)
qdisc pfifo 12: parent 1:2 limit 1000p
Sent 576453 bytes 7074 pkts (dropped 0, overlimits 0 requeues 0)
class prio 1:1 parent 1: leaf 11:
class prio 1:2 parent 1: leaf 12:
eth1
qdisc prio 1: bands 2 priomap 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Sent 0 bytes 0 pkts (dropped 0, overlimits 0 requeues 0)
qdisc pfifo 11: parent 1:1 limit 1000p
Sent 0 bytes 0 pkts (dropped 0, overlimits 0 requeues 0)
qdisc pfifo 12: parent 1:2 limit 1000p
Sent 0 bytes 0 pkts (dropped 0, overlimits 0 requeues 0)
class prio 1:1 parent 1: leaf 11:
class prio 1:2 parent 1: leaf 12:
```

Figure 41. Traffic Control Statistics Page

The following are key points from these statistics:

- This line is all the traffic seen on eth0:

```
qdisc prio 1: bands 2 priomap 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
```

- "Sent" means allowed or passed or seen:

```
Sent 5578871 bytes 27740 pkts (dropped 0, overlimits 0 requeues 0)
```

- This line is the filter for VOIP traffic incoming:

```
qdisc pfifo 11: parent 1:1 limit 1000p
```

- All traffic in this case was VOIP and was passed on up:

```
Sent 5533101 bytes 27477 pkts (dropped 0, overlimits 0 requeues 0)
```

- The following line is all non-VOIP traffic:

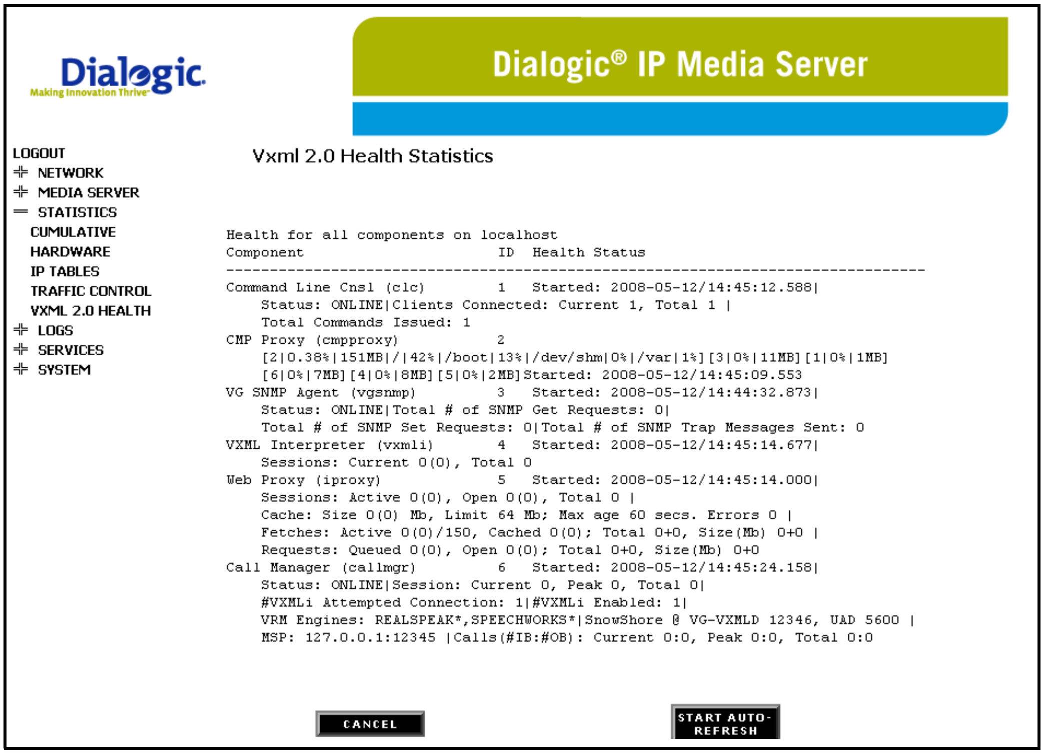
```
qdisc pfifo 12: parent 1:2 limit 1000p
```

- This traffic took the slow path in the IP Media Server as it is not as important

```
Sent 45770 bytes 263 pkts (dropped 0, overlimits 0 requeues 0)
```

VXML 2.0 Health

The VXML 2.0 Health menu displays system health information for VXML 2.0, as shown in Figure 42. This information can be useful for troubleshooting a VXML 2.0 configuration or application issue.



Vxml 2.0 Health Statistics

```
Health for all components on localhost
Component                      ID  Health Status
--------------------------------------------------------------------------------
Command Line Cnsl (clc)        1   Started: 2008-05-12/14:45:12.588|
    Status: ONLINE|Clients Connected: Current 1, Total 1 |
    Total Commands Issued: 1
CMP Proxy (cmpproxy)           2
    [2|0.38%|151MB|/|42%|/boot|13%|/dev/shm|0%|/var|1%][3|0%|11MB][1|0%|1MB]
    [6|0%|7MB][4|0%|8MB][5|0%|2MB]Started: 2008-05-12/14:45:09.553
VG SNMP Agent (vgsnmp)         3   Started: 2008-05-12/14:44:32.873|
    Status: ONLINE|Total # of SNMP Get Requests: 0|
    Total # of SNMP Set Requests: 0|Total # of SNMP Trap Messages Sent: 0
VXML Interpreter (vxmli)       4   Started: 2008-05-12/14:45:14.677|
    Sessions: Current 0(0), Total 0
Web Proxy (iproxy)             5   Started: 2008-05-12/14:45:14.000|
    Sessions: Active 0(0), Open 0(0), Total 0 |
    Cache: Size 0(0) Mb, Limit 64 Mb; Max age 60 secs. Errors 0 |
    Fetches: Active 0(0)/150, Cached 0(0); Total 0+0, Size(Mb) 0+0 |
    Requests: Queued 0(0), Open 0(0); Total 0+0, Size(Mb) 0+0
Call Manager (callmgr)         6   Started: 2008-05-12/14:45:24.158|
    Status: ONLINE|Session: Current 0, Peak 0, Total 0|
    #VXMLi Attempted Connection: 1|#VXMLi Enabled: 1|
    VRM Engines: REALSPEAK*,SPEECHWORKS*|SnowShore @ VG-VXMLD 12346, UAD 5600 |
    MSP: 127.0.0.1:12345 |Calls(#IB:#OB): Current 0:0, Peak 0:0, Total 0:0
```

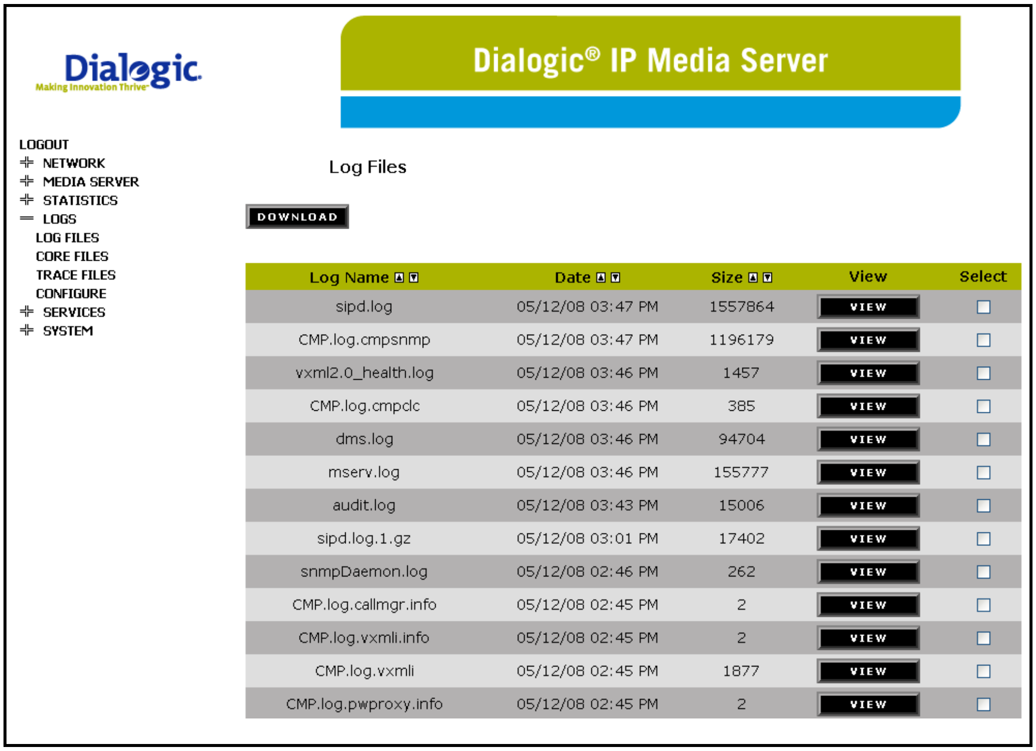
Figure 42. VXML 2.0 Health Statistics Page

Logs Menu

The Logs menu includes commands for configuring system logs, and viewing log files, core files, and trace files.

Log Files

There are several log files generated by the IP Media Server. The IP Media Server logs are listed in the Log Files screen.



Log Files

Log Name ▲▼	Date ▲▼	Size ▲▼	View	Select
sipd.log	05/12/08 03:47 PM	1557864	VIEW	□
CMP.log.cmpsnmp	05/12/08 03:47 PM	1196179	VIEW	□
vxml2.0_health.log	05/12/08 03:46 PM	1457	VIEW	□
CMP.log.cmpclc	05/12/08 03:46 PM	385	VIEW	□
dms.log	05/12/08 03:46 PM	94704	VIEW	□
mserv.log	05/12/08 03:46 PM	155777	VIEW	□
audit.log	05/12/08 03:43 PM	15006	VIEW	□
sipd.log.1.gz	05/12/08 03:01 PM	17402	VIEW	□
snmpDaemon.log	05/12/08 02:46 PM	262	VIEW	□
CMP.log.callmgr.info	05/12/08 02:45 PM	2	VIEW	□
CMP.log.vxmli.info	05/12/08 02:45 PM	2	VIEW	□
CMP.log.vxmli	05/12/08 02:45 PM	1877	VIEW	□
CMP.log.pwproxy.info	05/12/08 02:45 PM	2	VIEW	□

Figure 43. Log Files Page

The IP Media Server generates the following logs:

Table 14. IP Media Server Logs

Name[a]	Contents
<hostname>_system_info.log	Configuration for the IP Media Server as well as the computer hardware.
audit.log	All of the SNMP sets and user configuration changes made through the Web interface.
cache.log	Squid cache processes.
cache_access.log	Squid cache accesses.

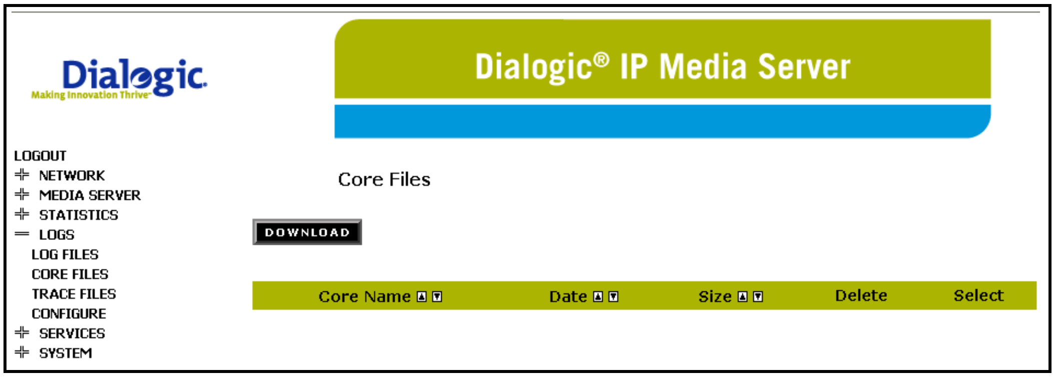
Table 14. IP Media Server Logs (Continued)

Name[a]	Contents
dms.log	Internal messages on the IP Media Server dealing with host software-to-DSP card interactions.
email_to_fax.log	Logs email to fax traffic
fido.log	Messages associated with fetching Internet domain objects (files, vxml pages over http).
messages.log	SIPD and UAD messages written when the Syslog option is enabled.
mserv.log	Details of creating and managing RTP streams on the IP Media Server.
msinit.log	Watchdog information about the Mserv and MSprovider processes.
msprovider.log	Information about license transactions.
sipd.log	SIP messages received and sent by the IP Media Server.
snmpDaemon.log	All output from snmpDaemon.
sr140app.log	Logs fax traffic
uad.log	Internal messages associated with VoiceXML 1.0 transfer functions.
vxmld.log	VoiceXML 1.0 messages on the IP Media Server.
vxml2d.log	Contains informatin logged by VXML 2.0 browser.
mrcpapp.log	Contains information logged about the interaction between the mrchapp and voice xml layers
MrcpClientLibrary.log	Contains information logged about MRCP activity.

[a] See also “Log Naming Convention” (page 114).

Core Files

Core files appear in this view when a failure has occurred. The Core Files contains a memory image of the terminated process. These files are useful in debugging.



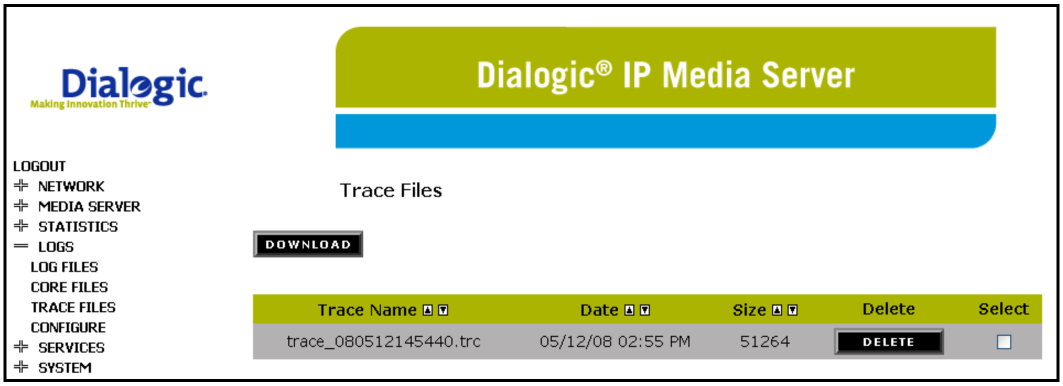
Core Files

Core Name	Date	Size	Delete	Select

Figure 44. Core Files Page

Trace Files

This window lists the output files from the trace feature (NETWORKS → UTILITIES → TRACE) on the IP Media Server. These files can be opened using network analyzer software.



Trace Files

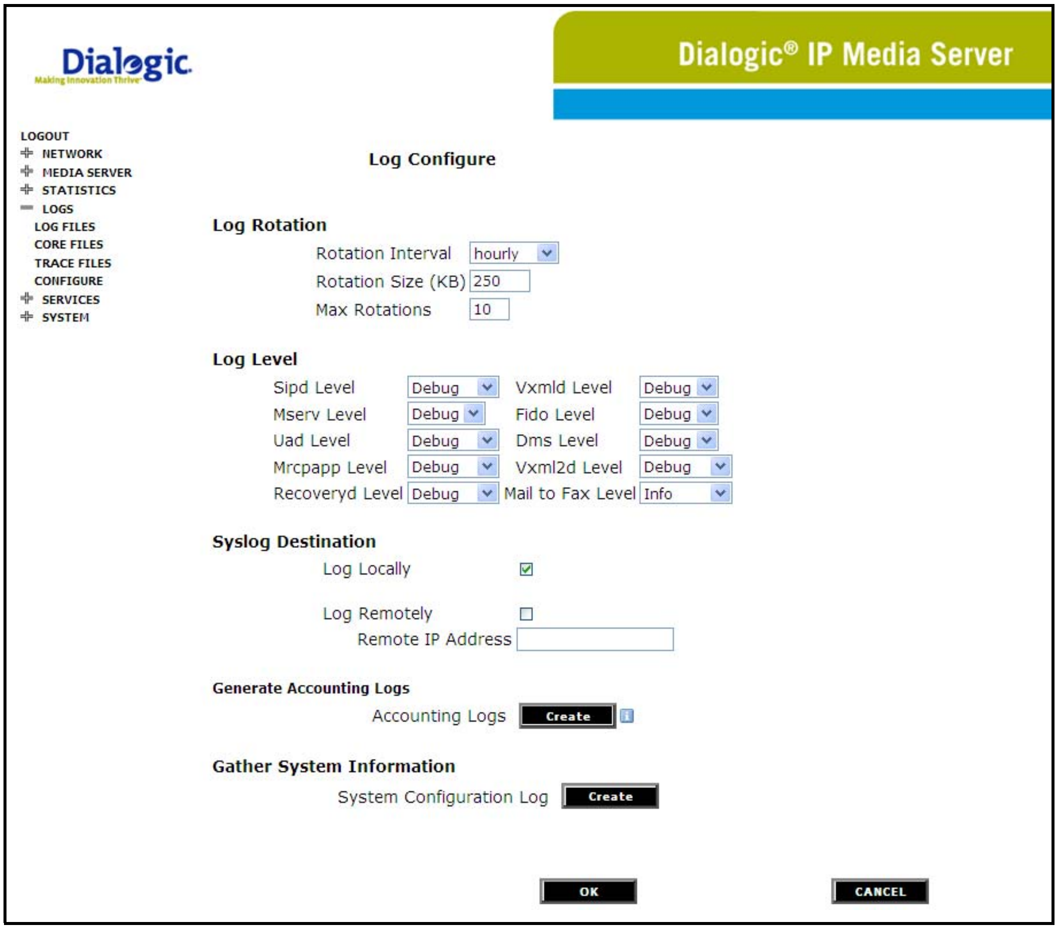
Trace Name	Date	Size	Delete	Select
trace_080512145440.trc	05/12/08 02:55 PM	51264	DELETE	□

Figure 45. Trace Files Page

Configure Logs

The log system is controlled by a set of parameters you configure using the LOGS→CONFIGURE menu.

Note: Only Administrators can configure the log system.



Log Configure

Log Rotation

Rotation Interval: hourly
Rotation Size (KB): 250
Max Rotations: 10

Log Level

Sipd Level	Debug	Vxmld Level	Debug
Mserv Level	Debug	Fido Level	Debug
Uad Level	Debug	Dms Level	Debug
Mrcpapp Level	Debug	Vxml2d Level	Debug
Recoveryd Level	Debug	Mail to Fax Level	Info

Syslog Destination

Log Locally ☑

Log Remotely ☐
Remote IP Address

Generate Accounting Logs

Accounting Logs

Gather System Information

System Configuration Log

Figure 46. Log Configure Page

Log Rotation

Note: If you change the log rotation values from the defaults, do not exceed file sizes of 2GB or available disk storage space.

Table 15. Log Rotation Parameters

Parameter	Values	Description
Rotation Interval	◆ Monthly ◆ Weekly ◆ Daily ◆ Hourly ◆ 30 minutes ◆ 15 minutes (Default : Hourly)	Interval at which the log files are checked for rotation. The interval can be: ◆ Monthly (at 4:42 AM, the first day of the month) ◆ Weekly (at 4:22 AM, first day of the week) ◆ Daily (at 4:02 AM) ◆ Hourly (at the top of the hour) ◆ 30 minutes ◆ 15 minutes
Rotation Size	integer: 1–250,000 (Default: 250)	Minimum size (in kilobytes) that a log file must be to be rotated at the next rotation interval. **Note:** Logs are rotated based on their size when they are checked. If you want the logs to be rotated at the interval chosen, make the rotation size small. **Caution:** Specifying a large rotation size creates very large log files which take longer to view and download. For maximum system efficiency, set rotation sizes to less than 50,000 KB.
Max Rotations	integer: 1–240 (Default: 10)	Number of rotations allowed for each log file. This determines how many log files are kept on the system before they are deleted.

Note: The log configuration parameters do not apply to the VXML 2.0 logs. These logs are preconfigured to have a maximum rotation size of 10MB and a maximum of 5 rotations.

Log Level

The Log Level section of the Log Configure screen enables you to configure the level of detail to be included in each log. Select the level of detail to record for each log from the drop-down list.

Table 16. Log Level Parameters

Level	Log Contents
Debug	All messages associated with a process. A log event that denotes information that is only required for component-level debugging.
Info	Informative messages regarding a process.
Warning	All warning messages about normal events associated with a process.
Error	All errors encountered by a process.
Critical	All critical messages generated by a process.
Fatal	Fatal messages associated with a process that denote an error condition that should never happen and that results in the loss of functionality.
None	No information is logged.

Syslog Destination

This option determines where syslog information will be saved.

Table 17. Syslog Destination Parameters

Parameter	Description
Log Locally	Logs the syslog information to the message.log file on the IP Media Server.
Log Remotely	Logs the syslog information to a remote system. Enter the IP address of the remote system in the Remote IP Address field.

Table 17. Syslog Destination Parameters

Parameter	Description
Generate Log Button	The Generate Log Button creates the accounting.log and the msaccounting.log files. The accounting.log is the clear xml formatted ascii text file for looking at the IP Media Server's Accounting Statistics over time. The msaccounting.log is the encrypted xml formatted Log file used for debug purposes.

Gather System Information

This option creates the System Configuration Log for the current system. This information includes system and IP Media Server configuration information. Once you click CREATE, the log file is generated and the Web page is redirected to the log files page. This new log file can be downloaded and sent to Dialogic Technical Support to aid in debugging software issues.

Log Naming Convention

Logs are configured to rotate based on a size parameter that is set in the LOG→CONFIGURE command. The convention for naming log files is <log file name>.log.n where n is changed every time a new log file is started. The current log file being used does not have an n extension. For example, the following logs might be found on the system:

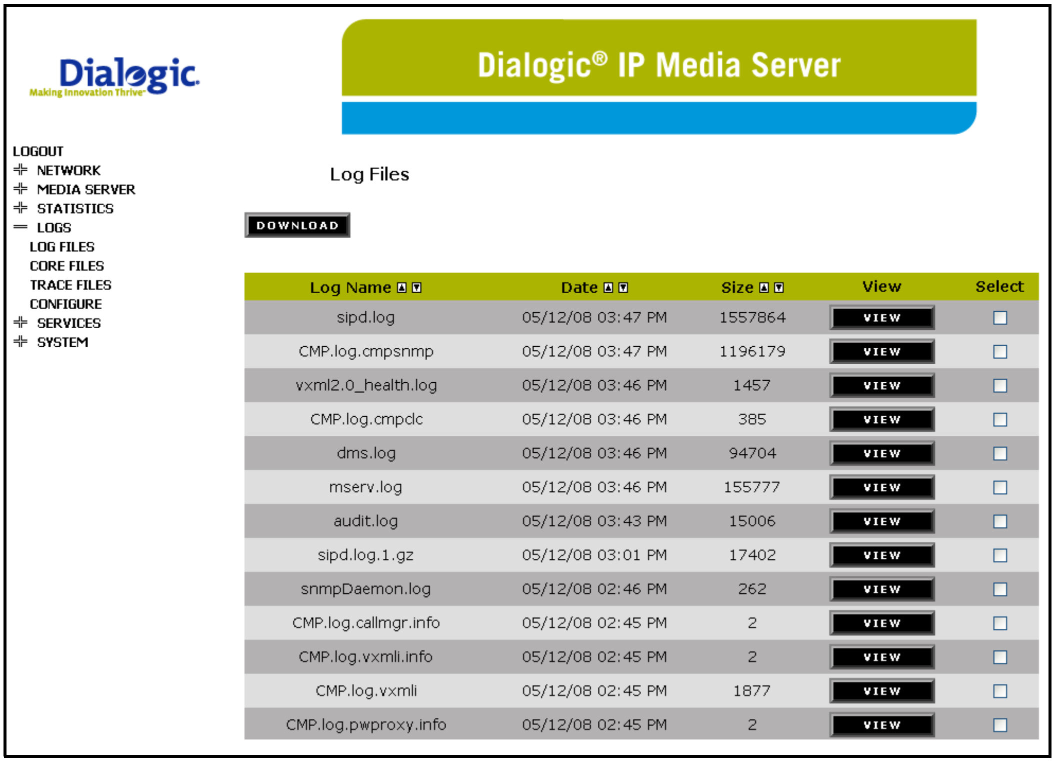
- sipd.log: the current sip log.
- sipd.log.1: the most recent sip log that was rotated.
- sipd.log.2: the next most recent sip log that was rotated.

.
.
.

- sipd.log.n: the sip log from n rotations ago, where n is the number of rotations.

Viewing and Downloading Logs

To view or download the log files, select LOGS→LOG FILES to display the Log Files page, which displays the available log files and the date/time they were last modified.



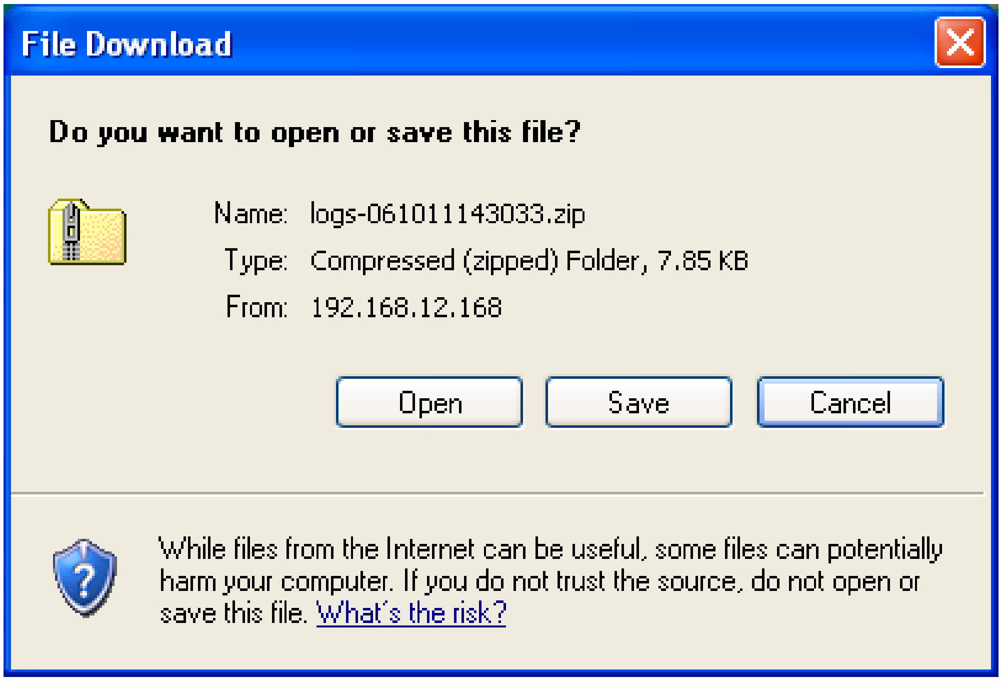
Log Name	Date	Size	View	Select
sipd.log	05/12/08 03:47 PM	1557864	VIEW	□
CMP.log.cmpsnmp	05/12/08 03:47 PM	1196179	VIEW	□
vxml2.0_health.log	05/12/08 03:46 PM	1457	VIEW	□
CMP.log.cmpclc	05/12/08 03:46 PM	385	VIEW	□
dms.log	05/12/08 03:46 PM	94704	VIEW	□
mserv.log	05/12/08 03:46 PM	155777	VIEW	□
audit.log	05/12/08 03:43 PM	15006	VIEW	□
sipd.log.1.gz	05/12/08 03:01 PM	17402	VIEW	□
snmpDaemon.log	05/12/08 02:46 PM	262	VIEW	□
CMP.log.callmgr.info	05/12/08 02:45 PM	2	VIEW	□
CMP.log.vxmli.info	05/12/08 02:45 PM	2	VIEW	□
CMP.log.vxmli	05/12/08 02:45 PM	1877	VIEW	□
CMP.log.pwproxy.info	05/12/08 02:45 PM	2	VIEW	□

Figure 47. Log Files Page

To download a file or files:

1 Click the checkbox(es) next to the file(s) you want to download.

2 Click DOWNLOAD at the top of the page. The selected file(s) are compressed into a ZIP file and the File Download screen appears with the name of the ZIP file:



Do you want to open or save this file?

Name: logs-061011143033.zip

Type: Compressed (zipped) Folder, 7.85 KB

From: 192.168.12.168

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Figure 48. Downloading a Log File

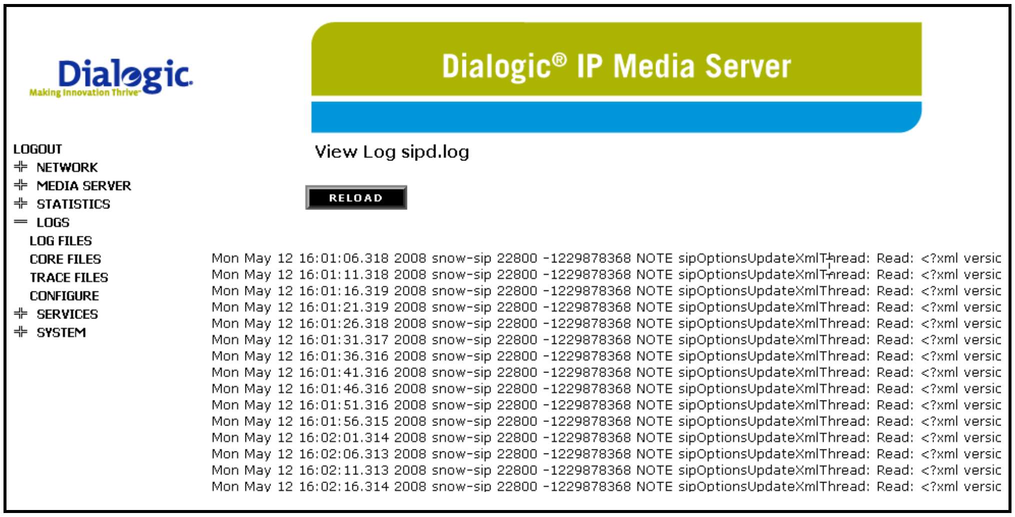
3 Select the preferred action:

- Open - Displays the a window to enable you to manipulate the log files.
- Save - Displays a window to enable you to select a location to save the log file.

To view a log file:

1 Click the VIEW button for that file.

This displays the log file in the display frame of the Web User Interface. If a file is being viewed on the browser, the standard browser finds tools that can be used.

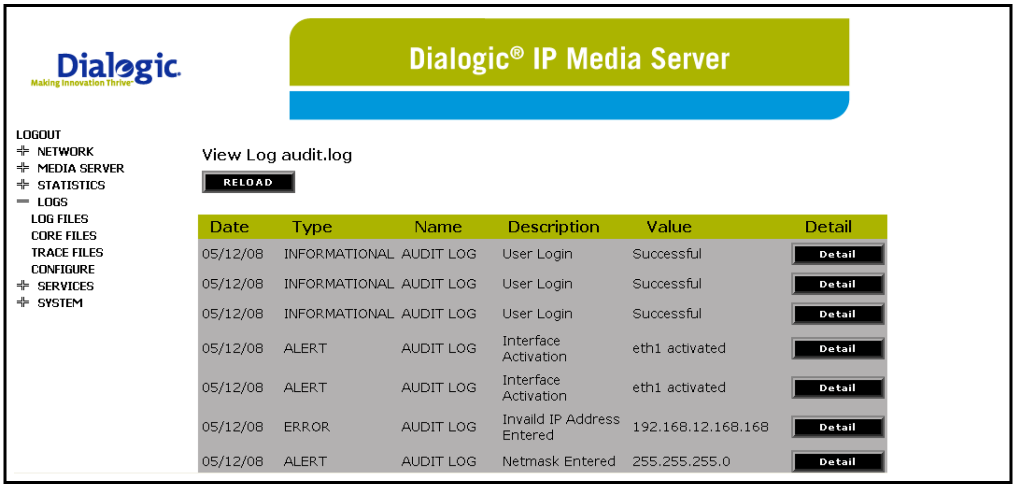


View Log sipd.log

```
Mon May 12 16:01:06.318 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:11.318 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:16.319 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:21.319 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:26.318 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:31.317 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:36.316 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:41.316 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:46.316 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:51.316 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:01:56.315 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:02:01.314 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:02:06.313 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:02:11.313 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
Mon May 12 16:02:16.314 2008 snow-sip 22800 -1229878368 NOTE sipOptionsUpdateXmlThread: Read: <?xml versic
```

Figure 49. Viewing Log File

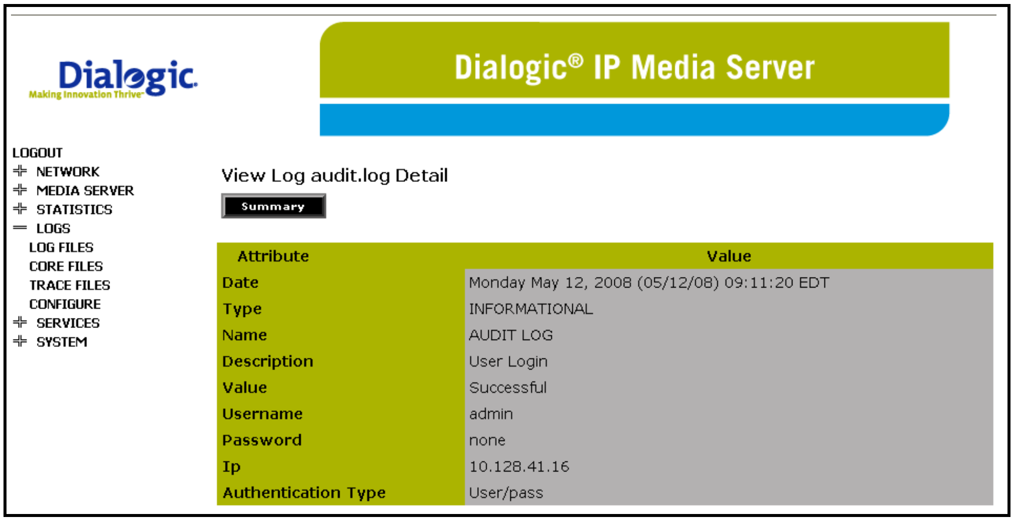
The audit log has a special table view:



View Log audit.log

Date	Type	Name	Description	Value	Detail
05/12/08	INFORMATIONAL	AUDIT LOG	User Login	Successful	Detail
05/12/08	INFORMATIONAL	AUDIT LOG	User Login	Successful	Detail
05/12/08	INFORMATIONAL	AUDIT LOG	User Login	Successful	Detail
05/12/08	ALERT	AUDIT LOG	Interface Activation	eth1 activated	Detail
05/12/08	ALERT	AUDIT LOG	Interface Activation	eth1 activated	Detail
05/12/08	ERROR	AUDIT LOG	Invaild IP Address Entered	192.168.12.168.168	Detail
05/12/08	ALERT	AUDIT LOG	Netmask Entered	255.255.255.0	Detail

1 To view the details of an entry from the audit log file, click the DETAIL button for that entry.

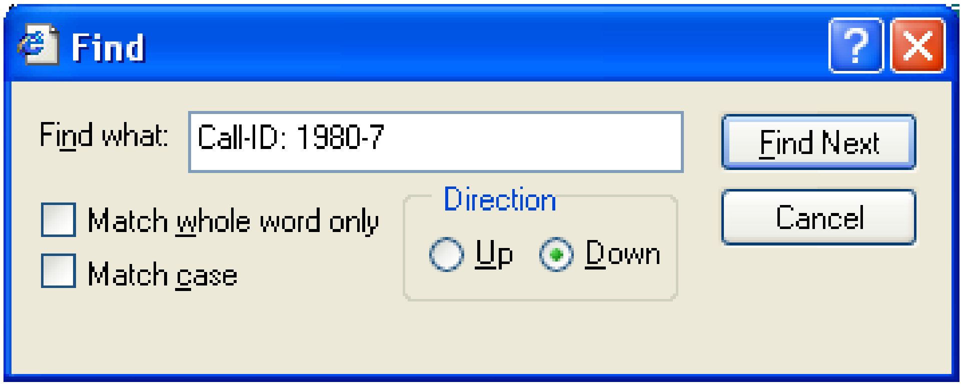


View Log audit.log Detail

Attribute	Value
Date	Monday May 12, 2008 (05/12/08) 09:11:20 EDT
Type	INFORMATIONAL
Name	AUDIT LOG
Description	User Login
Value	Successful
Username	admin
Password	none
Ip	10.128.41.16
Authentication Type	User/pass

Figure 50. Audit Log Detail Page

2 To search for a particular word or character string, use the browser Edit→Find dialog.



Find what: Call-ID: 1980-7

□ Match whole word only

□ Match case

Direction: ○ Up ● Down

Figure 51. Searching in a Log File

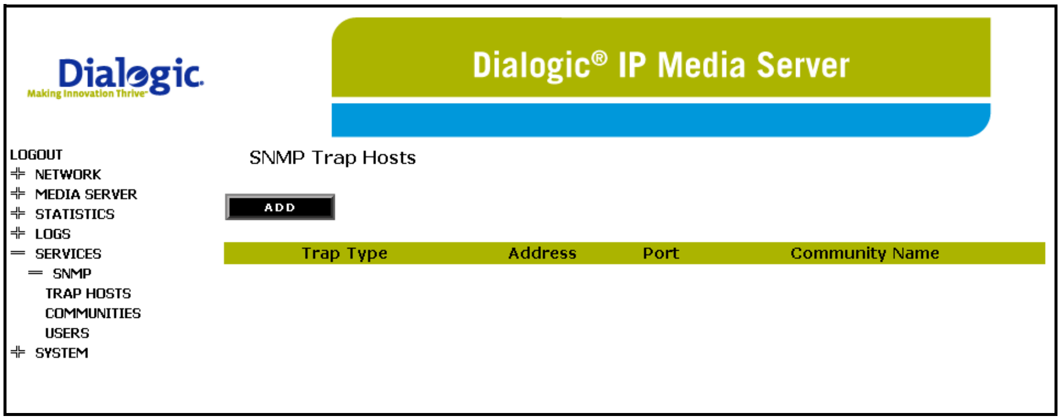
Services Menu

The Services menu options provide commands for configuring the SNMP functionality. Under the IP Media Server implementation of SNMP, users can add traps, communities, and users.

Note: Only Administrators have the permissions to configure the SNMP utility.

SNMP Trap Hosts

In this screen, administrators can add and delete trap hosts for the IP Media Server.



SNMP Trap Hosts

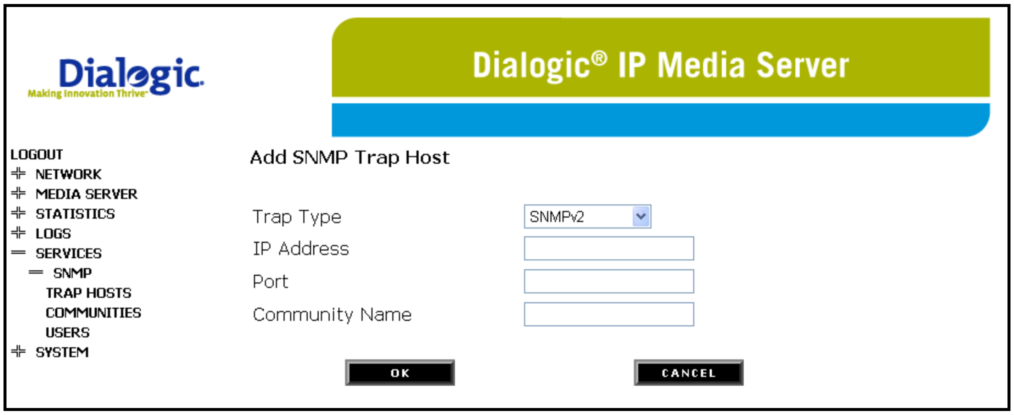
Trap Type	Address	Port	Community Name

Figure 52. SNMP Trap Hosts Page

To add a new trap host:

1 Click ADD.

The Add SNMP Trap Host page appears.



Add SNMP Trap Host

Trap Type SNMPv2
IP Address
Port
Community Name

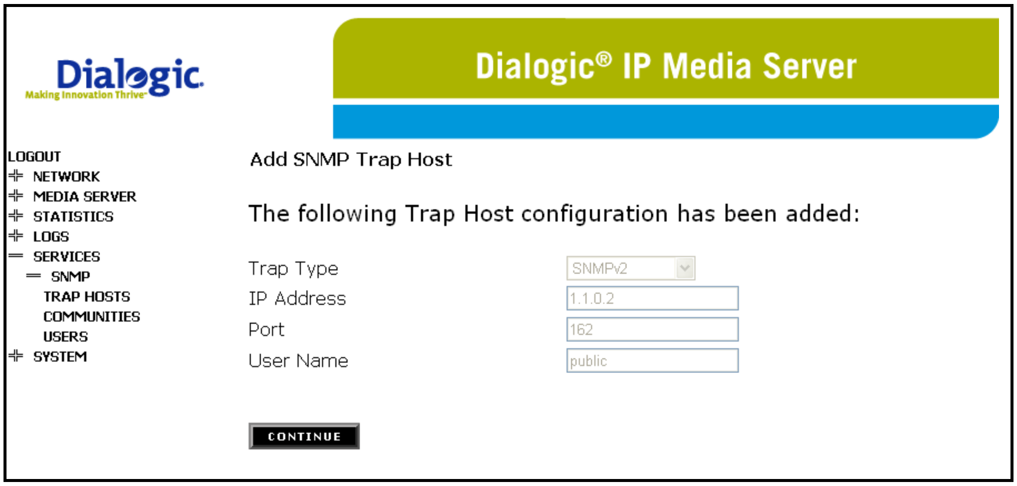
Figure 53. Add SNMP Trap Host Page

2 Select the trap type from the pull-down menu.

3 Enter the IP address.

4 Enter the Port and Community Name. These are optional. If not specified, the Port defaults to 162 and the Community defaults to Public.

5 Click OK. The next screen shows the new trap.



Add SNMP Trap Host

The following Trap Host configuration has been added:

Trap Type	SNMPv2
IP Address	1.1.0.2
Port	162
User Name	public

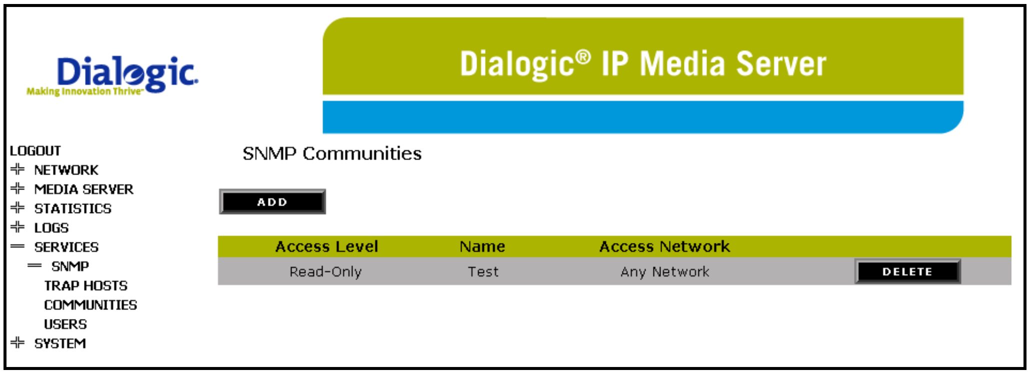
Figure 54. Add SNMP Trap Host Confirmation Page

SNMP Communities

In this screen, administrators can add and delete SNMP Communities for the IP Media Server. You can use the SNMP Community Names to manage the System from either an SNMPv1 or SNMPv2c management level.

To add a read/write community:

1 Click on the SERVICES→SNMP→COMMUNITIES options in the menu to display the SNMP Communities screen.

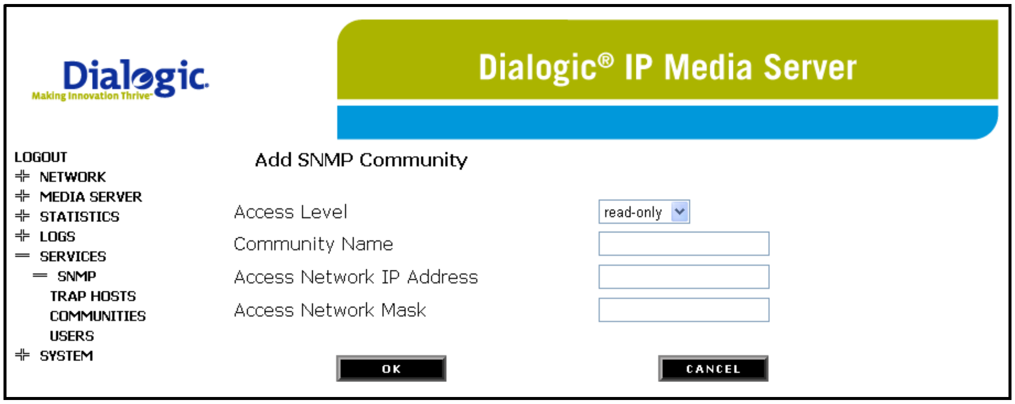


SNMP Communities

Access Level	Name	Access Network
Read-Only	Test	Any Network

Figure 55. SNMP Communities Page

2 Click ADD to display the Add SNMP Community page.



Add SNMP Community

Access Level	read-only
Community Name	
Access Network IP Address	
Access Network Mask	

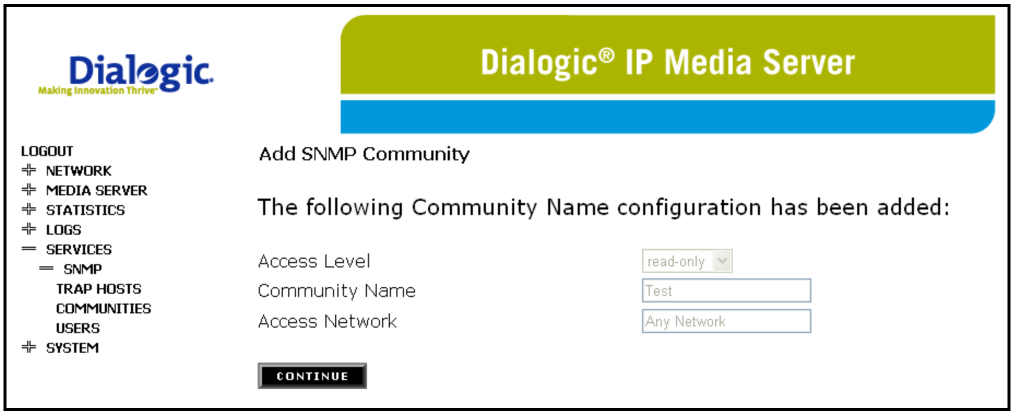
Figure 56. Add SNMP Community Page

3 Choose the access level as read-write.

4 Fill in the Community Name.

5 Leave the Access Network IP address and Access Network Mask fields blank.

6 Click OK when you are done. The following confirmation screen appears.



Add SNMP Community

The following Community Name configuration has been added:

Access Level	read-only
Community Name	Test
Access Network	Any Network

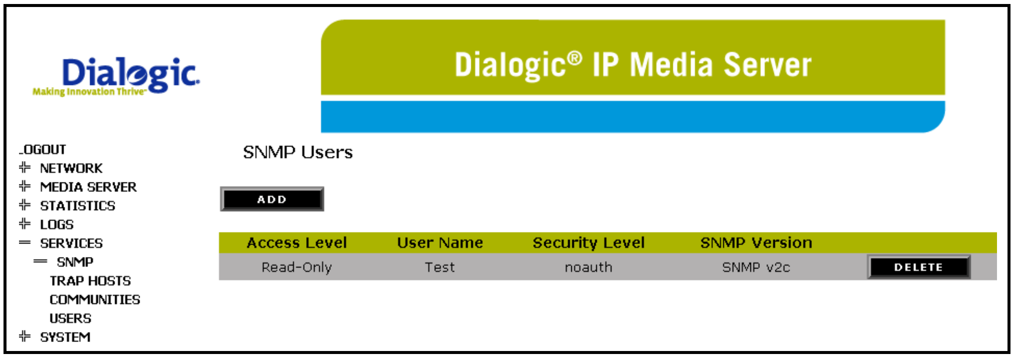
Figure 57. Add SNMP Community Confirmation Page

7 Click Continue to return to the SNMP Communities page.

SNMP Users

To add a read/write user:

1 Select the menu option SERVICES→SNMP→USERS to display the SNMP Users page.

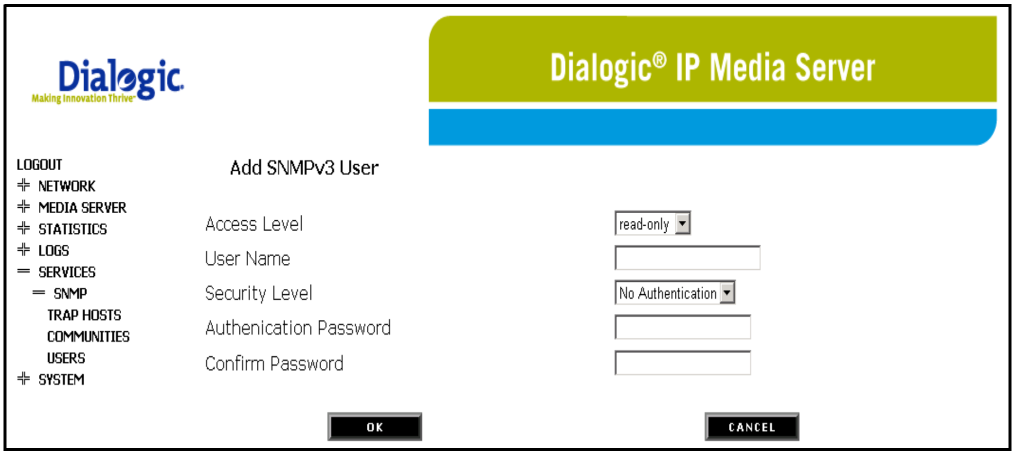


SNMP Users

Access Level	User Name	Security Level	SNMP Version	
Read-Only	Test	noauth	SNMP v2c	DELETE

Figure 58. SNMP Users Page

2 Click ADD to display the ADD SNMP User page.



Add SNMPv3 User

Access Level: read-only

User Name:

Security Level: No Authentication

Authenication Password:

Confirm Password:

Figure 59. Add SNMP User Page

3 Select the access level from the pull-down menu.

The choices are: read-only [default] and read-write.

4 Enter the new user name.

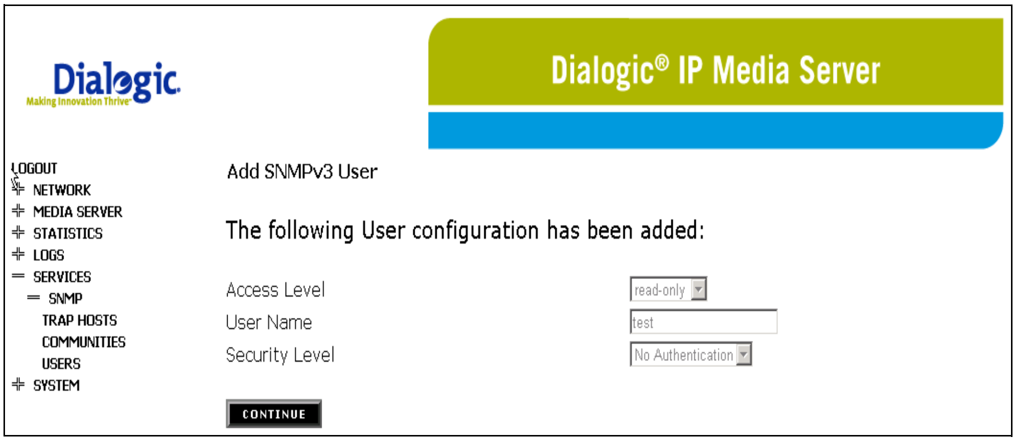
5 Select the security level from the pull-down menu.

The choices are: No Authentication [default] and Authenticated.

6 If the user is authenticated, enter the password and confirm. Leave the password blank if the user is not authenticated.

7 Click OK to continue.

The following screen appears to confirm the user changes.



Add SNMPv3 User

The following User configuration has been added:

Access Level: read-only

User Name: test

Security Level: No Authentication

Figure 60. Add SNMP User Confirmation Page

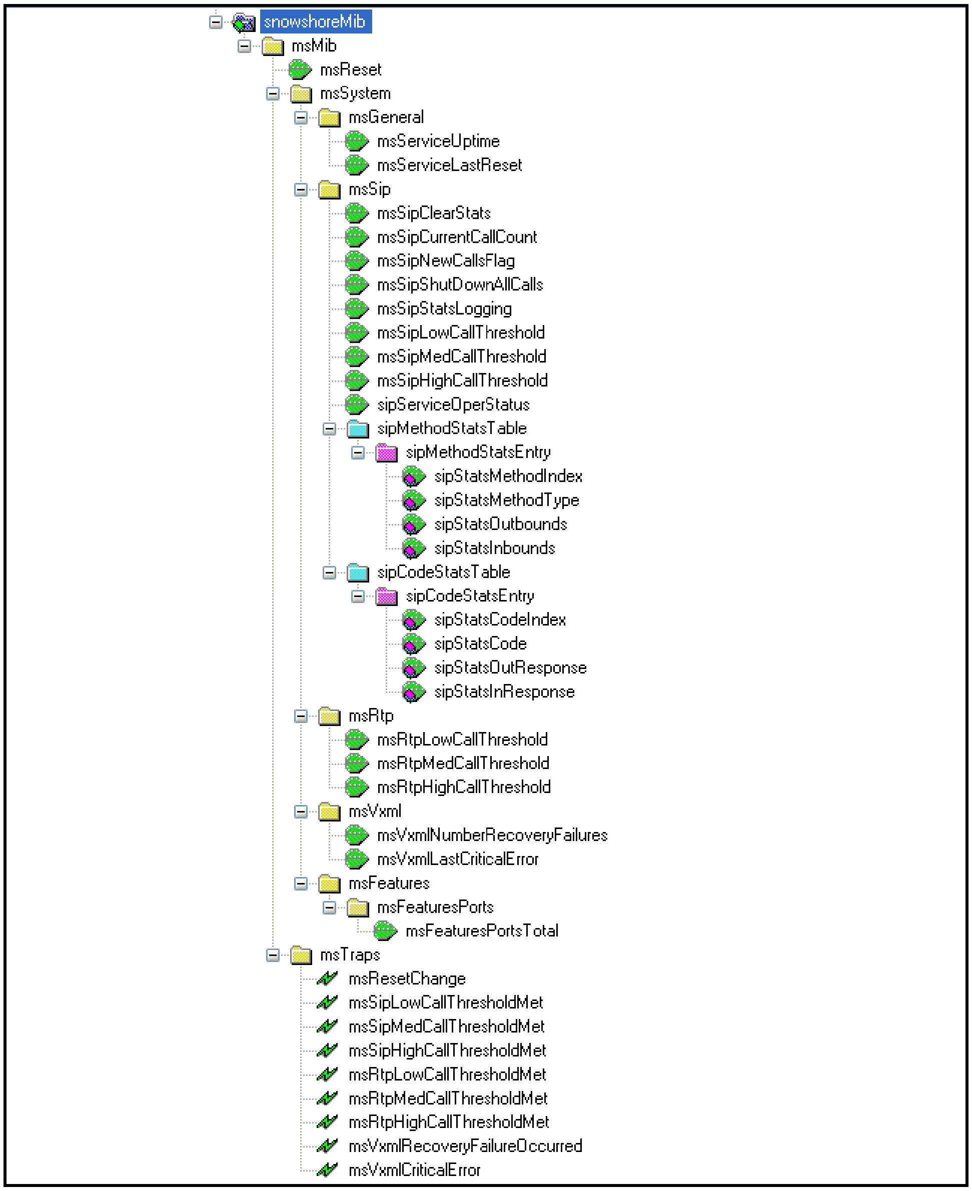
8 Click Continue to return to the SNMP Users page.

The Dialogic® IP Media Server Private MIB

The MIB Structure

The MIB (Management Information Base) structure in the IP Media Server is based on Net-SNMP. A private MIB gathers information about the IP Media Server and controls some of the functionality through SNMP. The IP Media Server supports SNMPv1, SNMPv2, and SNMPv3. Note that invalid values used in a set operation will result in an SNMP error.

Figure 61 shows the Dialogic® IP Media Server MIB tree structure.



```
snowshoreMib
  msMib
    msReset
    msSystem
      msGeneral
        msServiceUptime
        msServiceLastReset
      msSip
        msSipClearStats
        msSipCurrentCallCount
        msSipNewCallsFlag
        msSipShutDownAllCalls
        msSipStatsLogging
        msSipLowCallThreshold
        msSipMedCallThreshold
        msSipHighCallThreshold
        sipServiceOperStatus
        sipMethodStatsTable
          sipMethodStatsEntry
            sipStatsMethodIndex
            sipStatsMethodType
            sipStatsOutbounds
            sipStatsInbounds
        sipCodeStatsTable
          sipCodeStatsEntry
            sipStatsCodeIndex
            sipStatsCode
            sipStatsOutResponse
            sipStatsInResponse
      msRtp
        msRtpLowCallThreshold
        msRtpMedCallThreshold
        msRtpHighCallThreshold
      msVxml
        msVxmlNumberRecoveryFailures
        msVxmlLastCriticalError
      msFeatures
        msFeaturesPorts
          msFeaturesPortsTotal
    msTraps
      msResetChange
      msSipLowCallThresholdMet
      msSipMedCallThresholdMet
      msSipHighCallThresholdMet
      msRtpLowCallThresholdMet
      msRtpMedCallThresholdMet
      msRtpHighCallThresholdMet
      msVxmlRecoveryFailureOccurred
      msVxmlCriticalError
```

Figure 61. MIB Tree Structure

MIB Definitions

The MIB Tree Structure Object IDs (OIDs) are described in Table 18:

Table 18. MIB OIDs

MIB	OID	Description
msReset	1.3.6.1.4.1.9234.5.1	Resets the IP Media Server. It supports the get and set operations. The valid set option is 1 (to reset the MS). The subagent resets the IP Media Server by performing an init 3 followed by an init 4, when set to 1. Upon reset, the value is reset to 0. When a get is performed, it always returns a 0.
msServiceUptime	1.3.6.1.4.1.9234.5.2.1.1.0	Time since the IP Media Server services was last re-initialized. It supports the get operation. The time is displayed in the following format: "0 day, 14 hours, 17 minutes". This value is the time the 'get' occurred, minus the time the system was initialized. This is the uptime of the IP Media Server.
msServiceLastReset	1.3.6.1.4.1.9234.5.2.1.2.0	Time since the IP Media Server was last restarted or reset. It supports the get operation. The time is displayed in the following format: “Thu May 12 12:19:23 2005”.
msSipClearStats	1.3.6.1.4.1.9234.5.2.2.1.0	Clears the SIP statistics. It supports the get and set operations. The possible value for this to be set to is 1.
msSipCurrentCallCount	1.3.6.1.4.1.9234.5.2.2.2.0	Number of active calls. It only supports the get operation.
msSipNewCallsFlag	1.3.6.1.4.1.9234.5.2.2.3.0	Stops or enables calls on the IP Media Server. It supports the get and set operations. The possible values for this to be set to are 1 and 0.
msSipShutdownAllCalls	1.3.6.1.4.1.9234.5.2.2.4.0	Stops all calls on the IP Media Server. It supports the get and set actions. The possible value for this to be set to is 1.
msSipStatsLogging	1.3.6.1.4.1.9234.5.2.2.5.0	Stops or starts SIP stats logging on the IP Media Server. It supports the get and set operations. The possible values for this to be set to are 1 or 0. When this is set to 1, it turns on logging. If this is set to 0, this turns off logging.

Table 18. MIB OIDs (Continued)

MIB	OID	Description
msSipLowCallThreshold	1.3.6.1.4.1.9234.5.2.2.6.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the lower boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msSipLowCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value, use the following format: LowThreshold < MedThreshold < HighThreshold
msSipMedCallThreshold	1.3.6.1.4.1.9234.5.2.2.7.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the medium boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msSipMedCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold
msSipHighCallThreshold	1.3.6.1.4.1.9234.5.2.2.8.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the upper boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msSipHighCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold

Table 18. MIB OIDs (Continued)

MIB	OID	Description
sipServiceOperStatus	1.3.6.1.4.1.9234.5.2.2.9.0	Current health status of the sipd process. The possible values for this OID are: ◆ up The application is operating normally, and is processing (receiving and possibly issuing) SIP requests and responses. ◆ down The application is currently unable to process SIP messages. ◆ quiescing The application is currently operational, but has been administratively put into quiescent mode. Additional inbound transactions are rejected. This data is updated every 30 seconds.
sipMethodStatsTable sipMethodStatsEntry sipStatsMethodIndex sipStatsMethodType sipStatsOutbounds sipStatsInbounds	1.3.6.1.4.1.9234.5.2.2.10 1.3.6.1.4.1.9234.5.2.2.10.1.1 1.3.6.1.4.1.9234.5.2.2.10.1.1.0 1.3.6.1.4.1.9234.5.2.2.10.1.2.0 1.3.6.1.4.1.9234.5.2.2.10.1.3.0 1.3.6.1.4.1.9234.5.2.2.10.1.4.0	This table is indexed by sipStatsMethodIndex and sipStatsMethodType. This supports the get operation. This table is updated every 30 seconds.
"Req in" and "Req out" statistics for the following methods (INV, ACK, BYE, INFO, CANC, PRACK, OPTS, REFER, REG, Unknown) are packed in a table. For example: sipStatsMethodIndexsipStatsMethodTypesipOutResponsesipInResponse 1INV20 2ACK02		
sipCodeStatsTable sipCodeStatsEntry sipStatsCodeIndex sipStatsCode sipStatsOutResponse sipStatsInResponse	1.3.6.1.4.1.9234.5.2.2.11 1.3.6.1.4.1.9234.5.2.2.11.1.1 1.3.6.1.4.1.9234.5.2.2.11.1.1.0 1.3.6.1.4.1.9234.5.2.2.11.1.2.0 1.3.6.1.4.1.9234.5.2.2.11.1.3.0 1.3.6.1.4.1.9234.5.2.2.11.1.4.0	This table is indexed by sipStatsCodeIndex and sipStatsCode. This supports the get operation. This table is updated every 30 seconds.
"Req in" and "Req out" statistics for the following methods (1xx, 2xx, 3xx, 5xx, 6xx, IntErrs) are packed in a table. For example: sipCodeStatsTable sipStatsCodeIndexsipStatsCodesipOutResponsesipInResponse 11xx20 22xx02		

Table 18. MIB OIDs (Continued)

MIB	OID	Description
msRtpLowCallThreshold	1.3.6.1.4.1.9234.5.2.3.1.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the lower boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msRtpLowCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold
msRtpMedCallThreshold	1.3.6.1.4.1.9234.5.2.3.2.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the medium boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msRtpMedCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value use the following format: LowThreshold < MedThreshold < HighThreshold
msRtpHighCallThreshold	1.3.6.1.4.1.9234.5.2.3.3.0	Number of calls versus the maximum number of calls allowed. It supports the get and set operations. Its value is a percentage, and specifies the upper boundary. Valid values for the set operation range from 1 to 100. When the current call percentage exceeds this threshold, the msRtpHighCallThreshold trap is sent. The current call volume (as a percent of the current call load verses the total licenses available) is compared to this threshold. This comparison is made every 30 seconds. When setting this value, use the following format: LowThreshold < MedThreshold < HighThreshold
msVxmlNumberRecoveryFailures	1.3.6.1.4.1.9234.5.2.4.1.0	Number of failures that have occurred while attempting to recover Media Content files. Setting to 0 clears it.
msVxmlLastCriticalError	1.3.6.1.4.1.9234.5.2.4.2.0	Last Critical level error received.
msFeaturesPortsTotal	1.3.6.1.4.1.9234.5.2.5.1.1.0	Number of licensed ports available on the IP Media Server.

TRAP Definitions

Table 19. Trap OIDs and Descriptions

Trap	OID	Description
msResetChange	1.3.6.1.4.1.9234.5.3.1	The IP Media Server has been reset by SNMP. The following string is included in the trap message: “The IP Media Server Has Been Reset”.
msSipLowCallThresholdMet	1.3.6.1.4.1.9234.5.3.2	The IP Media Server call percentage has exceeded the low threshold value. The following string is included in the trap message: “Low Call Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msSipMedCallThresholdMet	1.3.6.1.4.1.9234.5.3.3	The IP Media Server call percentage has exceeded the medium threshold value. The following string is included in the trap message: “Med Call Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msSipHighCallThresholdMet	1.3.6.1.4.1.9234.5.3.4	The IP Media Server call percentage has exceeded the high threshold value. The following string is included in the trap message: “High Call Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msRtpLowCallThresholdMet	1.3.6.1.4.1.9234.5.3.5	The IP Media Server call percentage has exceeded the low threshold value. The following string is included in the trap message: "Low Call RTP Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msRtpMedCallThresholdMet	1.3.6.1.4.1.9234.5.3.6	The IP Media Server call percentage has exceeded the medium threshold value. The following string is included in the trap message: "Med Call RTP Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msRtpHighCallThresholdMet	1.3.6.1.4.1.9234.5.3.7	The IP Media Server call percentage has exceeded the high threshold value. The following string is included in the trap message: "High Call RTP Threshold is Met, Call Volume at %d” (where %d is the current percent call volume).
msVxmlRecoveryFailureOccurred	1.3.6.1.4.1.9234.5.3.8	An attempt to recover a recorded media content file has failed.
msVxmlCriticalError	1.3.6.1.4.1.9234.5.3.9	A critical level error has occurred in a VXML application. Contains the text of msVxmlLastCriticalError.

SNMP MIB-II

The IP Media Server supports SNMPv2 and SNMPv3 agent operation and includes the following Management Information Bases (MIBs) and all their specified managed objects:

RFC 1213 MIB-II

- system
- interface
- ip
- icmp
- tcp
- udp
- snmp

RFC 1907 SNMPv2

```
     snmpTRAP-coldStart, authenticationFailure
```

Unsupported OIDs

The following OIDs are not supported on the IP Media Server as part of the SNMP MIB-II specification.

System Group

- sysServices

Interfaces Group

- ifInUnknownProtos
- ifOutNUcastPkts

IP Group

- ipRouteMetric2
- ipRouteMetric3
- ipRouteMetric4
- ipRouteAge
- ipRouteMetric5

System Menu

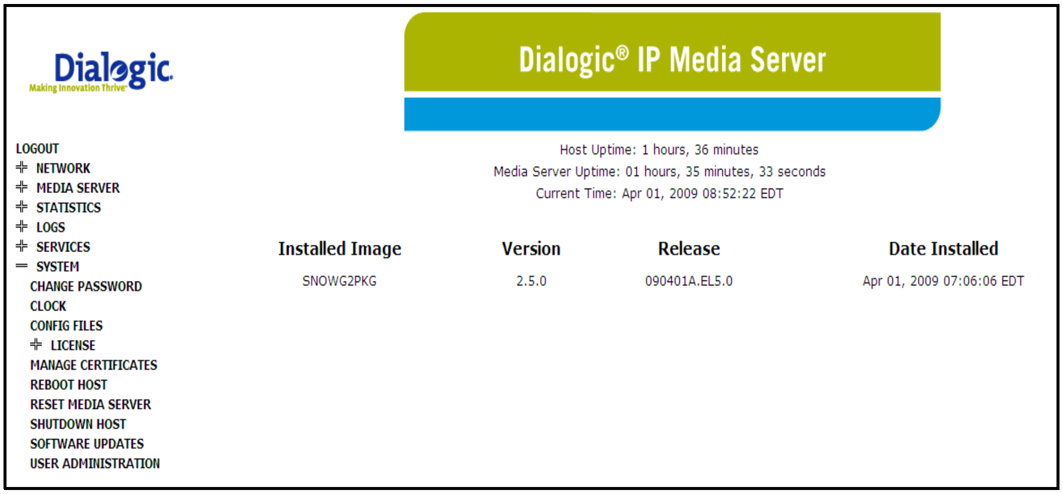
The SYSTEM menu contains commands for:

- Changing Administrator Password
- Configuring the Clock
- Backing Up and Restoring Configurations
- Managing Licenses
- Managing Certificates
- Rebooting the Host
- Resetting the Dialogic® IP Media Server
- Shutting Down the Host
- Updating Software
- Administering Users

These menu items are described in the following sections.

System Home Page

When the System menu is selected, the IP Media Server home page appears with updated status information (see “Web UI Home Page” (page 46)).



Host Uptime: 1 hours, 36 minutes
Media Server Uptime: 01 hours, 35 minutes, 33 seconds
Current Time: Apr 01, 2009 08:52:22 EDT

Installed Image	Version	Release	Date Installed
SNOWG2PKG	2.5.0	090401A.EL5.0	Apr 01, 2009 07:06:06 EDT

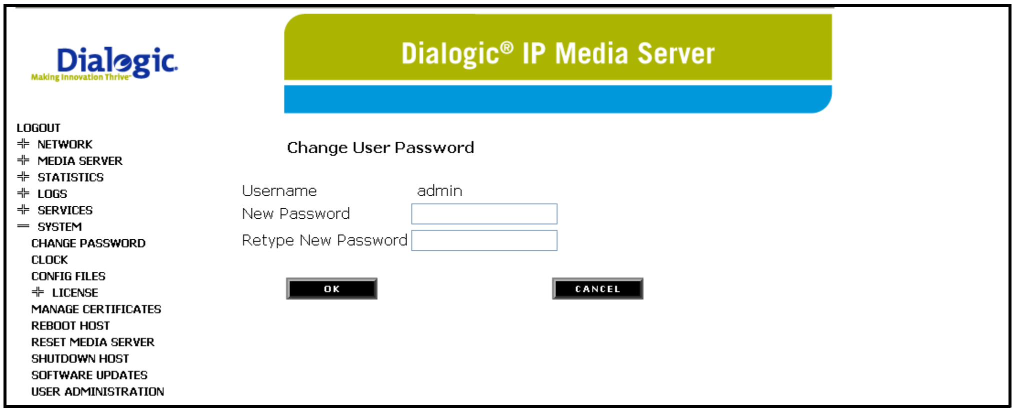
Figure 62. System Home Page

Changing Administrator Password

Note: Passwords are case sensitive.

To change the password of the account you are currently logged in on:

1 Select the SYSTEM→CHANGE PASSWORD command to display the Change Password page:



Change User Password

Username admin

New Password

Retype New Password

Figure 63. Change Password Page

2 Enter your current password.

3 Enter a new password.

4 Confirm your new password.

5 Click OK to make the change.

Configuring the Clock

Note: Only Administrators have access to the CLOCK command.

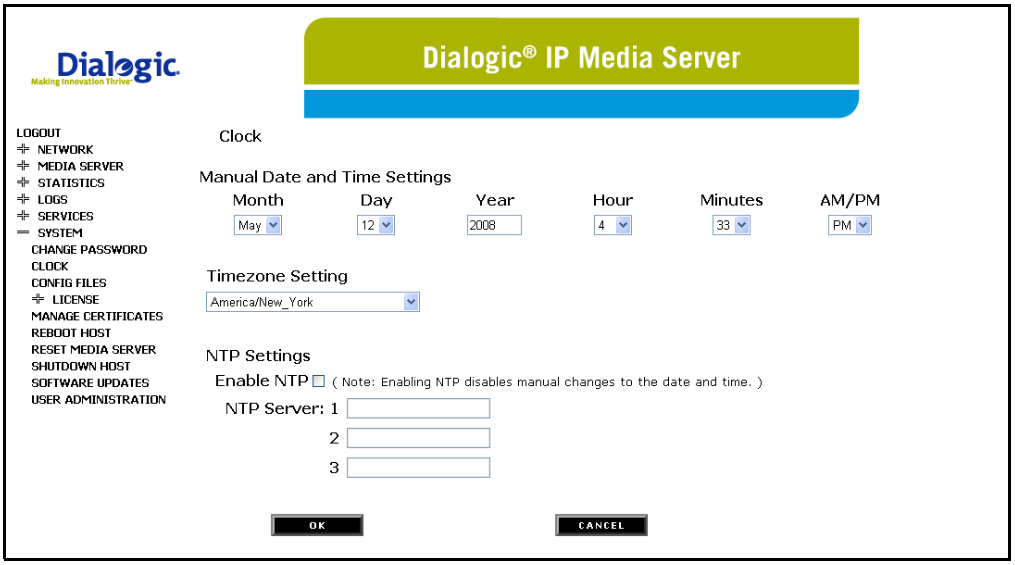
The system has an internal clock, but it can also be configured to source its clock from a network time protocol (NTP) server.

- If NTP is enabled, the system immediately starts using the NTP server.
- If NTP is not enabled, you can set the current system time, date, and time zone.

Note: The use of an NTP server across all servers in your network is strongly recommended, as it ensures that time and date stamps will be consistent and comparable across the network. This helps considerably when troubleshooting the IP Media Server.

To configure an NTP server:

1 Select CLOCK from the SYSTEM menu to display the Clock page.



Clock

Manual Date and Time Settings

Month	Day	Year	Hour	Minutes	AM/PM
May	12	2008	4	33	PM

Timezone Setting

America/New_York

NTP Settings

Enable NTP ☐ (Note: Enabling NTP disables manual changes to the date and time.)

NTP Server: 1

2

3

Figure 64. Clock Page

2 Check Enable NTP.

3 Enter the IP address of one or more NTP servers.

Note: You can configure up to three NTP servers.

Any changes take effect when you select OK.

The changes can be cancelled by clicking CANCEL.

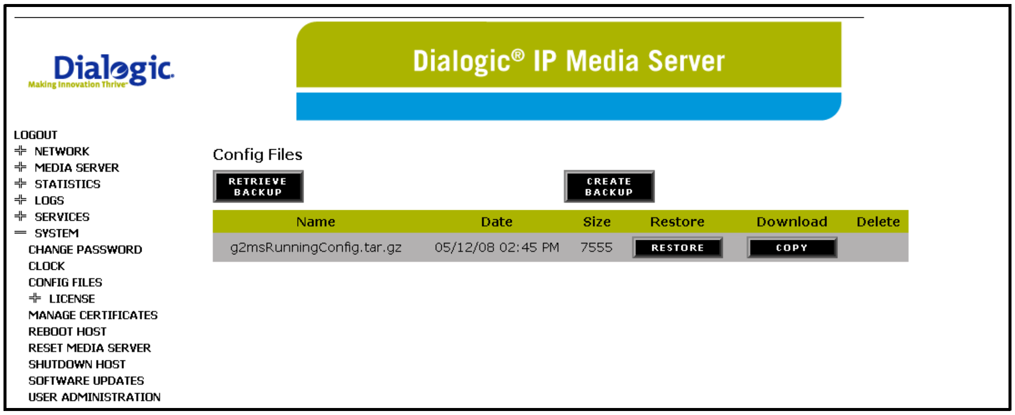
Backing Up and Restoring Configurations

The system provides the ability to back up all the configuration parameters. The backup files are stored together in a tar file and can be downloaded to another location on the network. The configuration can also be restored from a previously saved backup of the system.

Note: Only Administrators can create and delete backup configurations. All users can download a configuration.

To access the configuration backup services:

1 Select SYSTEM→CONFIG FILES to display the Config Files page.



Name	Date	Size	Restore	Download	Delete
g2msRunningConfig.tar.gz	05/12/08 02:45 PM	7555	RESTORE	COPY	

Figure 65. Config Files Page

The Config Files page contains a list of currently backed-up configurations, as well as the currently running configuration.

Note: The running configuration is saved each time the host reboots or the IP Media Server is reset. It is called `g2mRunningConfig.tar.gz`.

From the Config Files page you can perform several configuration file actions:

- Back up configurations
- Delete a stored backup
- Download a stored backup configuration
- Restore a backed-up configuration.

Backup Current Configurations

To back up the current set of configuration files:

1 Click CREATE BACKUP.

This action makes a copy the current configuration files (which are not necessarily identical to the running configuration) and creates a backup copy. The name of the backup is based on the date and time the backup was created. It is similar to:

```
g2msbackup.20050701114510.tar.gz
```

which is a backup file created on July 01, 2005 at 11:45:10.

Delete a Stored Backup

To delete a stored backup configuration:

1 Click the DELETE button beside the file name.

This action must be confirmed or cancelled. The backup of the running configuration cannot be deleted.

Download a Stored Backup Configuration

To download a stored backup configuration to another location:

1 Click the DOWNLOAD button beside the file name.

A standard file dialog appears, giving you the option of opening or saving the file.

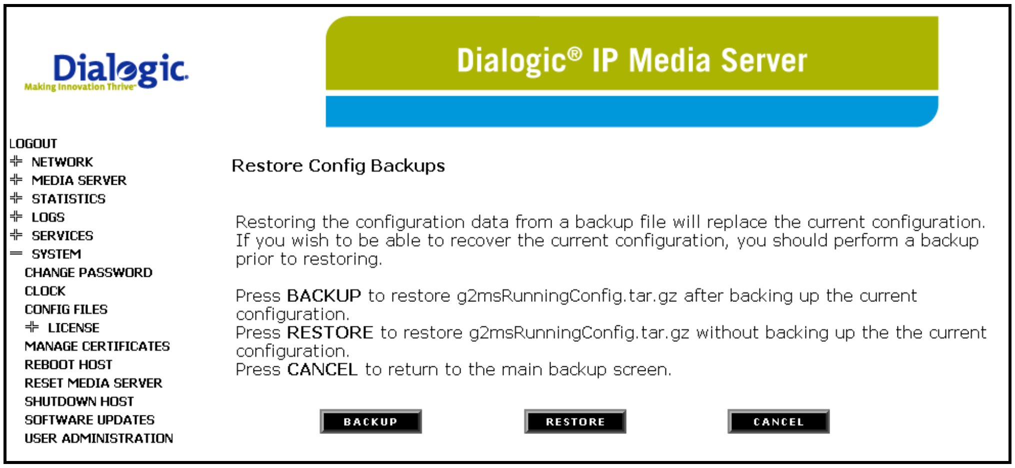
2 Click SAVE and select the directory where the configuration file is saved.

Restore a Backed-up Configuration

Note: Only Administrators can restore a configuration.

To restore a previously backed up configuration:

1 Click the RESTORE button beside the backup file name to display the Restore Config Backups page:



Restore Config Backups

Restoring the configuration data from a backup file will replace the current configuration. If you wish to be able to recover the current configuration, you should perform a backup prior to restoring.

Press BACKUP to restore g2msRunningConfig.tar.gz after backing up the current configuration.
Press RESTORE to restore g2msRunningConfig.tar.gz without backing up the the current configuration.
Press CANCEL to return to the main backup screen.

Figure 66. Restore Config Backups Page

There are two types of restorations available:

- Backup–Creates a copy of the current configuration files and then replaces them with the selected backup configuration.
- Restore–Overwrites the current configuration files with the selected backup configuration, but does not create a copy of the current configuration.

You can also cancel the restore action by clicking CANCEL.

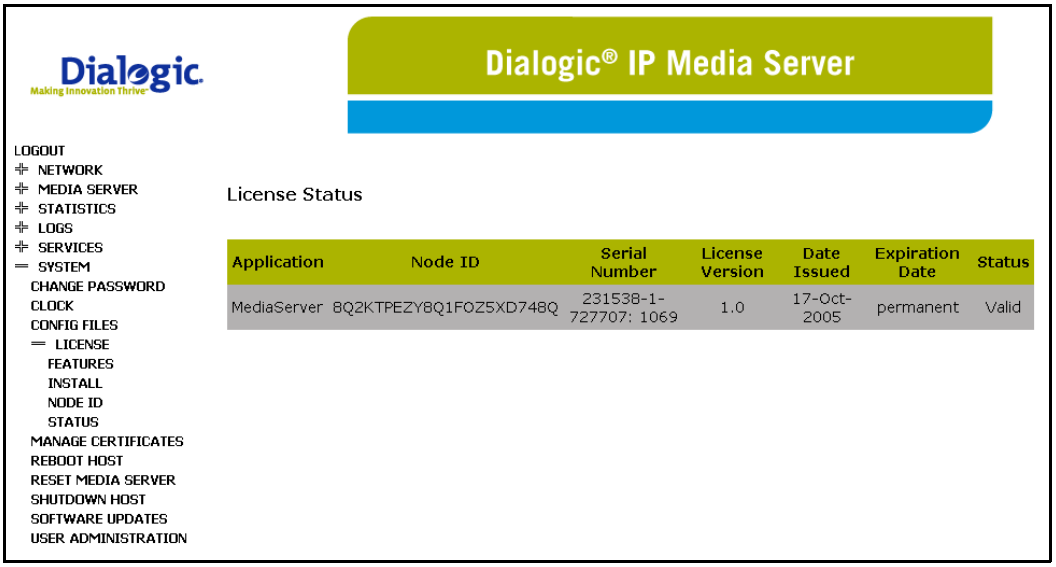
⚠ **Restoring the configuration data from a backup file can replace the current configuration. If you wish to be able to recover the current configuration, you should perform a backup prior to restoring.**

Restoring a configuration updates the configuration files, but does not affect the currently running configuration. The host must be rebooted for the restored configuration to take effect.

Managing Licenses

You use the IP Media Server Web UI to install and activate IP Media Server licenses, and to view the current status of licenses on your system. For detailed information on managing licenses, see the *Dialogic IP Media Server License Activation Guide*.

To manage licenses, select the SYSTEM→CONFIG FILES→LICENSE menu item. This displays the License Status page, which contains information about the currently active license.

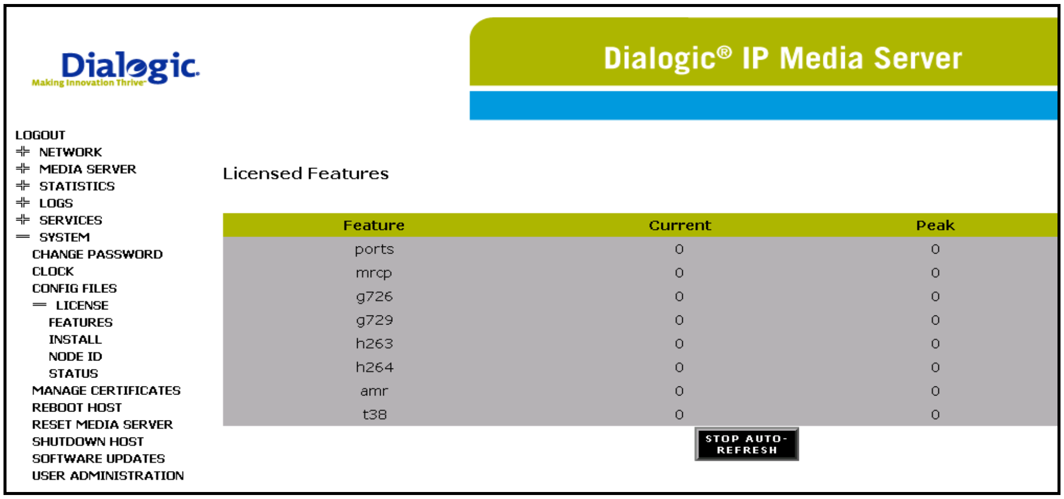


License Status

Application	Node ID	Serial Number	License Version	Date Issued	Expiration Date	Status
MediaServer	8Q2KTPEZY8Q1FOZ5XD748Q	231538-1-727707: 1069	1.0	17-Oct-2005	permanent	Valid

Figure 67. License Status Page

To view the features currently licensed on your system, and statistics about their usage, select the SYSTEM→CONFIG FILES→LICENSE→FEATURES menu to display the License Features page:



Licensed Features

Feature	Current	Peak
ports	0	0
mrcp	0	0
g726	0	0
g729	0	0
h263	0	0
h264	0	0
amr	0	0
t38	0	0

Figure 68. Licensed Features Page

To activate and install a license, use the NODE ID and INSTALL menus. For detailed information on using them, see the *License Activation Guide*.

Managing Certificates

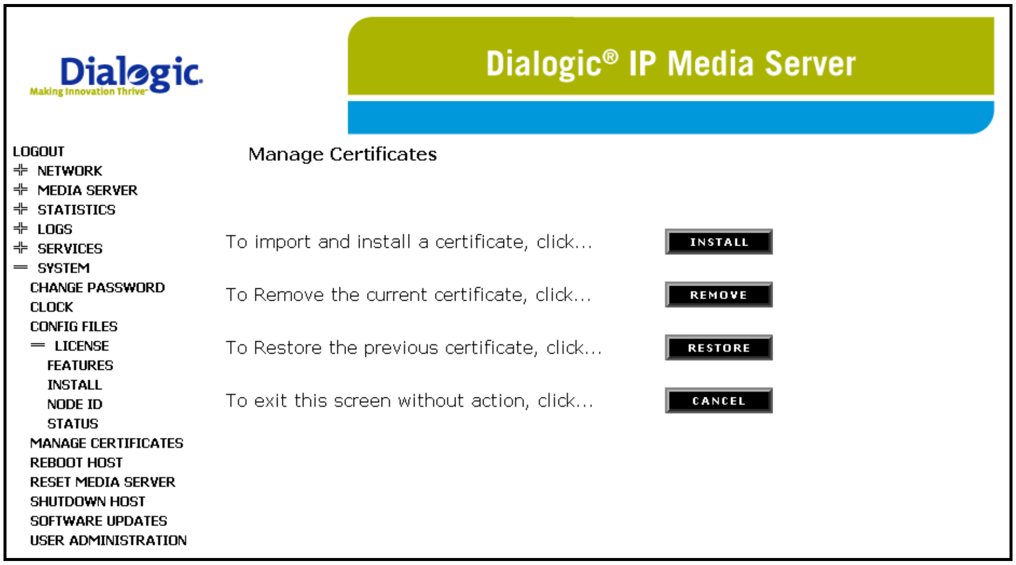
The Dialogic® IP Media Server Web User Interface can operate with HTTP or HTTPS. If HTTPS is being used, a padlock appears at the bottom right in the browser display. If HTTP is being used, a padlock does not appear.

To use HTTPS, the Dialogic® IP Media Server must have a server certificate and key, and the browser must have the matching client certificate.

A user-generated security certificate and key can be installed on the Dialogic® IP Media Server . The Web UI uses this certificate/key for HTTPS authentication.

To retrieve a certificate/key:

1 Select SYSTEM→MANAGE CERTIFICATES to display the manage Certificates page:



Manage Certificates

To import and install a certificate, click...

To Remove the current certificate, click...

To Restore the previous certificate, click...

To exit this screen without action, click...

Figure 69. Manage Certificates Page

This page provides the following options:

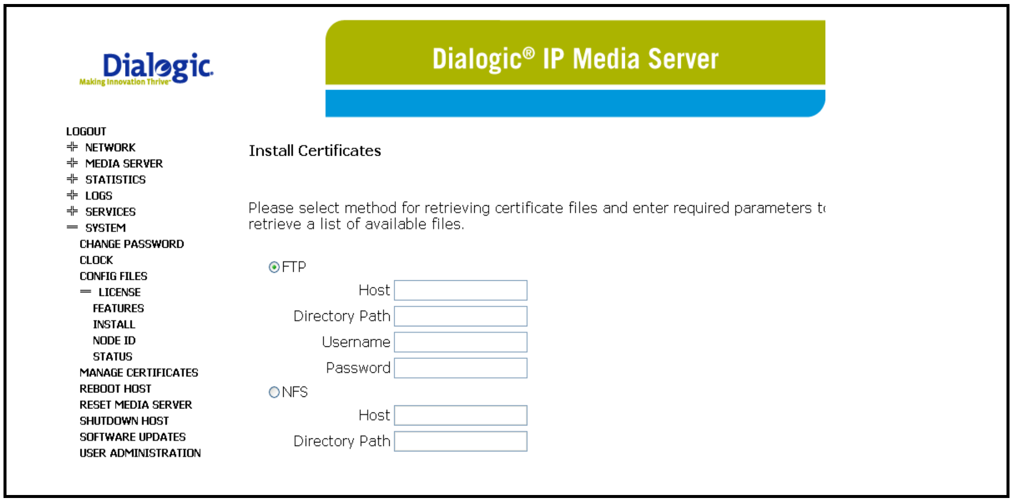
- INSTALL: Imports a certificate and key from a remote server and installs it on the Dialogic® IP Media Server .
- REMOVE: Removes the current certificate from the Dialogic® IP Media Server .
- RESTORE: Restores the previous certificate to the Dialogic® IP Media Server .
- CANCEL: Does nothing and returns to the system splash screen.

Installing a Certificate

When you click INSTALL, a certificate and key can be retrieved from a remote server using FTP or NFS. Enter the parameters for the FTP or NFS server that holds the certificates and keys. The Dialogic® IP Media Server attempts to access the server, and then displays the available certificates (.crt files) for retrieval. Only certificate files (<filename>.crt) are shown, but there must also be a matching valid key (<filename>.key) present for the certificate in order for the certificate to be displayed in the Web UI. The certificate and the key must have the same name with the appropriate file extension (xx.crt and xx.key). You can navigate through the directory structure, but the window only displays directories and certificates.

To install a certificate:

1 On the Manage Certificates page, click INSTALL to display the Install Certificates page:



Install Certificates

Please select method for retrieving certificate files and enter required parameters t retrieve a list of available files.

● FTP

Host

Directory Path

Username

Password

○ NFS

Host

Directory Path

Figure 70. Install Certificate Page

2 Click OK to install the certificate and display the results of the installation.

- If the installation is successful, the previous certificate (if there is one) is saved and the Web UI begins using the new certificate as soon as you click Continue.
- If the installation is not successful an error appears and the update of the certificate does not take place. The certificate is not kept for installation in the future.

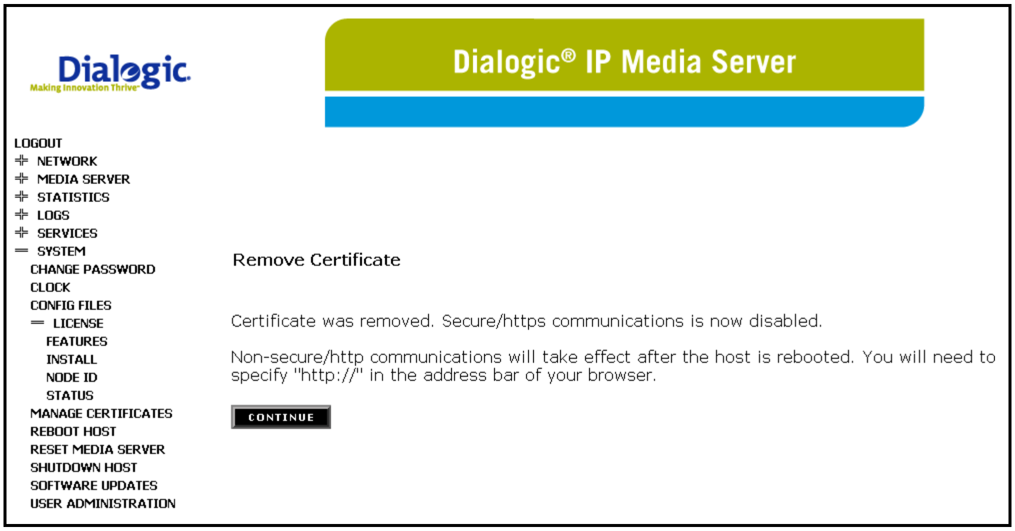
Click CANCEL to exit the screen and return to the system home page. If you click CANCEL, the command is terminated and the certificate is not installed. The certificate is not kept for installation in the future. To install it, it needs to be retrieved again.

Removing a Certificate

To remove the current certificate:

1 On the Manage Certificates page, click REMOVE to remove the current certificate and key from the system and save them.

The Remove Certificate page is displayed to confirm the removal:



Remove Certificate

Certificate was removed. Secure/https communications is now disabled.

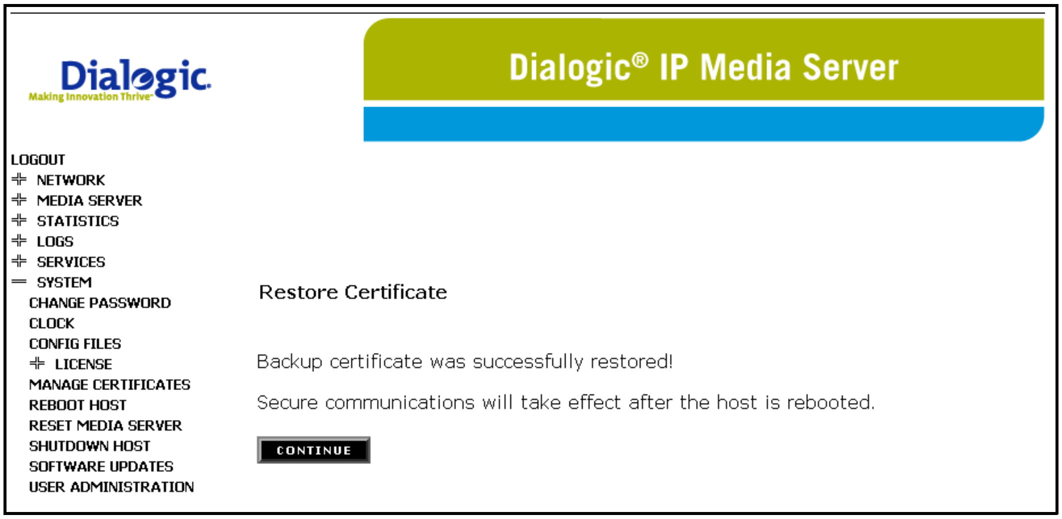
Non-secure/http communications will take effect after the host is rebooted. You will need to specify "http://" in the address bar of your browser.

Figure 71. Remove Certificate Page

The Web User Interface now uses HTTP when the CONTINUE button is clicked. The padlock icon at the bottom of the browser display disappears when the screen is next refreshed.

Restoring a Certificate

On the Manage Certificates page, click the RESTORE button to put the previous certificate (if there is one that has been removed or overwritten) back on the system. The Web User Interface uses HTTPS when the CONTINUE button is clicked. The padlock icon at the bottom of the browser display appears when the screen is refreshed.



Restore Certificate

Backup certificate was successfully restored!

Secure communications will take effect after the host is rebooted.

Figure 72. Restore Certificate Page

Rebooting the Host

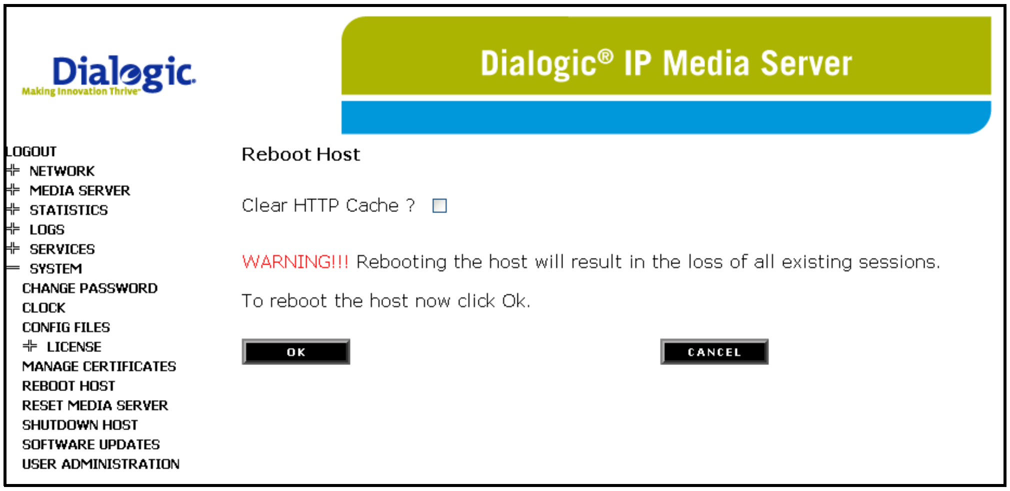
Rebooting the host causes all applications to stop and the operating system to reboot. After rebooting, the system reads and uses the configuration files for all services and interfaces. This action causes all traffic to be dropped and all existing sessions to be disconnected.

Note: Only Administrators can reset the Dialogic® IP Media Server .

Rebooting the host results in the loss of all existing sessions.

To reset the Dialogic® IP Media Server :

1 Select REBOOT HOST from the SYSTEM menu to display the Reboot Host page.



Reboot Host

Clear HTTP Cache ? □

WARNING!!! Rebooting the host will result in the loss of all existing sessions.

To reboot the host now click Ok.

Figure 73. Reboot Host Page

2 Click Clear HTTP Cache if you wish to delete all stored IP Media Server pages.

3 Click OK to reboot the IP Media Server host. Click Cancel to continue without rebooting.

When the action is complete, you are returned to the IP Media Server home page.

Resetting the Dialogic® IP Media Server

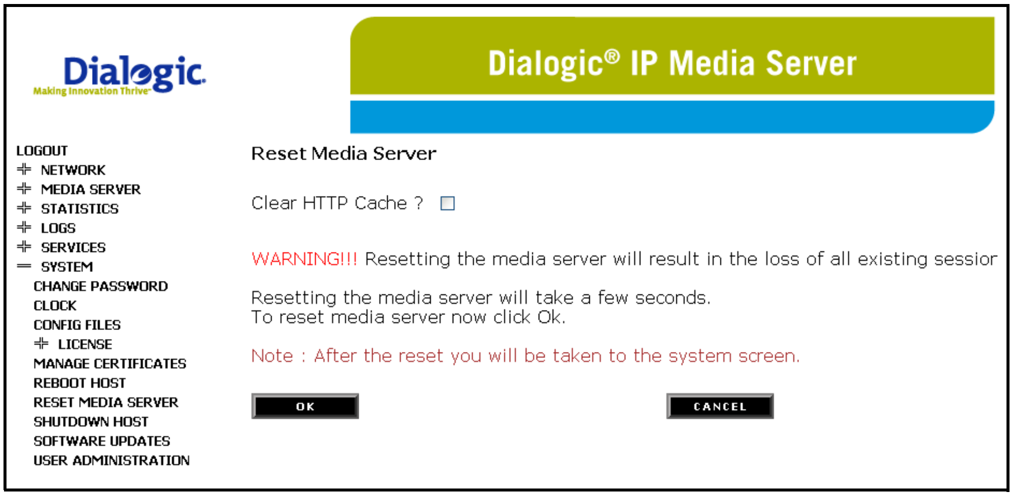
This command causes the Dialogic® IP Media Server application to reset and restart itself, but does not reboot the host.

Note: Only Administrators can reset the Dialogic® IP Media Server .

Resetting the IP Media Server results in the loss of all existing sessions.

To reset the Dialogic® IP Media Server :

1 Select RESET MEDIA SERVER from the SYSTEM menu to display the Reset Media Server page.



Reset Media Server

Clear HTTP Cache ? □

WARNING!!! Resetting the media server will result in the loss of all existing sessior

Resetting the media server will take a few seconds.
To reset media server now click Ok.

Note : After the reset you will be taken to the system screen.

Figure 74. Reset Media Server Page

2 Click Clear HTTP Cache if you wish to delete all stored IP Media Server pages.

3 Click OK to reset the IP Media Server. Click Cancel to continue without resetting the IP Media Server.

When the action is complete, you are returned to the IP Media Server home page.

Shutting Down the Host

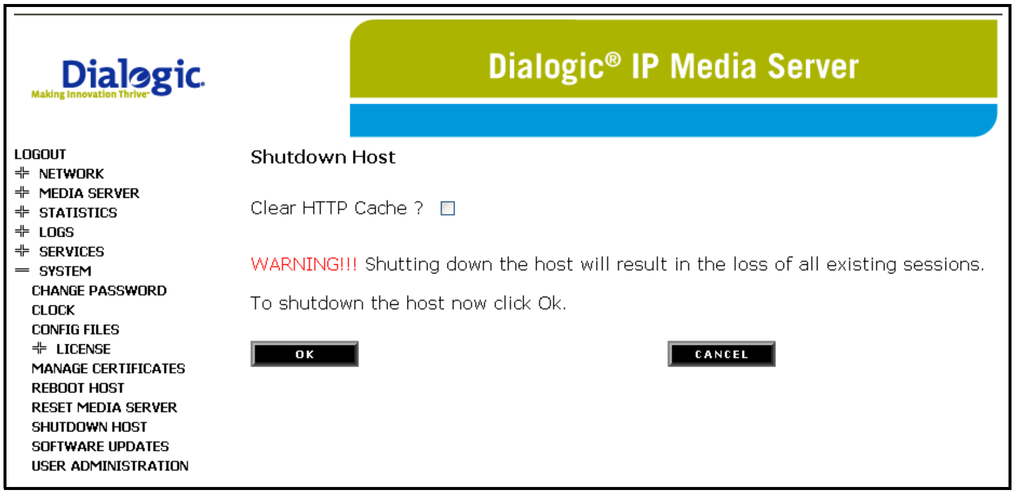
Shutting down the host stops all applications and the operating system. This action causes all traffic to be dropped and all existing sessions to be disconnected.

Note: Only Administrators can shut down the Dialogic® IP Media Server .

Shutting down the host results in the loss of all existing sessions.

To shut down the Dialogic® IP Media Server :

1 Select SHUTDOWN HOST from the SYSTEM menu to display the Shutdown Host page.



Shutdown Host

Clear HTTP Cache ? □

WARNING!!! Shutting down the host will result in the loss of all existing sessions.

To shutdown the host now click Ok.

Figure 75. Shutdown Host Page

2 Click Clear HTTP Cache if you wish to delete all stored IP Media Server pages.

3 Click OK to shut down the IP Media Server host. Click Cancel to continue without shutting down.

Updating Software

You can download and upgrade the Dialogic® IP Media Server software from a remote location. The software releases are digitally signed by Dialogic and contain checksums to ensure the files are not corrupted during the download process.

Note: Only Administrators have access to the software updates menu.

Releases can be downloaded from any ftp server. Releases can be obtained from the Dialogic Technical Support web site. This requires a user name, password, and directory, which can be obtained from Dialogic Technical Support.

To download a release and upgrade a system:

1 Download the desired release to the system using the Retrieve command.

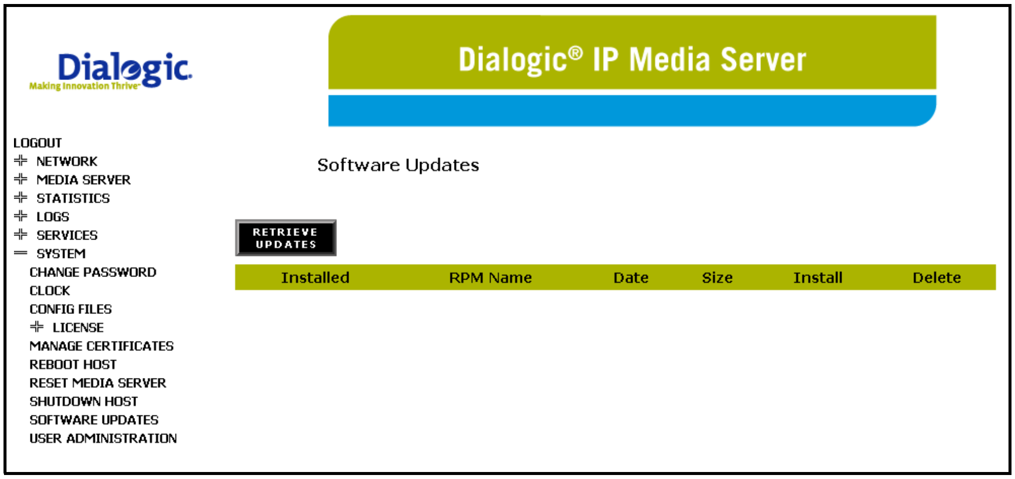
Performs download over ftp, and the Retrieve command checks to ensure the software release was downloaded successfully.

2 Using the Install command, select the release you want to install.

Saves the existing release, and installs the new release. Installing a new release of software causes the host to reboot.

Displaying the Releases Available on the System

1 Select SOFTWARE UPDATES from the SYSTEM menu to display the Software Updates page:

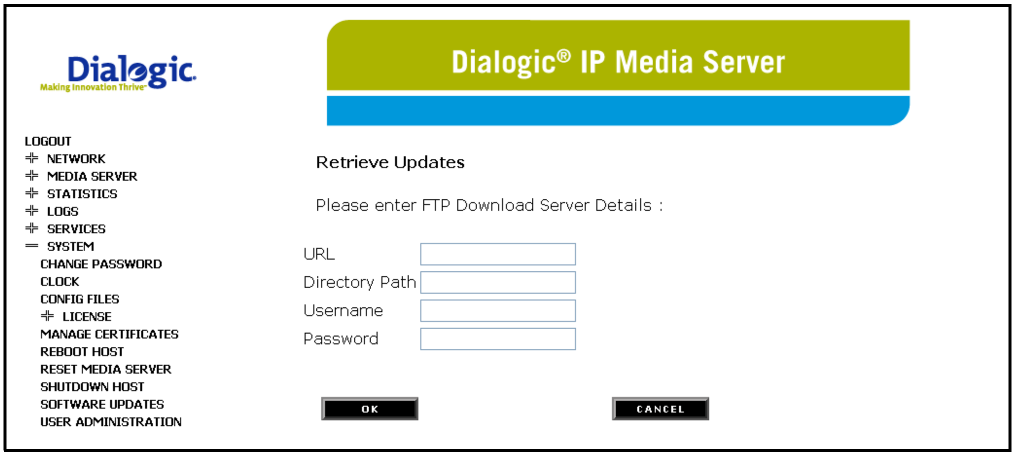


Software Updates

Installed	RPM Name	Date	Size	Install	Delete

Figure 76. Software Updates Page

2 Click Retrieve Updates to display the Retrieve Updates page.



Retrieve Updates

Please enter FTP Download Server Details :

URL
Directory Path
Username
Password

Figure 77. Retrieve Updates Page

3 Enter the location of updates for the IP Media Server and your login name and password. The Results page displays.

If you leave the Directory Path blank, the Results page includes all accessible directories on the RTP server. Updates that are currently on your computer are indicated with a checkmark in the folder icon on the left.

If necessary, navigate to the appropriate subdirectory to display the list of available updates.

4 Click Retrieve to download the update to your computer. The display returns to the Software Updates page, with the new update included in the list.

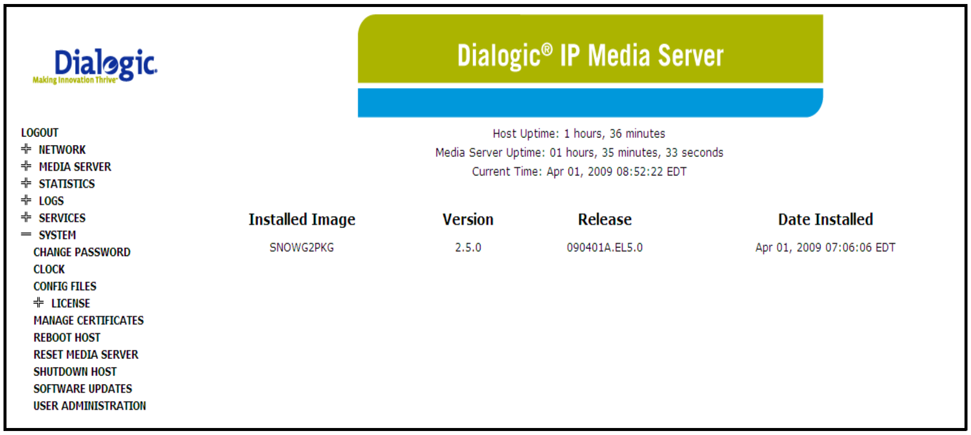
5 To install a new software update, click Install. This displays the Confirm Software Update page.

6 Click OK to complete the installation of the new software. The Software Update page is again displayed with a checkmark next to the newly installed software.

Viewing the Running Release

To display the current release on the system and when it was installed:

1 Click SYSTEM to display the system home page, which shows the running software release:



Host Uptime: 1 hours, 36 minutes
Media Server Uptime: 01 hours, 35 minutes, 33 seconds
Current Time: Apr 01, 2009 08:52:22 EDT

Installed Image	Version	Release	Date Installed
SNOWG2PKG	2.5.0	090401A.EL5.0	Apr 01, 2009 07:06:06 EDT

Figure 78. Running Software Release

Retrieving a Software Release

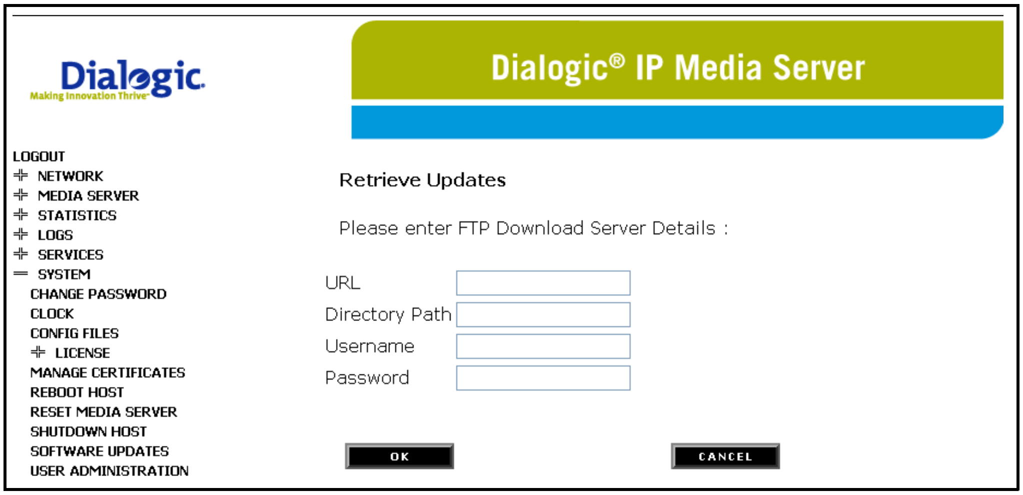
The FTP server stores the software releases. When it is accessed, a list of valid software releases appears and a RETRIEVE button appears for each release. The Installed column to the left of the release name contains a check mark if the release has already been downloaded to the system. If the Installed column is blank, the release has not been downloaded.

The window directories are also displayed and have a file folder icon to their left. You can navigate through the directory structure, but only other directories and IP Media Server releases are shown.

Click RETRIEVE UPDATES to download the selected software release to the IP Media Server. The standard FTP transfer progress dialog appears and gives information about the success and failure of the download.

To retrieve a software release and download it (without installing it):

1 On the Software Updates page, click RETRIEVE UPDATES to display the Retrieve Updates page:



Retrieve Updates

Please enter FTP Download Server Details :

Figure 79. Retrieving Software from an FTP Server

2 Enter the URL of the FTP server.

3 Enter the directory path (optional).

4 Enter user name.

5 Enter Password.

6 Click OK to have the system attempt to access the specified user on the FTP server.

Click CANCEL to return you to the Software Updates page.

Note: You can use any FTP server to store the software releases.

Installing a New Software Release

To install a new software release on the system:

1 Click the INSTALL button beside the release.

The screen displays the currently running release and asks you to confirm that you want to install the selected release. Select Confirm to install the new release and reboot the system.

Installing a new release reboots the host.

To remove a software release from the system:

1 Click the DELETE button beside the release to be deleted.

2 Click confirm to confirm the deletion, or click Cancel to stop.

Note: Deleting a software release does not affect the currently running system. It continues to operate and use the same release when reset.

Administering Users

The IP Media Server supports two access levels:

- Administrator—Can change the configuration of the system and execute administrative tasks.
- Operator—Can monitor the system, but cannot change configurations or execute administrative tasks.

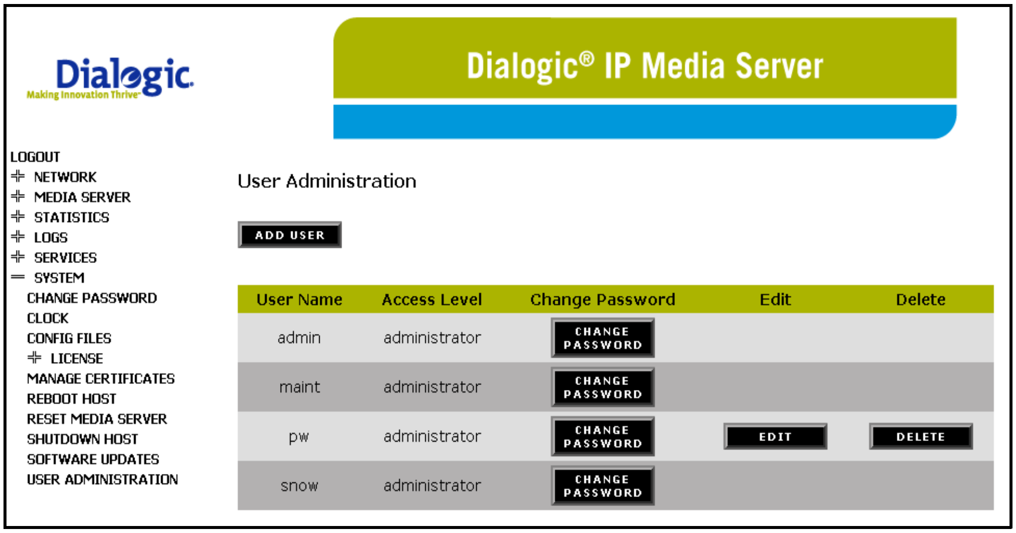
Commands that are only available to Administrators are noted as such. All other commands are usable by both operators and administrators.

Note: Only Administrators can perform user administration.

Use the SYSTEM→USER ADMINISTRATION command to display the User Administration page, which contains the currently configured users on the system. Administrators can add, delete, and change the attributes of other users.

The attributes are:

- password
- access level



User Administration

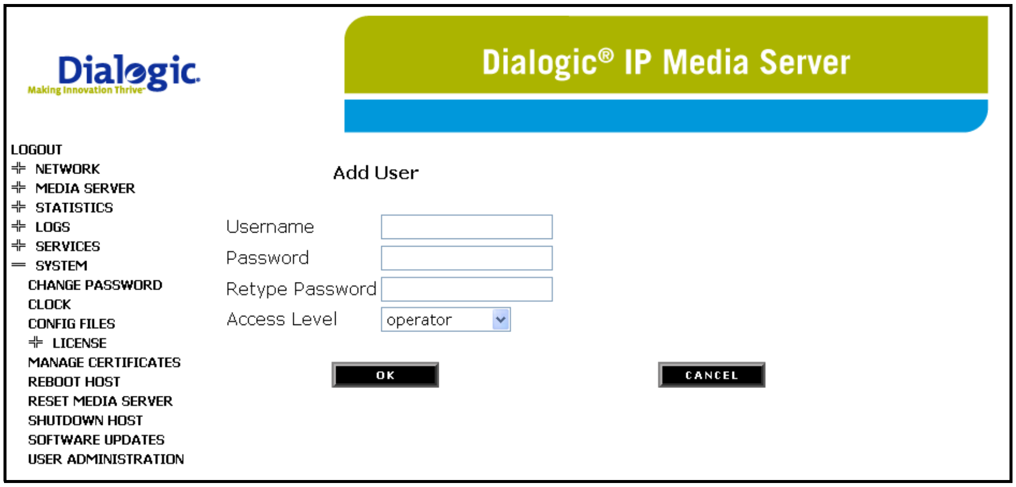
User Name	Access Level	Change Password	Edit	Delete
admin	administrator	CHANGE PASSWORD		
maint	administrator	CHANGE PASSWORD		
pw	administrator	CHANGE PASSWORD	EDIT	DELETE
snow	administrator	CHANGE PASSWORD		

Figure 80. User Administration Page

Adding a User

To add a new user:

1 Click ADD USER to display the Add User page.



Add User

Username

Password

Retype Password

Access Level operator

Figure 81. Add User Page

2 Fill in the following:

- Username
- Password
- Access level

Note: User names and passwords are case sensitive.

3 To complete the action, click OK.

To cancel the action, click CANCEL.

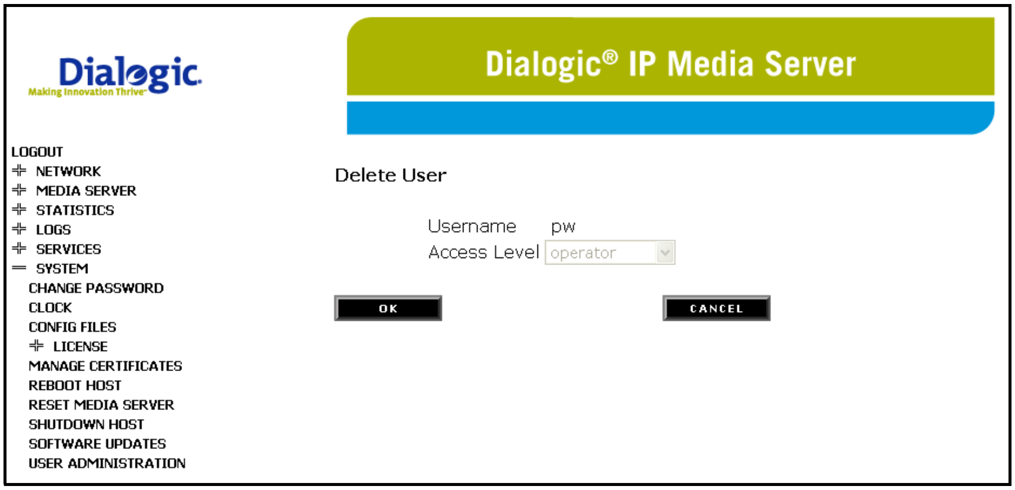
Deleting a User

To delete a user (Administrator only):

1 Click the DELETE button beside the user name.

A new screen appears to verify the change.

2 Click OK to delete the user. Click CANCEL to cancel.



Delete User

Username pw

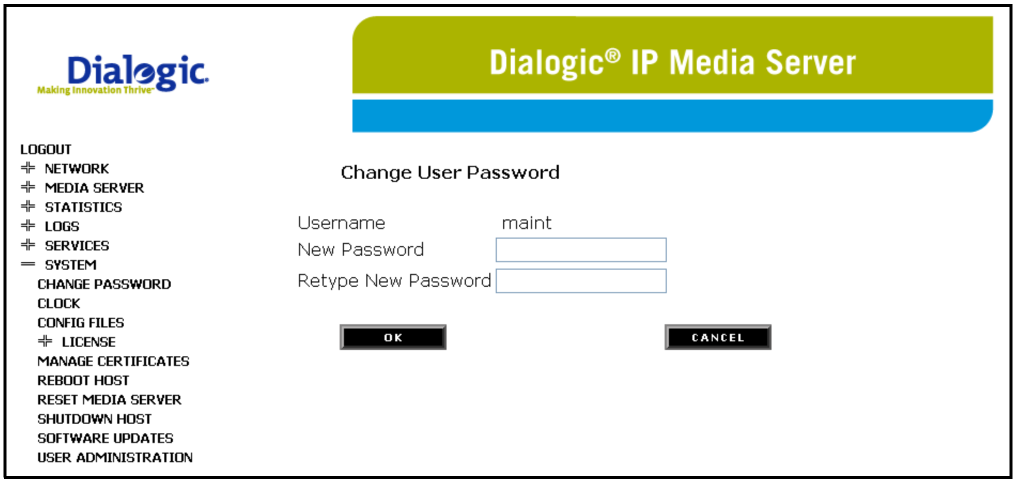
Access Level operator

Figure 82. Delete User Page

Resetting a Password

To reset the password of any other user, do the following:

1 Click the CHANGE PASSWORD button beside the user name to display the Change User Password page.



Change User Password

Username maint

New Password

Retype New Password

Figure 83. Change User Password Page

2 Enter a new password.

3 Confirm the new password.

4 Click OK to accept.

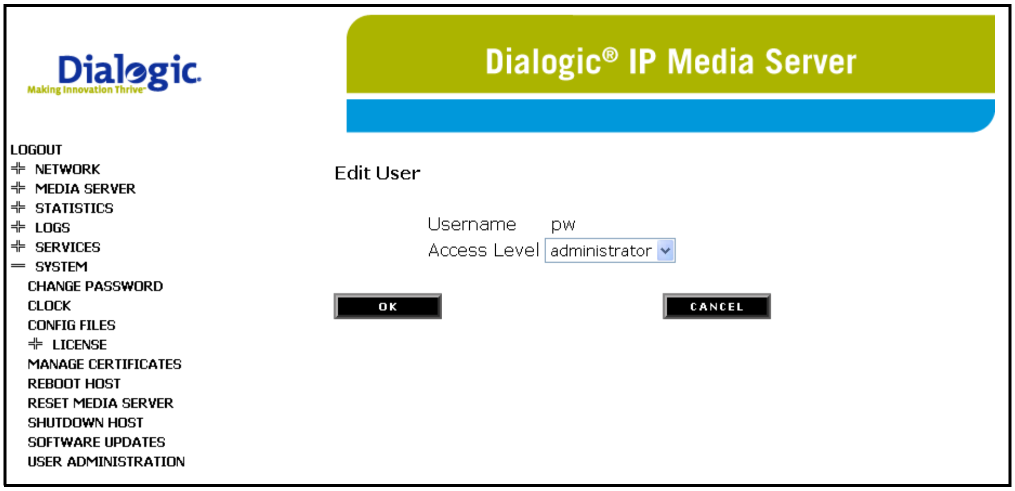
Click CANCEL to cancel the change.

Note: As Administrator, you cannot change your own password or delete your own username in USER ADMINISTRATION. You can change your password using the SYSTEM→CHANGE PASSWORD command.

Changing User Access Level

To change the access level of a user (administrator only), do the following:

1 Click the EDIT button beside the user name to display the Edit User page:



Edit User

Username pw
Access Level administrator

Figure 84. Edit User Page

2 Choose the access level ADMINISTRATOR or OPERATOR.

3 To accept the change, click OK.

To cancel the change, click CANCEL.

Accounting Mechanism

Monitoring Call Volume

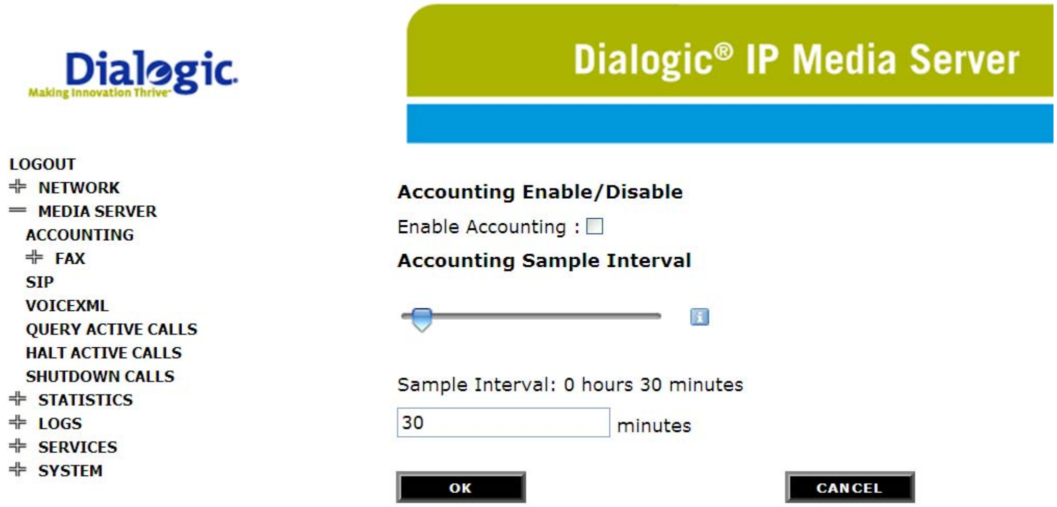
The IP Media Server has an accounting mechanism that provides details on what licensed resources a customer is using during a given time internal. The Web UI allows you to configure this time interval.

The accounting mechanism in the IP Media Server stores the data in two parts:

- xml format text log file
- secure private database

➢ Follow the steps below to configure the time interval.

1 From the Media Server menu, select Accounting. The following screen appears.



Accounting Enable/Disable

Enable Accounting : □

Accounting Sample Interval

Sample Interval: 0 hours 30 minutes

30 minutes

2 Accounting is disabled by default. Select the Enable Accounting checkbox to enable.

3 There are three ways to enter the sample interval:

- Slide the tab on the bar
- Click on the bar and use the mouse scroll wheel
- Type the sample interval in the box.

4 Click OK.

5 Changes require you to reset or reboot the IP Media Server.

A - Compliance and Standards Information

This chapter describes the IP Media Server's compliance with standards.

Supported Protocols and Standards

The following is a list of currently supported protocols and RFC standards.

Table 20. Supported Protocols and Standards

Protocols	RFC #
ARP	RFC 826
DNS	RFC 1034, RFC 1035, RFC 2181
Ethernet v2	RFC 894
	Gigabit Ethernet specification IEEE 802.3z. 802.3x.
	RFC 2665, General Ethernet statistics
FTP	RFC 959, 2228, 2640, 2773
HTTP/1.0	RFC 1945
HTTP/1.1	RFC 2068, 2616
ICMP	RFC 792, 950
Internet Host-Apps	RFC 1123
Internet Host-Comm.	RFC 1122
IP	RFC 791
MIME	RFC 1341
NFS v2	RFC 1094
NFS v3	RFC 1813
NTPv3	RFC 1305
RTP	RFC 1889, 1890, 2833
SIP	RFC 2543 RFC2543bis-03 RFC 2976, “The SIP Info Method” draft-ietf-sip-session-timer-04 RFC 2976 RFC 4240 draft-vandyke-mscml-09, “Media Server Control Markup Language (MSCML) and Protocol”, Van Dyke, J., Burger, E., July 2006, work in progress
SDP	RFC 2327
TELNET	RFC 854

Table 20. Supported Protocols and Standards (Continued)

Protocols	RFC #
TFTPv2	RFC 1350
URI	RFC 2396
URL	1738
VXML	V1.0, V2.0 W3C

Product Safety and Emissions - Regulatory Compliance Notices

The IP Media Server complies with industry safety and emissions requirements, as indicated below.

Safety	UL 60950-1, First Edition CAN/CSA-C22.2 No. 60950-1-03 EN 60950-1:2001 IEC 60950-1:2001	USA Canada Europe Global (CB)
EMC Emissions	FCC 47 CFR Part 15 Class A ICES-003 Issue 3 Class A EN 55022:1998/A1:2000/A2:2003 Class A VCCI Class A ITE AS/NZS CISPR22:2002 Class A	USA Canada Europe Japan Australia
EMC Immunity	EN 55024:1998/A1:2001/A2:2003 EN 61000-3-2:2000 EN 61000-3-3:1995/A1:2001	Europe Europe Europe

EN 550022 Class A Required Warning

Warning: This is a Class A product. In a domestic environment, this product can cause radio interference, in which case the user might be required to take adequate measures.

United States:
FCC CFR 47 Part 15 Required Instructions

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this manual, can cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user is required to correct the interference at his own expense.

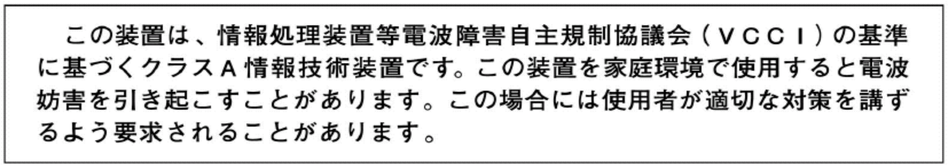
Canada

This Class A digital apparatus complies with Canadian Standard ICES-003.

Cet appareil numérique de la class A est conforme à la norme NMB-003 du Canada.

VCCI Japan

ITE Class A Statement (For Class A Products).



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Translation: This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

B - Troubleshooting

This appendix describes some basic trouble shooting techniques you can use when working with the IP Media Server. It includes the following topics:

- Collecting Information for Technical Support
- Log Files
- Network Connectivity
- Current Calls
- Establishing Sessions Using Complex Codecs Immediately After Power Up
- NFS Mounted Devices
- Recovering after a Power Failure

Collecting Information for Technical Support

As part of the issue reporting process, download log files and any core dump files from the IP Media Server and send a zipped version of these files to Dialogic Technical Support, together with the running configuration files. You can upload the collected log files to the Dialogic® IP Media Server Technical Support FTP server. Please contact Dialogic Technical Support to obtain a user account and password.

- *audit.log*
- *cache.log*
- *cache_access.log*
- *dms.log*
- *fido.log* (and any *fido.log.1*, *fido.log.2*, etc.)
- *mserv.log* (and any *mserv.log.1*, *mserv.log.2*, etc.)
- *msinit.log* (and any *msinit.log.1*, *msinit.log.2*, etc.)
- *msprovider.log*
- *sipd.log* (and any *sipd.log.1*, *sipd.log.2*, etc.)
- *uad.log** (and any *uad.log.1*, *uad.log.2*, etc.)
- *vxmld.log** (and any *vxmld.log.1*, *vxmld.log.2*, etc.)
- *<hostname>_system_info.log*
- Any and all core files
- Running configuration: *g2mscurrent.tar.gz* file, and the version and build of the IP Media Server software you are running.
- *accounting.log* (and any accounting.log.1, accounting.log.2 etc)
- *msaccounting.log* and any msaccounting.log.1, msaccounting.log.2 etc.
- *snowshore_additional_install.log*

* These files are only required when the reported issues involve VoiceXML applications.

Log Files

The log files contain detailed information about the operation of the IP Media Server. The log files include:

Table 21. IP Media Server Log Files

File	Contents
audit.log	IP Media Server persisted settings.
fido.log	Messages associated with fetching Internet domain objects (files, vxml pages over http).
email_to_fax	Information regarding email to fax
mserv.log	Details of creating and managing RTP streams on the IP Media Server.
msinit.log	Log entries of the IP Media Server initialization.
msprovider.log	License information.
sipd.log	SIP messages received and sent by the IP Media Server.
sr140app.log	Details of creating and managing fax on the IP Media Server.
uad.log	Internal messages associated with VoiceXML transfer functions.
vxmld.log	VoiceXML 1.0 messages on the IP Media Server.
pw_metricsfile	Record of VoiceXML 2.0 messages on the IP Media Server.
accounting.log	clear text log created from the generate accounting log button in logconfigure
msaccounting.log	encrypted log created from the Generate accounting log button in logconfigure.
snowshore_additional_install.log	Use to verify installation or upgrade.

The primary log file for troubleshooting call setup issues is the sipd log. This log file can be viewed and processed to look for all the messages for a particular call. Each message carries a time stamp. Useful tags to search for in the log file are:

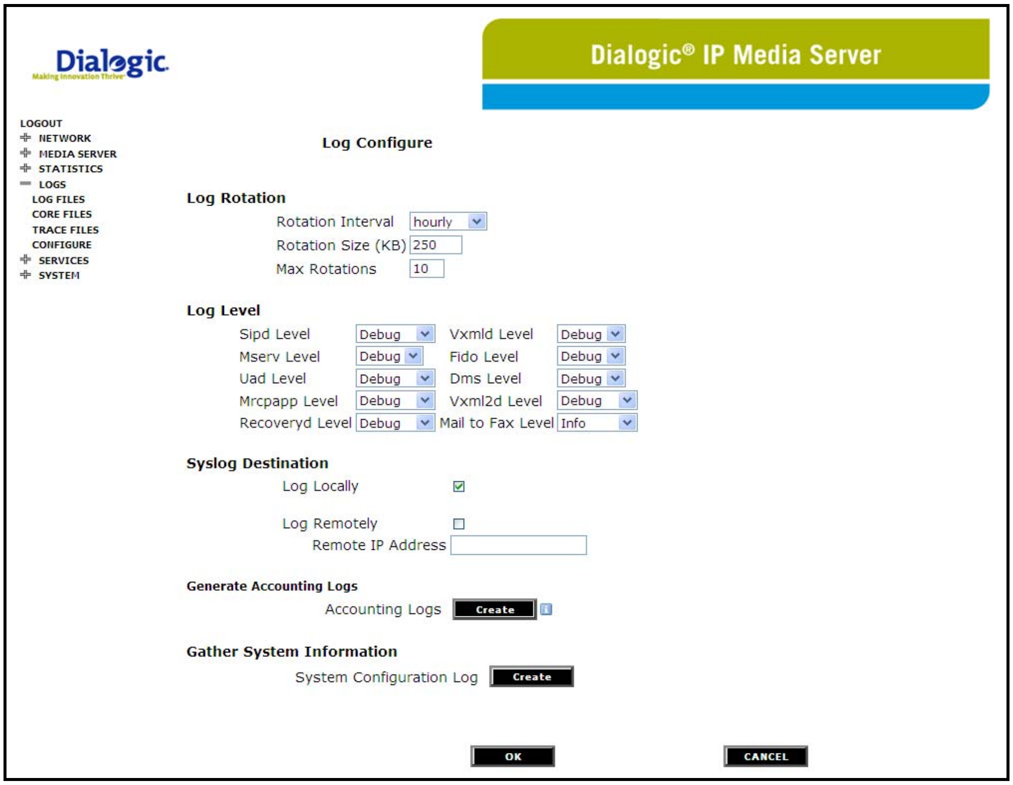
1 By Call-ID: For example, using *Call-ID: 12995-7@172.17.100.245* can find all the SIP messages associated with a particular call.

2 By 400 and 500 type messages: For example, using *SIP/2.0 400* or *SIP/2.0 500* can find all error messages in the file. These messages can be related to a particular call, and often lead to the reason the call failed.

In addition to these log files, it would be useful for you to generate the system information log file at the time the issue occurs. To generate this log file:

1 Log in to the IP Media Server Web UI.

2 Select LOGS→CONFIGURE to display the Log Configure page:



Log Configure

Log Rotation

Rotation Interval: hourly
Rotation Size (KB): 250
Max Rotations: 10

Log Level

Sipd Level	Debug	Vxmld Level	Debug
Mserv Level	Debug	Fido Level	Debug
Uad Level	Debug	Dms Level	Debug
Mrcpapp Level	Debug	Vxml2d Level	Debug
Recoveryd Level	Debug	Mail to Fax Level	Info

Syslog Destination

Log Locally ☑

Log Remotely ☐
Remote IP Address

Generate Accounting Logs

Accounting Logs

Gather System Information

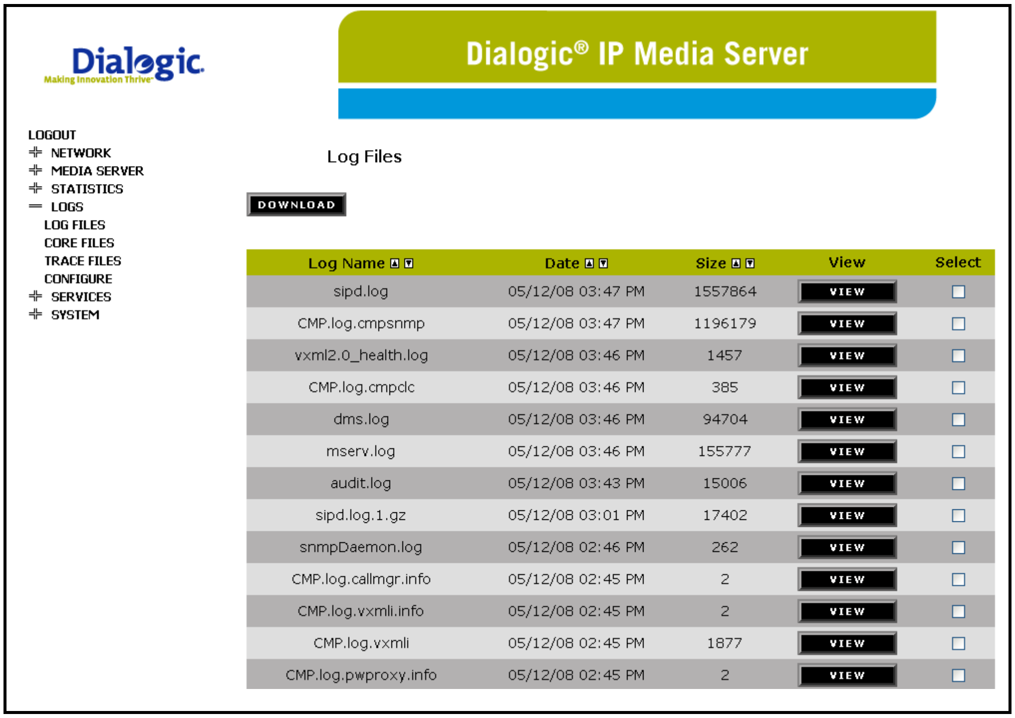
System Configuration Log

Figure 85. Log Configure Page

3 Click the System Configuration Log Create button.

4 Click OK.

The log file is generated and the Log Files page is displayed:



Log Files

Log Name	Date	Size	View	Select
sipd.log	05/12/08 03:47 PM	1557864	VIEW	□
CMP.log.cmpsnmp	05/12/08 03:47 PM	1196179	VIEW	□
vxml2.0_health.log	05/12/08 03:46 PM	1457	VIEW	□
CMP.log.cmpclc	05/12/08 03:46 PM	385	VIEW	□
dms.log	05/12/08 03:46 PM	94704	VIEW	□
mserv.log	05/12/08 03:46 PM	155777	VIEW	□
audit.log	05/12/08 03:43 PM	15006	VIEW	□
sipd.log.1.gz	05/12/08 03:01 PM	17402	VIEW	□
snmpDaemon.log	05/12/08 02:46 PM	262	VIEW	□
CMP.log.callmgr.info	05/12/08 02:45 PM	2	VIEW	□
CMP.log.vxmli.info	05/12/08 02:45 PM	2	VIEW	□
CMP.log.vxmli	05/12/08 02:45 PM	1877	VIEW	□
CMP.log.pwproxy.info	05/12/08 02:45 PM	2	VIEW	□

Figure 86. Log Files Page

The file <hostname>_system_info.log is the name of the file that was created.

Network Connectivity

If a call cannot be successfully placed, check that there is connectivity to the required networks.

1 Ping the devices used in the call: Using the NETWORK→UTILITIES→PING command, try pinging the application server IP address and the IP address of the RTP device.

2 If either ping command fails, check to ensure that the interfaces are active (NETWORK→INTERFACES) and that one of the interfaces is designated as supporting SIP and RTP.

3 Check the routing table for routes, network masks, and default gateways.

Current Calls

To determine how many calls are currently active on the system, use the statistics page on the Web UI. This command displays the current number of calls on the IP Media Server for a given application service type.

Establishing Sessions Using Complex Codecs Immediately After Power Up

If establishing sessions using a complex codec (G.726, G.729, AMR) on the EdgeMedia EDP-10 DSP card, please note that it takes approximately one minute for the card to initialize after the rest of the IP Media Server processes have completed initialization. If calls are placed during that time, the following SIP response will be returned:

480 BUSY HERE

and the following error message is logged:

```
create_rtp: resultcode=400 Resulttext=”Busy”
   reason=”Out of hw_assist resources”
```

NFS Mounted Devices

NFS mounted devices can be used to retrieve remote announcements. These devices are auto-mounted by the IP Media Server. This requires that the NFS server has exported its disks for mounting. If it appears that a server could not be accessed (because error messages were seen in the SIP, mserv, and fido logs), check that:

1 The device can be reached over the network (ping).

2 The NFS server has the correct permissions for exporting its disk.

Recovering after a Power Failure

When a system reboots, it does a file system check. Under most circumstances, the system recovers automatically and reboots. In rare circumstances, the system can have issues and be unable to recover the file system. In this case, use the following procedure.

1. Connect to the serial port of the IP Media Server.
2. Power up the system and watch the terminal page. As the file check happens, it can find bad files that need to be repaired.
3. When asked to repair a file, type `y`.

   At the end of this process, the system should reboot and recover.

If the system does not recover, contact Dialogic Technical Support for repair and return procedures.

Note: It is recommended that a UPS be used to power the system to avoid issues from power fluctuations.

C - Required Red Hat Enterprise Linux Packages

The following details the inclusive list of Red Hat Enterprise Linux 4 Update 5 packages required for IP Media Server Release 2.5.0 operation.

```
acl-2.2.23-5.3.el4
acpid-1.0.3-2
am-utils-6.0.9-15.RHEL4
anacron-2.3-32
apmd-3.0.2-24
apr-0.9.4-24.5
apr-util-0.9.4-21
ash-0.3.8-20
aspell-0.50.5-4.EL4
aspell-en-0.51-11
at-3.1.8-80+AF8-EL4
atk-1.8.0-2
atk-devel-1.8.0-2
attr-2.4.16-3.1.el4
audit-1.0.15-3.EL4
audit-libs-1.0.15-3.EL4
authconfig-4.6.10-rhel4.3
autofs-4.1.3-199.3
basesystem-8.0-4
bash-3.0-19.3
bc-1.06-17.1
beecrypt-3.1.0-6
bind-libs-9.2.4-24.EL4
bind-utils-9.2.4-24.EL4
binutils-2.15.92.0.2-22
bluez-bluefw-1.0-6
bluez-hcidump-1.11-1
```

```
bluez-libs-2.10-2
bluez-utils-2.10-2.1
BRKTBOSsetup-5.2.2-20
BRKTBOSsetup-fw-3.2.1-32
bzip2-1.0.2-13.EL4.3
bzip2-libs-1.0.2-13.EL4.3
checkpolicy-1.17.5-1
chkconfig-1.3.13.5.EL4-1
chkfontpath-1.10.0-2
cmp-proxy-EL40+AF8-7.0.12-1
cmp-snmp-EL40+AF8-7.0.12-1
compat-libstdc296-2.96-132.7.2
compat-libstdc33-3.2.3-47.3
comps-4ES-0.20070421
coreutils-5.2.1-31.6
cpio-2.5-13.RHEL4
cpp-3.4.6-8
cracklib-2.8.9-1.3
cracklib-dicts-2.8.9-1.3
crash-4.0-3.9
crontabs-1.10-7
cryptsetup-0.1-4
cups-1.1.22-0.rc1.9.20
cups-libs-1.1.22-0.rc1.9.20
curl-7.12.1-11.el4
cyrus-sasl-2.1.19-5.EL4
cyrus-sasl-md5-2.1.19-5.EL4
cyrus-sasl-plain-2.1.19-5.EL4
db4-4.2.52-7.1
dbus-0.22-12.EL.9
dbus-glib-0.22-12.EL.9
desktop-file-utils-0.9-3.el4
device-mapper-1.02.17-3.el4
dhclient-3.0.1-59.EL4
dhcpv6+AF8-client-0.10-17+AF8-EL4
diffutils-2.8.1-12
diskdumputils-1.3.25-1
distcache-1.4.5-6
dmraid-1.0.0.rc14-5+AF8-RHEL4+AF8-U5
dos2unix-3.1-21.2
dosfstools-2.8-18
dump-0.4b39-3.EL4.2
e2fsprogs-1.35-12.5.el4
ed-0.2-36
eject-2.0.13-11
ElectricFence-2.2.2-19
elfutils-0.97.1-4
elfutils-libelf-0.97.1-4
emacs-21.3-19.EL.4
emacs-common-21.3-19.EL.4
emacs-leim-21.3-19.EL.4
enscript-1.6.1-33.el4
```

```
ethtool-1.8-4
expat-1.95.7-4
expect-5.42.1-1
fbset-2.1-17
file-4.10-3.EL4.5
filesystem-2.3.0-1
findutils-4.1.20-7.el4.3
finger-0.17-26.EL4.1
fontconfig-2.2.3-7
fontconfig-devel-2.2.3-7
fonts-xorg-75dpi-6.8.2-1.EL
freetype-2.1.9-5.el4
freetype-devel-2.1.9-5.el4
ftp-0.17-23.EL4
gawk-3.1.3-10.1
gcc-3.4.6-8
gd-2.0.28-5.4E
gdb-6.3.0.0-1.143.el4
gdbm-1.8.0-24
gettext-0.14.1-13
ghostscript-7.07-33
ghostscript-fonts-5.50-13
glib-1.2.10-15
glib2-2.4.7-1
glib2-devel-2.4.7-1
glibc-2.3.4-2.36
glibc-common-2.3.4-2.36
glibc-devel-2.3.4-2.36
glibc-headers-2.3.4-2.36
glibc-kernheaders-2.4-9.1.100.EL
gmp-4.1.4-3
gnupg-1.2.6-9
gnutls-1.0.20-3.2.3
gpm-1.20.1-71.RHEL4
grep-2.5.1-32.3
groff-1.18.1.1-3.EL4
grub-0.95-3.8
gtk2-2.4.13-22
gtk2-devel-2.4.13-22
gzip-1.3.3-16.rhel4
hal-0.4.2-6.EL4
hdparm-5.7-2
hesiod-3.0.2-30
hotplug-2004+AF8-04+AF8-01-7.8
htmlview-3.0.0-8
httpd-2.0.52-32.ent
httpd-suexec-2.0.52-32.ent
hwdata-0.146.28.EL-1
ImageMagick-6.0.7.1-17
indexhtml-4.1-1
info-4.7-5.el4.2
initscripts-7.93.29.EL-1
```

```
iproute-2.6.9-3.EL4.7
ipsec-tools-0.3.3-6.rhel4.1
iptables-1.2.11-3.1.RHEL4
iptstate-1.3-4
iputils-20020927-19.EL4.5
irda-utils-0.9.16-3
isdn4k-utils-3.2-18.p1.1
jpackage-utils-1.7.3-1jpp.1.el4
jwhois-3.2.2-6.EL4.1
kbd-1.12-2.el4.4
kernel-2.6.9-55.EL
kernel-devel-2.6.9-55.EL
kernel-smp-2.6.9-55.EL
kernel-smp-devel-2.6.9-55.EL
kernel-utils-2.4-13.1.99
krb5-libs-1.3.4-47
krb5-workstation-1.3.4-47
krbafs-1.2.2-6
kudzu-1.1.95.22-1
less-382-4.rhel4
lftp-3.0.6-3
lha-1.14i-17
libacl-2.2.23-5.3.el4
libattr-2.4.16-3.1.el4
libcap-1.10-20
libgcc-3.4.6-8
libgcrypt-1.2.0-3
libgpg-error-1.0-1
libgssapi-0.8-1
libidn-0.5.6-1
libjpeg-6b-33
libjpeg-devel-6b-33
libjs-1.5-0.pm.9
libmng-1.0.8-1
libmng-devel-1.0.8-1
libpcap-0.8.3-10.RHEL4
libpng-1.2.7-1.el4.2
libpng-devel-1.2.7-1.el4.2
libselinux-1.19.1-7.3
libsepol-1.1.1-2
libstdc3.4.6-8
libtermcap-2.0.8-39
libtermcap-devel-2.0.8-39
libtiff-3.6.1-12
libtool-libs-1.5.6-4.EL4.1
libungif-4.1.3-1.el4.2
libungif-progs-4.1.3-1.el4.2
libusb-0.1.8-3
libuser-0.52.5-1.el4.1
libwvstreams-3.75.0-2
libxml2-2.6.16-10
libxml2-python-2.6.16-10
```

```
libxslt-1.1.11-1
lm+AF8-sensors-2.8.7-2.40.3
lockdev-1.0.1-6.2
logrotate-3.7.1-6.RHEL4
logwatch-5.2.2-2.EL4
lrzsz-0.12.20-19
lsof-4.72-1.4
lvm2-2.02.21-5.el4
lynx-2.8.5-18.2
m4-1.4.1-16
mailcap-2.1.17-1
mailx-8.1.1-37.EL4
make-3.80-6.EL4
MAKEDEV-3.15.2-3
man-1.5o1-10.rhel4
man-pages-1.67-12.EL4
mdadm-1.12.0-2
mgetty-1.1.31-2
mingetty-1.07-3
minicom-2.00.0-19
mkbootdisk-1.5.2-1
mkinitrd-4.2.1.10-1.1
mktemp-1.5-20
mod+AF8-auth+AF8-pgsql-2.0.1-7.1
mod+AF8-perl-1.99+AF8-16-4
mod+AF8-ssl-2.0.52-32.ent
module-init-tools-3.1-0.pre5.3.4
mtools-3.9.9-9
mtr-0.54-10
mt-st-0.8-1
mx-2.0.5-3
nano-1.2.4-1
nc-1.10-22
ncurses-5.4-13
ncurses-devel-5.4-13
netconfig-0.8.21-1.1
netdump-0.7.16-10
net-snmp-5.1.2-11.EL4.10
net-snmp-libs-5.1.2-11.EL4.10
net-snmp-utils-5.1.2-11.EL4.10
net-tools-1.60-37.EL4.9
NetworkManager-0.3.1-4.el4
newt-0.51.6-9.rhel4
nfs-utils-1.0.6-80.EL4
nfs-utils-lib-1.0.6-8
nscd-2.3.4-2.36
nss+AF8-db-2.2-29
nss+AF8-ldap-226-18
ntp-4.2.0.a.20040617-6.el4
ntsysv-1.3.13.5.EL4-1
numactl-0.6.4-1.39
openldap-2.2.13-7.4E
```

```
openssh-3.9p1-8.RHEL4.20
openssh-clients-3.9p1-8.RHEL4.20
openssh-server-3.9p1-8.RHEL4.20
openssl-0.9.7a-43.16
pam+AF8-ccreds-3-3.rhel4.2
pam+AF8-krb5-2.1.8-1
pam+AF8-passwdqc-0.7.5-2
pam+AF8-smb-1.1.7-5
pam-0.77-66.21
pango-1.6.0-9
pango-devel-1.6.0-9
parted-1.6.19-16.EL
passwd-0.68-10.1
patch-2.5.4-20
pax-3.0-9
pciutils-2.1.99.test8-3.4
pcmcia-cs-3.2.7-3.5
pcre-4.5-3.2.RHEL4
pdksh-5.2.14-30.3
perl-5.8.5-36.RHEL4
perl-Filter-1.30-6
perl-URI-1.30-4
phoneweb-EL40+AF8-7.0.12-1
php-4.3.9-3.22.4
php-pear-4.3.9-3.22.4
php-pgsql-4.3.9-3.22.4
pinfo-0.6.8-7
pkgconfig-0.15.0-3
policycoreutils-1.18.1-4.12
popt-1.9.1-22+AF8-nonptl
portmap-4.0-63
postgresql-7.4.16-1.RHEL4.1
postgresql-docs-7.4.16-1.RHEL4.1
postgresql-libs-7.4.16-1.RHEL4.1
postgresql-server-7.4.16-1.RHEL4.1
ppp-2.4.2-6.4.RHEL4
prelink-0.3.3-0.EL4
procmail-3.22-14
procps-3.2.3-8.6
psacct-6.3.2-39.rhel4
psmisc-21.4-4.1
pyOpenSSL-0.6-1.p23
python-2.3.4-14.4
pyxf86config-0.3.19-1
PyXML-0.8.3-6
qt-3.3.3-10.RHEL4
qt-devel-3.3.3-10.RHEL4
quota-3.12-6.el4
rdate-1.4-2
rdist-6.1.5-38.40.2
readline-4.3-13
readline-devel-4.3-13
```

```
redhat-logos-1.1.26-1
redhat-lsb-3.0-8.EL
redhat-menus-3.7.1-2
redhat-release-4ES-6.1
rhnlib-2.1.1-3.el4
rhpl-0.148.5-1
rmt-0.4b39-3.EL4.2
rootfiles-8-1
rpm-4.3.3-22+AF8-nonptl
rpmdb-redhat-4-0.20070421
rpm-libs-4.3.3-22+AF8-nonptl
rpm-python-4.3.3-22+AF8-nonptl
rp-pppoe-3.5-22
rsh-0.17-25.4
rsync-2.6.3-1
schedutils-1.4.0-2
seamonkey-nspr-1.0.8-0.2.el4
sed-4.1.2-6.el4
selinux-policy-targeted-1.17.30-2.145
sendmail-8.13.1-3.2.el4
sendmail-cf-8.13.1-3.2.el4
setarch-1.6-1
setools-2.3-4
setserial-2.17-17
setup-2.5.37-1.3
setuptool-1.17-2
sg3+AF8-utils-1.22-3.1
sg3+AF8-utils-libs-1.22-3.1
shadow-utils-4.0.3-61.RHEL4
slang-1.4.9-8
slocate-2.7-13.el4.6
specspo-9.0.92-1.3
squid-2.5.STABLE14-1.4E
star-1.5a25-6
statserial-1.1-35
strace-4.5.15-1.el4.1
stunnel-4.05-3
sudo-1.6.7p5-30.1.3
symlinks-1.2-22
sysklogd-1.4.1-26+AF8-EL
syslinux-2.11-1
sysreport-1.3.15-8
system-config-mouse-1.2.9-1
system-config-network-tui-1.3.22.0.EL.4.2-1
system-config-securitylevel-tui-1.4.19.2-1
SysVinit-2.85-34.4
talk-0.17-26
tar-1.14-12.RHEL4
tcl-8.4.7-2
tcp+AF8-wrappers-7.6-37.2
tcpdump-3.8.2-10.RHEL4
tcsh-6.13-9.el4.1
```

```
telnet-0.17-31.EL4.3
termcap-5.4-3
time-1.7-25
tmpwatch-2.9.1-1
traceroute-1.4a12-24.EL4.1
ttmkfdir-3.0.9-20.el4
tzdata-2007d-1.el4
udev-039-10.15.EL4
unix2dos-2.2-24.1
unixODBC-2.2.11-1.RHEL4.1
unzip-5.51-9.EL4.5
up2date-4.5.5-5.el4
urw-fonts-2.2-6.1
usbutils-0.11-7.RHEL4.1
usermode-1.74-2
utempter-0.5.5-5
util-linux-2.12a-16.EL4.25
valgrind-3.1.1-1.EL4
valgrind-callgrind-0.10.1-2.EL4
vconfig-1.8-4
VFlib2-2.25.6-25
vg-scriptmanager-4.0.0-1
vg-setup-2.0.0-3
vg-xerces-EL40-2.0.0-3
vim-common-6.3.046-0.40E.7
vim-enhanced-6.3.046-0.40E.7
vim-minimal-6.3.046-0.40E.7
vixie-cron-4.1-44.EL4
vsftpd-2.0.1-5.EL4.5
wget-1.10.2-0.40E
which-2.16-4
wireless-tools-28-0.pre16.3.3.EL4
wireshark-0.99.5-EL4.1
words-3.0-3.2
wvdial-1.54.0-3
Xaw3d-1.5-24
Xerces-c-2.3.0-37
xinetd-2.3.13-4.4E.1
xmlsec1-1.2.6-3
xmlsec1-openssl-1.2.6-3
xorg-x11-devel-6.8.2-1.EL.18
xorg-x11-font-utils-6.8.2-1.EL.18
xorg-x11-libs-6.8.2-1.EL.18
xorg-x11-Mesa-libGL-6.8.2-1.EL.18
xorg-x11-xfs-6.8.2-1.EL.18
ypbind-1.17.2-13
yp-tools-2.8-7
zip-2.3-27
zlib-1.2.1.2-1.2
zlib-devel-1.2.1.2-1.2
```

The following details the inclusive list of Red Hat Enterprise Linux 5 Update 1 packages required for IP Media Server Release 2.5.0 operation.

```
acl-2.2.39-2.1.el5
acpid-1.0.4-5
amtu-1.0.4-4
anacron-2.3-45.el5
apmd-3.2.2-5
apr-1.2.7-11
apr-util-1.2.7-6
aspell-0.60.3-7.1
aspell-en-6.0-2.1
at-3.1.8-82.fc6
atk-1.12.2-1.fc6
atk-devel-1.12.2-1.fc6
attr-2.4.32-1.1
audit-1.5.5-7.el5
audit-libs-1.5.5-7.el5
audit-libs-python-1.5.5-7.el5
authconfig-5.3.12-2.el5
autofs-5.0.1-0.rc2.55
basesystem-8.0-5.1.1
bash-3.1-16.1
bc-1.06-21
beecrypt-4.1.2-10.1.1
bind-libs-9.3.3-10.el5
bind-utils-9.3.3-10.el5
binutils-2.17.50.0.6-5.el5
bluez-gnome-0.5-5.fc6
bluez-hcidump-1.32-1
bluez-libs-3.7-1
bluez-utils-3.7-2
BRKTBOSsetup-5.2.2-20
BRKTBOSsetup-fw-3.2.1-32
bzip2-1.0.3-3
bzip2-libs-1.0.3-3
cairo-1.2.4-2.el5
ccid-1.0.1-6.el5
checkpolicy-1.33.1-2.el5
chkconfig-1.3.30.1-1
chkfontpath-1.10.1-1.1
cmp-proxy-EL40+AF8-7.0.12-1
cmp-snmp-EL40+AF8-7.0.12-1
compat-libstdc296-2.96-138
compat-libstdc33-3.2.3-61
comps-extras-11.1-1.1
conman-0.1.9.2-8.el5
coolkey-1.1.0-5.el5
coreutils-5.97-12.1.el5
cpio-2.6-20
cpp-4.1.2-14.el5
cpuspeed-1.2.1-1.48.el5
cracklib-2.8.9-3.3
```

```
cracklib-dicts-2.8.9-3.3
crash-4.0-4.6.1
crontabs-1.10-8
cryptsetup-luks-1.0.3-2.2.el5
cups-1.2.4-11.14.el5
cups-libs-1.2.4-11.14.el5
curl-7.15.5-2.el5
cyrus-sasl-2.1.22-4
cyrus-sasl-lib-2.1.22-4
cyrus-sasl-plain-2.1.22-4
db4-4.3.29-9.fc6
dbus-1.0.0-6.el5
dbus-glib-0.70-5
dbus-python-0.70-7.el5
Deployment+AF8-Guide-en-US-5.1.0-11
desktop-file-utils-0.10-7
device-mapper-1.02.20-1.el5
device-mapper-multipath-0.4.7-12.el5
dhcdbd-2.2-1.el5
dhclient-3.0.5-7.el5
dhcpv6+AF8-client-0.10-33.el5
diffutils-2.8.1-15.2.2
distcache-1.4.5-14.1
dmidecode-2.7-1.28.2.el5
dmraid-1.0.0.rc13-4.el5
dos2unix-3.1-27.1
dosfstools-2.11-6.2.el5
dump-0.4b41-2.fc6
e2fsprogs-1.39-10.el5
e2fsprogs-libs-1.39-10.el5
ed-0.2-38.2.2
eject-2.1.5-4.2.el5
ElectricFence-2.2.2-20.2.2
elfutils-0.125-3.el5
elfutils-libelf-0.125-3.el5
elfutils-libelf-devel-0.125-3.el5
emacs-common-21.4-19.el5
emacs-leim-21.4-19.el5
enscript-1.6.4-4.1.el5
ethtool-5-1.el5
expat-1.95.8-8.2.1
expect-5.43.0-5.1
fbset-2.1-22
file-4.17-9.0.1.el5
filesystem-2.4.0-1
findutils-4.2.27-4.1
finger-0.17-32.2.1.1
firstboot-tui-1.4.27.3-1.el5
fontconfig-2.4.1-6.el5
fontconfig-devel-2.4.1-6.el5
freetype-2.2.1-19.el5
freetype-devel-2.2.1-19.el5
```

```
ftp-0.17-33.fc6
gawk-3.1.5-14.el5
gcc-4.1.2-14.el5
GConf2-2.14.0-9.el5
gd-2.0.33-9.3.fc6
gdb-6.5-25.el5
gdbm-1.8.0-26.2.1
gettext-0.14.6-4.el5
ghostscript-8.15.2-9.1.el5
ghostscript-fonts-5.50-13.1.1
giflib-4.1.3-7.1.el5.1
glib2-2.12.3-2.fc6
glib2-devel-2.12.3-2.fc6
glibc-2.5-18
glibc-common-2.5-18
glibc-devel-2.5-18
glibc-headers-2.5-18
gmp-4.1.4-10.el5
gnome-python2-gconf-2.16.0-1.fc6
gnu-efi-3.0c-1.1
gnupg-1.4.5-13
gnutls-1.4.1-2
gpm-1.20.1-74.1
grep-2.5.1-54.2.el5
groff-1.18.1.1-11.1
grub-0.97-13
gtk2-2.10.4-19.el5
gtk2-devel-2.10.4-19.el5
gzip-1.3.5-9.el5
hal-0.5.8.1-25.el5
hdparm-6.6-2
hesiod-3.1.0-8
htmlview-4.0.0-1.el5
httpd-2.2.3-11.el5
hwdata-0.211-1
ifd-egate-0.05-15
ImageMagick-6.2.8.0-3.el5.4
info-4.8-14.el5
initscripts-8.45.17.EL-1
iproute-2.6.18-4.el5
ipsec-tools-0.6.5-8.el5
iptables-1.3.5-1.2.1
iptables-ipv6-1.3.5-1.2.1
iptstate-1.4-1.1.2.2
iputils-20020927-43.el5
irda-utils-0.9.17-2.fc6
irqbalance-0.55-6.el5
isdn4k-utils-3.2-50.1
jpackage-utils-1.7.3-1jpp.2.el5
jwhois-3.2.3-8.el5
kbd-1.12-19.el5
kernel-2.6.18-53.el5
```

```
kernel-devel-2.6.18-53.el5
kernel-headers-2.6.18-53.el5
kexec-tools-1.101-194.4.el5
keyutils-libs-1.2-1.el5
kpartx-0.4.7-12.el5
krb5-libs-1.6.1-17.el5
krb5-workstation-1.6.1-17.el5
ksh-20060214-1.4
kudzu-1.2.57.1.15-1
less-394-5.el5
lftp-3.5.1-2.fc6
libacl-2.2.39-2.1.el5
libaio-0.3.106-3.2
libattr-2.4.32-1.1
libcap-1.10-26
libdrm-2.0.2-1.1
libevent-1.1a-3.2.1
libFS-1.0.0-3.1
libgcc-4.1.2-14.el5
libgcrypt-1.2.3-1
libgpg-error-1.4-2
libgssapi-0.10-2
libhugetlbfs-1.0.1-1.el5
libhugetlbfs-lib-1.0.1-1.el5
libICE-1.0.1-2.1
libIDL-0.8.7-1.fc6
libidn-0.6.5-1.1
libjpeg-6b-37
libjpeg-devel-6b-37
libjs-1.5-0.pm.9
libmng-1.0.9-5.1
libmng-devel-1.0.9-5.1
libnl-1.0-0.10.pre5.4
libnotify-0.4.2-6.el5
libpcap-0.9.4-11.el5
libpng-1.2.10-7.0.2
libpng-devel-1.2.10-7.0.2
libselinux-1.33.4-4.el5
libselinux-python-1.33.4-4.el5
libsemanage-1.9.1-3.el5
libsepol-1.15.2-1.el5
libSM-1.0.1-3.1
libstdc4.1.2-14.el5
libsysfs-2.0.0-6
libtermcap-2.0.8-46.1
libtermcap-devel-2.0.8-46.1
libtiff-3.8.2-7.el5
libtool-ltdl-1.5.22-6.1
libusb-0.1.12-5.1
libuser-0.54.7-2.el5.2
libutempter-1.1.4-3.fc6
libvolume+AF8-id-095-14.9.el5
```

```
libwnck-2.16.0-4.fc6
libwvstreams-4.2.2-2.1
libX11-1.0.3-8.0.1.el5
libXau-1.0.1-3.1
libXcursor-1.1.7-1.1
libXdmcp-1.0.1-2.1
libXext-1.0.1-2.1
libXfixes-4.0.1-2.1
libXft-2.1.10-1.1
libXi-1.0.1-3.1
libXinerama-1.0.1-2.1
libxml2-2.6.26-2.1.2
libxml2-python-2.6.26-2.1.2
libXrandr-1.1.1-3.1
libXrender-0.9.1-3.1
libXres-1.0.1-3.1
libxslt-1.1.17-2
libXt-1.0.2-3.1.fc6
libXxf86vm-1.0.1-3.1
lm+AF8-sensors-2.10.0-3.1
lockdev-1.0.1-10
logrotate-3.7.4-7
logwatch-7.3-5
lrzsz-0.12.20-22.1
lsof-4.78-3
lvm2-2.02.26-3.el5
lynx-2.8.5-28.1
m2crypto-0.16-6.el5.1
m4-1.4.5-3.el5.1
mailcap-2.1.23-1.fc6
mailx-8.1.1-44.2.2
make-3.81-1.1
MAKEDEV-3.23-1.2
man-1.6d-1.1
man-pages-2.39-10.el5
mcstrans-0.2.6-1.el5
mdadm-2.5.4-3.el5
mesa-libGL-6.5.1-7.5.el5
mgetty-1.1.33-9.fc6
microcode+AF8-ctl-1.17-1.42.el5
mingetty-1.07-5.2.2
minicom-2.1-3
mkbootdisk-1.5.3-2.1
mkinitrd-5.1.19.6-19
mktemp-1.5-23.2.2
mlocate-0.15-1.el5
mod+AF8-perl-2.0.2-6.3.el5
mod+AF8-ssl-2.2.3-11.el5
module-init-tools-3.3-0.pre3.1.34.el5
mozldap-6.0.4-1.el5
mtools-3.9.10-2.fc6
mtr-0.71-3.1
```

```
mx-2.0.6-2.2.2
nano-1.3.12-1.1
nash-5.1.19.6-19
nc-1.84-10.fc6
ncurses-5.5-24.20060715
ncurses-devel-5.5-24.20060715
net-snmp-5.3.1-19.el5
net-snmp-libs-5.3.1-19.el5
net-tools-1.60-73
NetworkManager-0.6.4-6.el5
newt-0.52.2-9
nfs-utils-1.0.9-24.el5
nfs-utils-lib-1.0.8-7.2.z2
notification-daemon-0.3.5-8.el5
nscd-2.5-18
nspr-4.6.5-3.el5
nss+AF8-db-2.2-35.1
nss+AF8-ldap-253-5.el5
nss-3.11.7-1.3.el5
nss-tools-3.11.7-1.3.el5
ntp-4.2.2p1-7.el5
ntsysv-1.3.30.1-1
numactl-0.9.8-2.el5
OpenIPMI-2.0.6-5.el5.4
OpenIPMI-libs-2.0.6-5.el5.4
openldap-2.3.27-8
openssh-4.3p2-24.el5
openssh-clients-4.3p2-24.el5
openssh-server-4.3p2-24.el5
openssl-0.9.8b-8.3.el5+AF8-0.2
ORBit2-2.14.3-4.el5
pam+AF8-ccreds-3-5
pam+AF8-krb5-2.2.14-1
pam+AF8-passwdqc-1.0.2-1.2.2
pam+AF8-pkcs11-0.5.3-23
pam+AF8-smb-1.1.7-7.2.1
pam-0.99.6.2-3.26.el5
pango-1.14.9-3.el5
pango-devel-1.14.9-3.el5
paps-0.6.6-17.el5
parted-1.8.1-12.el5
passwd-0.73-1
patch-2.5.4-29.2.2
pax-3.4-1.2.2
pciutils-2.2.3-4
pcmciautils-014-5
pcre-6.6-1.1
pcsc-lite-1.3.1-7
pcsc-lite-libs-1.3.1-7
perl-5.8.8-10
perl-String-CRC32-1.4-2.fc6
perl-URI-1.35-3
```

```
phoneweb-EL40+AF8-7.0.12-1
php-5.1.6-15.el5
pinfo-0.6.9-1.fc6
pkgconfig-0.21-1.fc6
pkinit-nss-0.7.3-1.el5
pm-utils-0.99.3-6.el5.17
policycoreutils-1.33.12-12.el5
popt-1.10.2-47.el5
portmap-4.0-65.2.2.1
postgresql-8.1.9-1.el5
postgresql-docs-8.1.9-1.el5
postgresql-libs-8.1.9-1.el5
postgresql-server-8.1.9-1.el5
ppp-2.4.4-1.el5
prelink-0.3.9-2.1
procmail-3.22-17.1
procps-3.2.7-8.1.el5
psacct-6.3.2-41.1
psmisc-22.2-5
pygobject2-2.12.1-5.el5
pyOpenSSL-0.6-1.p24.7.2.2
python-2.4.3-19.el5
python-elementtree-1.2.6-5
python-sqlite-1.1.7-1.2.1
python-urlgrabber-3.1.0-2
pyxf86config-0.3.31-2.fc6
PyXML-0.8.4-4
qt-3.3.6-23.el5
quota-3.13-1.2.3.2.el5
rdate-1.4-6
rdist-6.1.5-44
readahead-1.3-7.el5
readline-5.1-1.1
readline-devel-5.1-1.1
redhat-logos-4.9.16-1
redhat-lsb-3.1-12.3.EL
redhat-menus-6.7.8-2.el5
redhat-release-5Server-5.1.0.2
redhat-release-notes-5Server-9
rhel-instnum-1.0.7-1.el5
rhn-check-0.4.16-1.el5
rhn-client-tools-0.4.16-1.el5
rhnlib-2.2.5-1.el5
rhnsd-4.6.1-1.el5
rhn-setup-0.4.16-1.el5
rhpl-0.194.1-1
rmt-0.4b41-2.fc6
rng-utils-2.0-1.14.1.fc6
rootfiles-8.1-1.1.1
rpm-4.4.2-47.el5
rpm-libs-4.4.2-47.el5
rpm-python-4.4.2-47.el5
```

```
rp-pppoe-3.5-32.1
rsh-0.17-37.el5
rsync-2.6.8-3.1
sed-4.1.5-5.fc6
selinux-policy-2.4.6-104.el5
selinux-policy-targeted-2.4.6-104.el5
sendmail-8.13.8-2.el5
sendmail-cf-8.13.8-2.el5
setarch-2.0-1.1
setools-3.0-3.el5
setserial-2.17-19.2.2
setup-2.5.58-1.el5
setuptool-1.19.2-1
shadow-utils-4.0.17-12.el5
slang-2.0.6-4.el5
smartmontools-5.36-3.1.el5
sos-1.7-9.1.el5
specspo-13-1.el5
sqlite-3.3.6-2
squid-2.6.STABLE6-4.el5
startup-notification-0.8-4.1
strace-4.5.16-1.el5.1
stunnel-4.15-2
sudo-1.6.8p12-10
svrcore-4.0.4-3.el5
symlinks-1.2-24.2.2
sysfsutils-2.0.0-6
sysklogd-1.4.1-40.el5
syslinux-3.11-4
system-config-network-tui-1.3.99-2.el5
system-config-securitylevel-tui-1.6.29.1-1.el5
SysVinit-2.86-14
talk-0.17-29.2.2
tar-1.15.1-23.0.1.el5
tcl-8.4.13-3.fc6
tcp+AF8-wrappers-7.6-40.4.el5
tcpdump-3.9.4-11.el5
tcsh-6.14-12.el5
telnet-0.17-38.el5
termcap-5.5-1.20060701.1
time-1.7-27.2.2
tmpwatch-2.9.7-1.1.el5.1
traceroute-2.0.1-2.el5
tree-1.5.0-4
ttmkfdir-3.0.9-23.el5
tzdata-2007d-1.el5
udev-095-14.9.el5
unix2dos-2.2-26.2.2
unixODBC-2.2.11-7.1
unzip-5.52-2.2.1
urw-fonts-2.3-6.1.1
usbutils-0.71-2.1
```

```
usermode-1.88-3.el5
util-linux-2.13-0.45.el5
valgrind-3.2.1-6.el5
vconfig-1.9-2.1
vg-scriptmanager-4.0.0-1
vg-setup-2.0.0-3
vg-xerces-EL40-2.0.0-3
vim-common-7.0.109-3.el5.3
vim-enhanced-7.0.109-3.el5.3
vim-minimal-7.0.109-3.el5.3
vixie-cron-4.1-72.el5
vsftpd-2.0.5-10.el5
wget-1.10.2-7.el5
which-2.16-7
wireless-tools-28-2.el5
wireshark-0.99.6-1.el5
words-3.0-9
wpa+AF8-supplicant-0.4.8-10.1.fc6
wvdial-1.54.0-5.2.2.1
Xaw3d-1.5E-10.1
Xerces-c-2.3.0-37
xmlsec1-1.2.9-8.1
xorg-x11-filesystem-7.1-2.fc6
xorg-x11-fonts-ISO8859-1-75dpi-7.1-2.1.el5
xorg-x11-font-utils-7.1-2
xorg-x11-proto-devel-7.1-9.fc6
xorg-x11-xfs-1.0.2-4
ypbind-1.19-8.el5
yp-tools-2.9-0.1
yum-3.0.1-5.el5
yum-metadata-parser-1.0-8.fc6
yum-rhn-plugin-0.5.2-3.el5
yum-security-1.0.4-3.el5
yum-updatesd-3.0.1-5.el5
zip-2.31-1.2.2
zlib-1.2.3-3
zlib-devel-1.2.3-3
```

Index