



PoE VoIP Paging Server Operations Guide

*SiP Compliant
Part #010878*

Document Part #930132F
for Firmware Version 1.2.0

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

Operations Guide 930132F
SiP Compliant 010878

COPYRIGHT NOTICE:

© 2011, CyberData Corporation, ALL RIGHTS RESERVED.

This manual and related materials are the copyrighted property of CyberData Corporation. No part of this manual or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This manual, and the products, software, firmware, and/or hardware described in this manual are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this manual, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this manual or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this manual or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this manual and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) "open source" or "free software" licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software.

Software or firmware developed by Cyberdata that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.



Phone: (831) 373-2601
Technical Support Ext. 333
support@CyberData.net
Fax: (831) 373-4193
Company and product information at www.CyberData.net

Revision History

Revision	Date Released	Description of Changes
A	3/01/2007	This is the first release of this manual
B	4/13/2007	Changes the Authenticate ID and password character limit from 30 to 25 in Table 2-4, "SIP Setup Parameters" .
C	6/12/2007	Removes step "Select Partition 1 or Partition 2 for the Kernel and the Application" in Section 2.8, "Rebooting the Paging Server" .
D	3/10/2008	Adds information about the Multicast TTL in Chapter 2, "Implementing the VoIP Paging Server (Table 2-5, "PGROUPS Setup Parameters") and Chapter C, "How to Use the Multicast Extensions" .
E	1/22/2009	<p>Firmware updated to version 1.2.0. which adds a feature to bypass the DTMF entry. If the DTMF is bypassed, the Paging Server will relay audio to Paging Group 00.</p> <p>Updates Figure 2-10, "PGROUPS Setup"</p> <p>Updates Table 2-5, "PGROUPS Setup Parameters"</p> <p>Adds Note about where to obtain the latest firmware in Section 2.7, "Upgrading the Firmware".</p> <p>Firmware: This revision provides information for firmware version 1.2.0. Release notes detailing the difference between this firmware version and earlier firmware versions is available in the firmware zip file at the following URL:</p> <p>http://www.cyberdata.net/support/voip/index.html</p>
F	5/16/2011	<p>Updates Section 2.3.3.1, "Confirm Power on, Network Connectivity, and Baud Rate".</p> <p>Updates Section 2.3.4, "Restore the Factory Default Settings as Required".</p> <p>Updates Figure 2-4, "Paging Server Indicator Lights".</p>

Contents

Chapter 1 Product Overview	1
Chapter 2 Implementing the VoIP Paging Server	3
2.1 Parts List	3
2.2 Typical Installation	4
2.3 Setting up the Paging Server	5
2.3.1 Connect to the Power Source	5
2.3.2 Connect to the Network	5
2.3.3 Confirm that the Paging Server is Up and Running	6
Confirm Power on, Network Connectivity, and Baud Rate	6
Verify Network Activity	6
2.3.4 Restore the Factory Default Settings as Required	7
2.4 Configuring the Paging Server	8
2.4.1 Gather the Required Configuration Information	8
Static or DHCP Addressing?	8
Username and Password for Configuration GUI	8
SIP Settings	8
2.4.2 Log in to the Configuration GUI	8
2.4.3 Configure the Network Parameters	10
2.4.4 Change the Default Username and Password	12
2.4.5 Configure the SiP Parameters	14
2.5 Set up the PGROUPS	17
2.6 Operating the Paging Server	19
2.7 Upgrading the Firmware	20
2.8 Rebooting the Paging Server	22
Appendix A Setting Up a TFTP Server	23
A.1 Set up a TFTP Server	23
A.1.1 In a LINUX Environment	23
A.1.2 In a Windows Environment	23
Appendix B Troubleshooting/Technical Support	24
B.1 Frequently Asked Questions (FAQ)	24
B.1.1 Documentation	24
B.2 Contact Information	24
B.3 Warranty	25
B.3.1 Warranty & RMA Returns within the United States	25
B.3.2 Warranty & RMA Returns Outside of the United States	25
B.3.3 Spare in the Air Policy	26
B.3.4 Return and Restocking Policy	26
B.3.5 Warranty and RMA Returns Page	26
Appendix C How to Use the Multicast Extensions	27
C.1 Sending IP Multicast Datagrams	27
C.2 Receiving IP Multicast Datagrams	29
C.3 Establishing a Default Multicast Interface	30
C.4 Mtest	31
Index	32

1 Product Overview

The VoIP Paging Server is a POE enabled, single SIP-endpoint enabling user defined paging zones through a multicasting connection to CyberData VoIP speakers.

SIP compliant IP-PBX's that do not support grouping of SIP endpoints or paging can now support up to 100 different paging zones.



Product features

- SIP compliancy
- 10/100BaseT Ethernet Connection
- Multi-zone paging for up to 100 Zones
- TFTP-based firmware upgrades
- PoE enabled
- Connector for optional external power supply

Supported

- HTTP Web-based configuration
Provides an intuitive GUI for easy system configuration and verification of speaker operations.
- DHCP Client
- TFTP Client
- RTP Version 2 Multicast and Unicast
- Audio Codec
 - G.711 U-law
 - DTMF detection/generation

Product specifications

PoE VoIP Paging Server Specifications	
Regulatory Compliance	FCC Class A, UL 60950, CE
Power Requirement	PoE or 48V DC
Baud Rate	10/100 Mbps
Protocol	SiP compliant
Part Number	010878
Dimensions	6.11"L x 4.05"W x 1.15" H
Weight	1.2 pounds


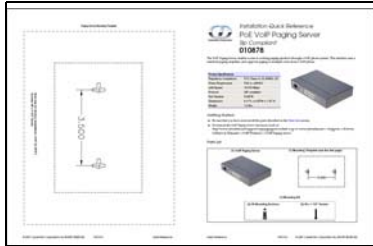
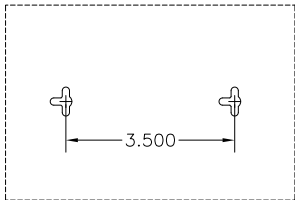

2 Implementing the VoIP Paging Server

The topics in this chapter provide information on setting up, configuring, and using the PoE VoIP Paging Server.

2.1 Parts List

The packaging for the Paging Server includes the parts in this illustration.

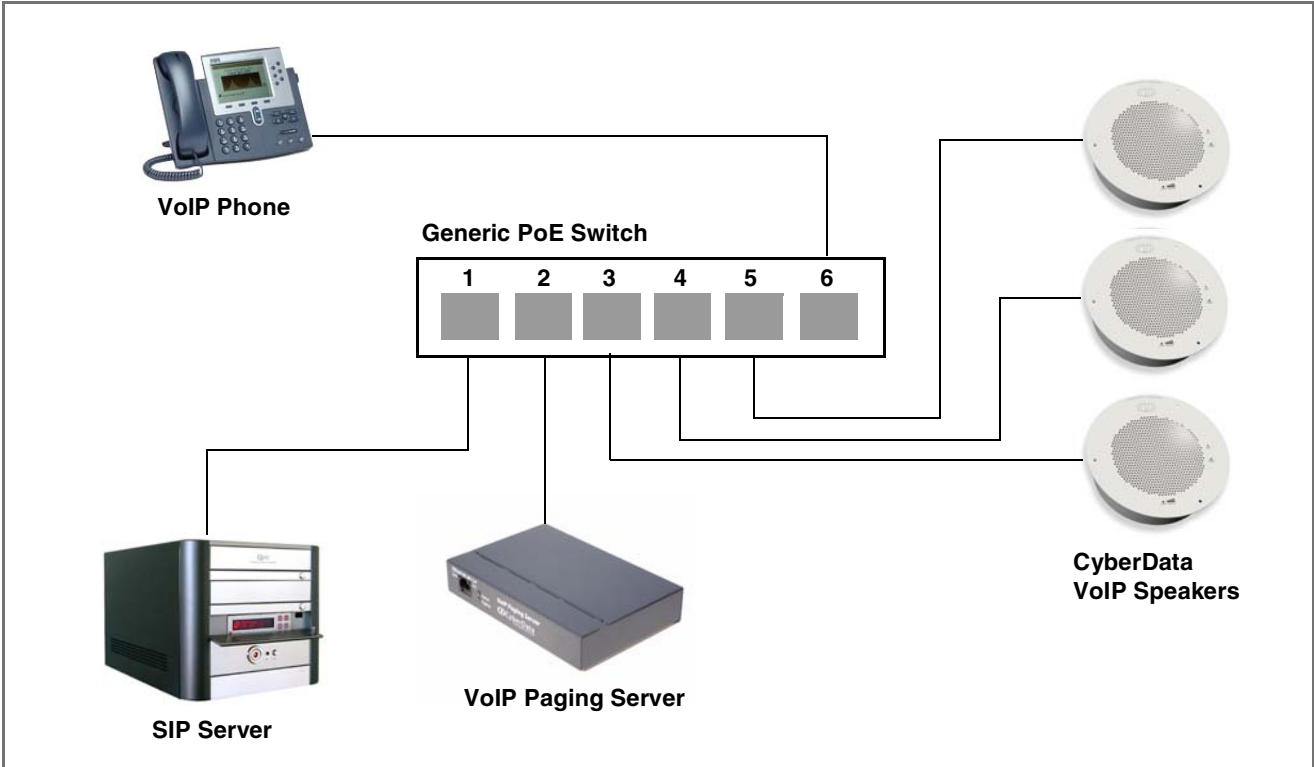
Table 2-1. Parts List

Quantity	Part Name	Illustration
1	VoIP Paging Server	
1	Installation Quick Reference Guide	
1	Mounting Template (located on the last page of the <i>Installation Quick Reference</i>)	
1	Mounting Kit (part #070057A) which includes: (2) #4-6 x 7/8" Mounting Anchors (2) #4 x 1-1/4" Round Phillips Wood Screws	

2.2 Typical Installation

Figure 2-1 illustrates how the Paging Server is normally installed as part of a paging system.

Figure 2-1. Typical Installation



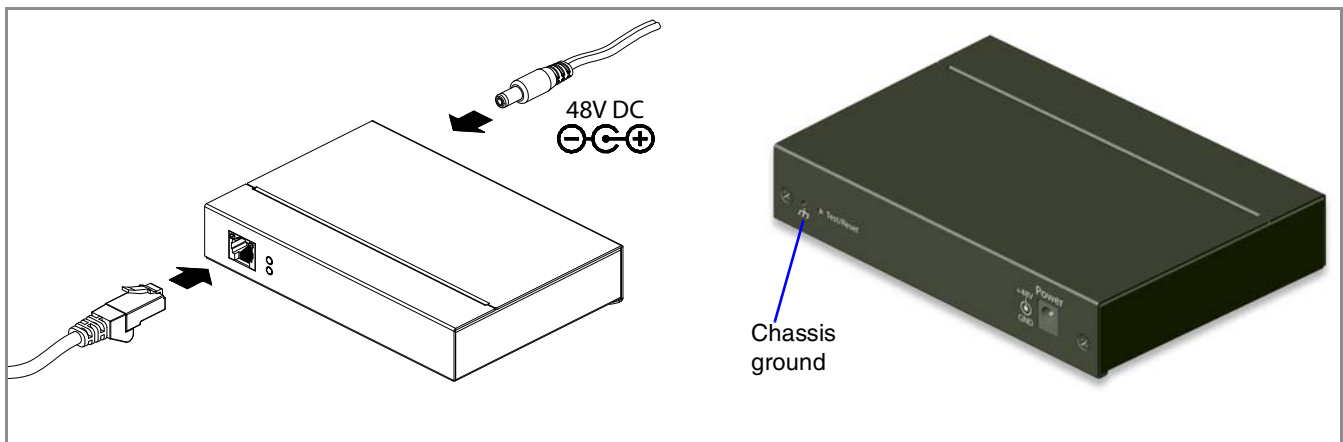
2.3 Setting up the Paging Server

Before you set up the Paging Server, be sure that you have received all the parts described in [Section 2.1, "Parts List"](#).

2.3.1 Connect to the Power Source

To use PoE, plug a Cat 5 Ethernet cable from the Paging Server **Ethernet** port to your network. As an alternative to PoE, you can plug one end of a +48V DC power supply into the Paging Server, and plug the other end into a receptacle. If required, connect the earth grounding wire to the chassis ground on the back of the unit.

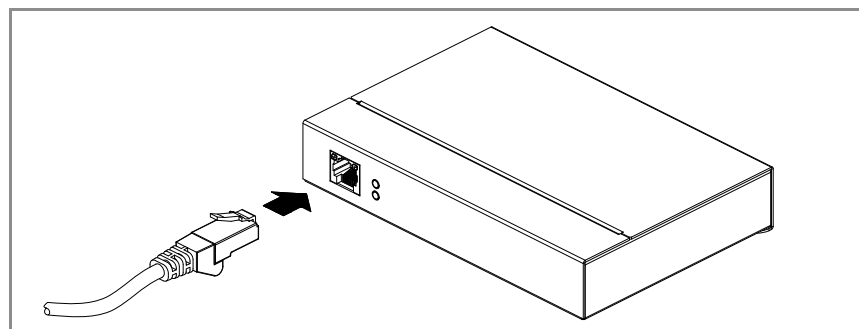
Figure 2-2. Connecting to the Power Source



2.3.2 Connect to the Network

Plug one end of a standard Ethernet cable into the Paging Server **Ethernet** port. Plug the other end into your network.

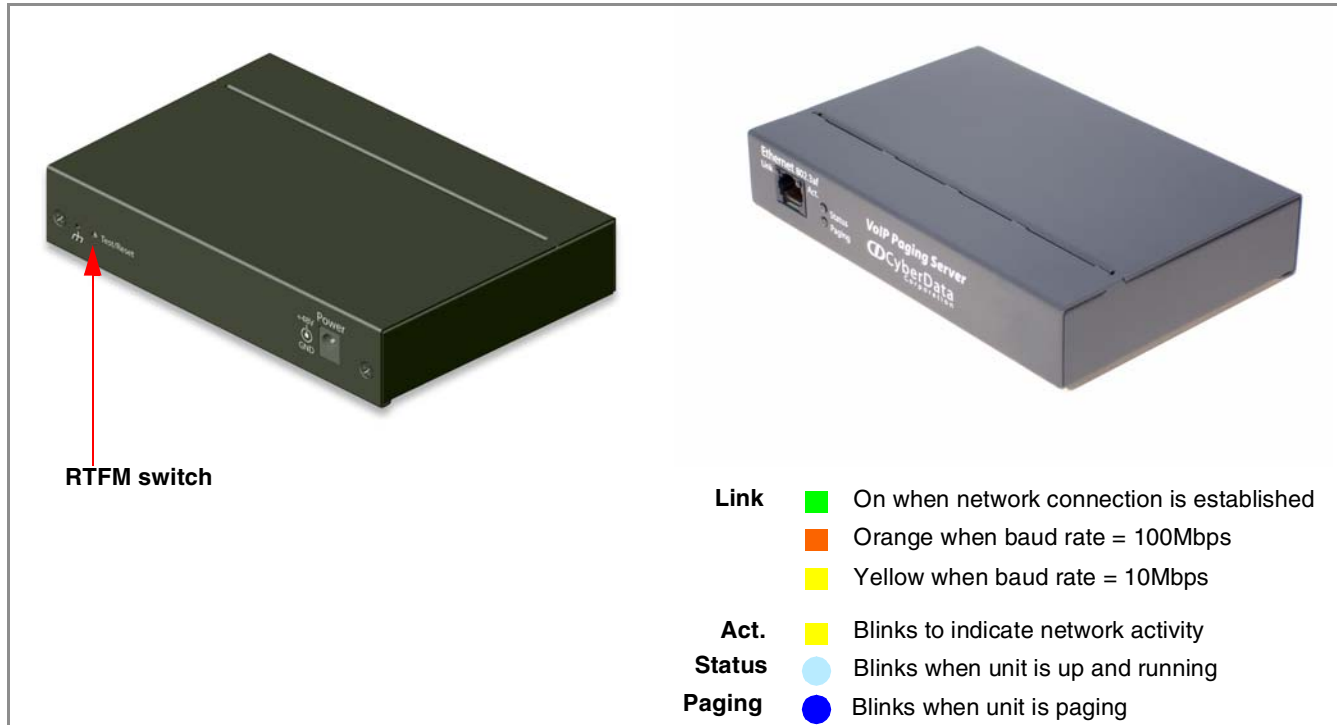
Figure 2-3. Connecting to the Network



2.3.3 Confirm that the Paging Server is Up and Running

The indicator lights on the front of the Paging Server verify the unit's operations.

Figure 2-4. Paging Server Indicator Lights



2.3.3.1 Confirm Power on, Network Connectivity, and Baud Rate

When you plug in the Ethernet cable or power supply:

- The round, pale blue **Status** light on the front of the Paging Server comes on indicating that the power is on. Once the device has been initialized, this light blinks at one second intervals.
- The square, green **Link** light above the Ethernet port indicates that the network connection has been established. The Link light changes color to confirm the auto-negotiated baud rate:
 - This light is yellow at 10 Mbps.
 - It is orange at 100 Mbps.
- The dark blue **Paging** light comes on after the device is booted and initialized. This light blinks when a page is in progress.

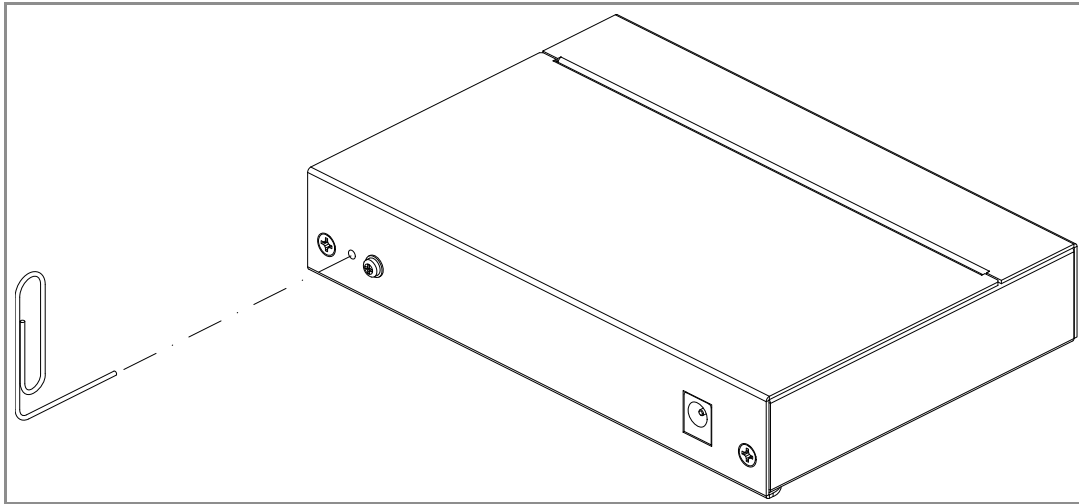
2.3.3.2 Verify Network Activity

The square, yellow **Act** light blinks when there is network activity.

2.3.4 Restore the Factory Default Settings as Required

The Paging Server is delivered with factory set default values for the following parameters. Use the **RTFM** switch (see [Figure 2-5](#)) on the back of the unit to restore these parameters to the factory default settings.

Figure 2-5. RTFM Switch



Note When you perform this procedure, the factory default settings are restored for *all* the following parameters.

Parameter	Factory Default Setting
IP Addressing	static
IP Address	192.168.3.10
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
Username	admin
Password	admin

To restore these parameters to the factory default settings:

1. Press and hold the **RTFM** switch for at least 20 seconds.
2. Release the switch. The **Status** and the **Paging** LEDs will go off. The **Link** and **Activity** LEDs will come on for one second and go off to indicate that the reset process is starting.
3. During the reset process, the **Link** LED will come on and the **Activity** LED will blink. After five seconds, the **Status** and **Paging** LEDs come back on.
4. The Paging Server settings are restored to the factory defaults.

2.4 Configuring the Paging Server

Use this section to configure the VoIP paging server.

2.4.1 Gather the Required Configuration Information

Have the following information available before you configure the Paging Server.

2.4.1.1 Static or DHCP Addressing?

Know whether your system uses static or dynamic (DHCP) IP addressing. If it uses static addressing, you also need to know the values to assign to the following Paging Server parameters:

- IP Address
- Subnet Mask
- Default Gateway

2.4.1.2 Username and Password for Configuration GUI

Determine the Username and Password that will replace the defaults after you initially log in to the configuration GUI.

- The Username is case-sensitive, and must be from four to 25 alphanumeric characters long.
- The Password is case-sensitive, and must be from four to 20 alphanumeric characters long.

2.4.1.3 SIP Settings

To configure the SIP parameters, determine whether you want to register the server. If you do, determine the number of minutes the registration lease remains valid, and whether you want to automatically unregister when you reboot. To configure the SIP parameters, you also need to determine the values for these parameters:

- SIP Server IP Address
- Remote and Local SIP Port Numbers
- SIP User ID, and Authenticate ID and Password for this User ID

2.4.2 Log in to the Configuration GUI

To log in:

1. For the initial configuration of the Paging Server, open your browser and enter the following address:

`http://192.168.3.10`

Note To work with the Paging Server configuration *after* the initial configuration, log in using the IP address you assign to the device. [Section 2.4.3, "Configure the Network Parameters"](#) provides instructions for entering the IP address.

- When prompted, use the following default **Username** and **Password** to open the configuration Home page:

Username: **admin**

Password: **admin**

Figure 2-6. Home Page



- On the **Home Page**, review the setup details and navigation buttons described in [Table 2-1](#).

Table 2-1. Home Page Overview






Web Page Item	Description
Device Name	Shows the device name.
Serial #	Device serial number.
Ethernet Address	Device ethernet address.
IP Addressing	Shows the current IP addressing setting (DHCP or static).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the DNS Server 1 address.
DNS Server 2	Shows the DNS Server 2 address.
	Link to the Network Setup web page.
	Link to the Admin Settings web page.

Table 2-1. Home Page Overview

Web Page Item	Description
	Link to the SIP Setup web page.
	Link to the PGroups Setup web page.
	Link to the Upgrade Firmware web page.

At this point you can:

- Review the Paging Server’s **Current Settings**. Use the RTFM switch to restore the factory default settings. See [Section 2.3.4, "Restore the Factory Default Settings as Required"](#).
- Configure the network parameters. Click **Network Setup** and refer to [Section 2.4.3, "Configure the Network Parameters"](#) for instructions.
- Configure the Admin parameters. Click **Admin Settings** and refer to [Section 2.4.4, "Change the Default Username and Password"](#) for instructions.
- Configure the SIP parameters. Click **SIP Setup** and see [Section 2.4.5, "Configure the SiP Parameters"](#).
- Configure the PGROUPS parameters. Click **PGROUPS Setup** and refer tofor instructions.

Note Click the **Upgrade Firmware** button any time you need to upload new versions of the firmware or **Reboot** the Paging Server. Refer to [Section 2.7, "Upgrading the Firmware"](#) and [Section 2.8, "Rebooting the Paging Server"](#) for instructions.

2.4.3 Configure the Network Parameters

Configuring the network parameters enables your network to recognize the Paging Server and communicate with it. Click **Network Setup** on the Home page to open the **Network Configuration** page.

Figure 2-7. Network Setup Page



On the **Network Setup** page, enter values for the parameters indicated in [Table 2-2](#).

Table 2-2. Network Setup Parameters




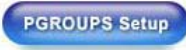

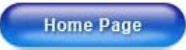
Web Page Item	Description
IP Addressing*	Select either DHCP IP Addressing or Static IP Addressing by marking the appropriate radio button. If you select Static , configure the remaining parameters indicated in Table 2-2 . If you select DHCP , go to Step 3 .
IP Address*	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1*	Enter the DNS Server 1 address.
DNS Server 2*	Enter the DNS Server 2 address.
	Click on this button to save your configuration settings. Changing a parameter that has an asterisk next to it will cause a system reboot when saved.
	Link to the Admin Settings web page.
	Link to the SIP Setup web page.

Table 2-2. Network Setup Parameters

Web Page Item	Description
	Link to the PGROUPS Setup web page.
	Link to the Upgrade Firmware web page.
	Link to the Home page.

On this page:

1. Specify whether you use **Static** or **DHCP IP Addressing** by marking the appropriate radio button. Then, if you select Static, go to [Step 2](#).

Note Changing the **IP Addressing** selection causes the system to reboot when click Save Settings.

2. For Static IP Addressing, also enter values for the following parameters:
 - a. The Paging Server's **IP Address**: The Paging Server is delivered with a factory default IP address. Change the default address to the correct IP address for your system.

Note Changing the Paging Server's **IP Address** causes the system to reboot when you click Save Settings.

- b. The **Subnet Mask**.
 - c. The **Default Gateway**.
3. Click **Save Settings** when you finish.

2.4.4 Change the Default Username and Password

On the Home page, click **Admin Settings** to open the **Administrator Settings** page. After changing the Username and Password on this page, new browser requests will require you to log in using these new parameters.

Figure 2-8. Administrator Settings Page

4. On the **Administrator Settings** page, enter values for the parameters indicated in [Table 2-3](#).

Table 2-3. Administrator Settings Parameters


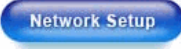



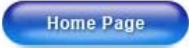
Web Page Item	Description
Device Name	Enter the name of the device.
Change Web Access Username	Use this field to change the Web Access Username
Change Web Access Password	Use this field to change the Web Access Password
Re-enter New Password	Use this field to re-enter a new password
	Click on this button to save your configuration settings. Changing a parameter that has an asterisk next to it will cause a system reboot when saved.
	Link to the Network Setup web page.
	Link to the SIP Setup web page.
	Link to the PGROUPS Setup web page.

Table 2-3. Administrator Settings Parameters

Web Page Item	Description
	Link to the Upgrade Firmware web page.
	Link to the Home page.

To change the default Web access Username and Password:

1. Enter the new Username from four to 25 alphanumeric characters in the **Change Username** field. The Username is case-sensitive.
2. Enter the new Password from four to 20 alphanumeric characters in the **Change Password** field. The Password is case-sensitive.
3. Enter the new password again in the **Re-enter New Password** field.
4. Click **Save Settings**.

2.4.5 Configure the SiP Parameters

The SIP parameters enable the Paging Server to contact and register with the SIP server. On the Home page, click **SIP Setup** to open the **SIP Configuration** page.

Figure 2-9. SIP Setup Page

The screenshot shows the 'SIP Setup' configuration page for the VoIP Paging Server. The page header includes the CyberData Corporation logo and the product name 'VOIP PAGING SERVER'. The main section is titled 'SIP Setup' and contains the following fields:

- SIP Server : 192.168.3.1 *
- Remote SIP Port: 5060 *
- Local SIP Port: 5060 *
- SIP User ID: 207 *
- Authenticate ID: 207 *
- Authenticate Password: ext207 *
- SIP Registration: Yes No *
- Unregister on Reboot: Yes No *
- Register Expiration (minutes): 60 *

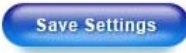




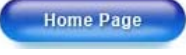
A note below the fields states: '* changing this parameter causes system reboot when saved'. A 'Save Settings' button is located below the fields. At the bottom of the page, there are five navigation buttons: 'Network Setup', 'Admin Settings', 'PGROUPS Setup', 'Upgrade Firmware', and 'Home Page'.

5. On the **SIP Setup** page, enter values for the parameters indicated in [Table 2-4](#).

Table 2-4. SIP Setup Parameters

Web Page Item	Description
SIP Server*	Enter the SIP server represented as either a numeric IP address in dotted decimal notation or the fully qualified host name (FQHN) up to 64 characters.
Remote SIP Port*	Enter the Remote SIP Port number (default is 5060).
Local SIP Port*	Enter the Local SIP Port number (default is 5060).
SIP User ID*	Enter the SIP User ID (up to 25 alphanumeric characters).
Authenticate ID*	Enter the Authenticate ID (up to 25 alphanumeric characters).
Authenticate Password*	Enter the Authenticate Password (up to 25 alphanumeric characters).
SIP Registration*	Enable/Disable SIP Registration.
Unregister on Reboot*	<ul style="list-style-type: none"> • Select Yes to automatically unregister the speaker when it is rebooted. • Select No to keep the speaker registered when it is rebooted.
Register Expiration*	Enter the SIP Registration lease time in minutes (default is 60 minutes).

Table 2-4. SIP Setup Parameters

Web Page Item	Description
	Click on this button to save your configuration settings. Changing a parameter that has an asterisk next to it will cause a system reboot when saved.
	Link to the Network Setup web page.
	Link to the Admin Settings web page.
	Link to the PGROUPS Setup web page.
	Link to the Upgrade Firmware web page.
	Link to the Home page.

1. Enter the IP address of the **SIP Server**.
2. Enter the port numbers used for SIP signaling:
 - a. **Remote SIP Port**
 - b. **Local SIP Port**
3. Enter the SIP registration parameters:
 - a. **SIP User ID**
 - b. **Authenticate ID**
 - c. **Authenticate Password**
4. For **SIP Registration**, designate whether you want the VoIP Paging Server to register with your SIP server.
5. At **Unregister on Reboot**:
 - a. Select **Yes** to automatically unregister the Paging Server when you reboot it. [Section 2.8, "Rebooting the Paging Server"](#) provides instructions on that process.
 - b. Select **No** to keep the Paging Server registered when you reboot it.
6. In the **Register Expiration** field, enter the number of minutes the Paging Server registration lease remains valid with the SIP Server. The Paging Server automatically re-registers with the SIP server before the lease expiration timeout.

2.5 Set up the PGROUPS

Note A PGROUP is a way of assigning multicast addresses and port numbers when configuring multicast paging speakers.

To assign a multicast address, you must first configure the CD VoIP speakers that you want to put into a paging zone by entering a particular multicast address and port number combination in the web configuration for these speakers.

1. Click on the **PGROUPS Setup** button to open the **PGROUPS Setup** page. See [Figure 2-10](#).

Figure 2-10. PGROUPS Setup

CyberData Corporation
VOIP PAGING SERVER

PGROUPS Setup

Device Name: CD_Paging_Server

Multicast TTL:

Bypass DTMF:

Bypassing DTMF will cause the paging server to forward to PG00 after answering a call.

	Enable Multicast IP Address	Port: 2000-65535	PGROUP Name
00	<input checked="" type="checkbox"/> 224.224.224.224	9876	Zone 00
01	<input type="checkbox"/> 224.224.224.224	9876	Zone 01
02	<input type="checkbox"/> 224.224.224.224	9876	Zone 02
03	<input type="checkbox"/> 224.224.224.224	9876	Zone 03
04	<input type="checkbox"/> 224.224.224.224	9876	Zone 04
05	<input type="checkbox"/> 224.224.224.224	9876	Zone 05
06	<input type="checkbox"/> 224.224.224.224	9876	Zone 06
07	<input type="checkbox"/> 224.224.224.224	9876	Zone 07
08	<input type="checkbox"/> 224.224.224.224	9876	Zone 08
09	<input type="checkbox"/> 224.224.224.224	9876	Zone 09

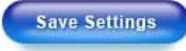


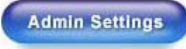



must reboot for changes to take effect

Page: [1](#), [2](#), [3](#), [4](#), [5](#), [6](#), [7](#), [8](#), [9](#), [10](#)

Other PGROUPS pages (1-100)

2. On the **PGROUPS Setup** page, enter values for the parameters indicated in [Table 2-5](#).

Table 2-5. PGROUPS Setup Parameters

Web Page Item	Description
Multicast TTL	The Multicast TTL field allows you to adjust the Multicast TTL. TTL is "time to live" and it describes how many networks (routers) a packet will go through before it is discarded. For more information, see Appendix C, "How to Use the Multicast Extensions .
Bypass DTMF	Check this box to bypass the DTMF entry. If the DTMF is bypassed, the Paging Server will relay audio to Paging Group 00 .
Device Name	Shows the name of the device.
Enable	Check this box to enable the PGROUP.
Multicast IP Address	Enter the multicast IP Address of a MGROUP.
Port 2000-65535	Enter the port number of a MGROUP.
PGROUP Name	Assign an identifier to the MGROUP.
	Click on this button to save your configuration settings.
	Click on this button to reboot the system.
	Link to the Network Setup web page.
	Link to the Admin Settings web page.
	Link to the SIP Setup web page.
	Link to the Upgrade Firmware web page.
	Link to the Home page.

3. After changing the parameters, click **Save Settings**.

2.6 Operating the Paging Server

- When you call to make a page, the Paging Server generates a tone over the phone.
- When you hear this tone, enter the two-digit code for the zone that you want to page.
- The Paging Server establishes a connection to a zone.
- The Paging Server generates another tone to the phone.
- When you hear this tone, you can begin speaking.

Note For *page-all*, you simply configure *all* speakers with a particular multicast address and port number combination, which represents one of the 100 zones that the paging server will support initially. Each speaker can still be part of 100 other paging zones in addition to the one *page-all* zone.

2.7 Upgrading the Firmware

The firmware on the board consists of two files: a Kernel and an Application, that can be loaded separately. Uploading the firmware files requires a host machine running a TFTP server. If you need to set up this server, [Appendix A, "Setting up a TFTP server"](#) provides instructions.

Figure 2-11. Firmware Upgrade Page

CyberData Corporation
VOIP PAGING SERVER

Firmware Upgrade

System Configuration	
Bootname:	u-boot-1.X.X

	Partition 1	Partition 2
Kernel	xxx-image-at75.bin	▶xxx-image-at75.bin
Application	xxx-romdisk-at75.img	▶xxx-romdisk-at75.img

Reboot System

Reboot

Load New Firmware to Partition 1

TFTP Server IP:

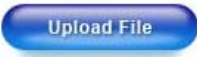

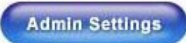



New Filename:

Upload File

Network Setup Admin Settings SIP Setup PGROUPS Setup Home Page

To upload a firmware file, log in as instructed in [Section 2.4.2, "Log in to the Configuration GUI"](#). [Table 2-6](#) shows the web page items on the **Firmware Upgrade** page.

Table 2-6. Firmware Upgrade Parameters

Web Page Item	Description
System Configuration	Shows the current configuration.
Bootname	Shows the current boot loader filename.
Kernel	Shows the current kernel filename for partition 1 and 2.
Application	Shows the current application filename for partition 1 and 2.
TFTP Server IP address	Enter the TFTP Server IP address.
New Filename	Use this field to enter the new file name for the kernel or application firmware file that you are uploading.
	Click on this button to automatically upload the selected firmware and reboot the system.
	Link to the Network Setup web page.
	Link to the Admin Settings web page.
	Link to the SIP Setup web page.
	Link to the Home page.
	Click on this button to reboot the system.

1. On the Home page, click **Upgrade Firmware** to open the **Firmware Upgrade** page.
2. Enter the **TFTP Server IP** address.
3. Enter the Kernel or Application **New Filename** for the firmware file you are uploading.

Note You can obtain the latest Paging Server firmware from the CyberData website:
<http://www.cyberdata.net/products/voip/digitalanalog/pagingserver/downloads.html>

4. Select the **Partition** to which the firmware is uploaded.
5. Click **Upload File** to automatically upload the selected firmware, and reboot your system.

2.8 Rebooting the Paging Server

To reboot the system, log in as instructed in [Section 2.4.2, "Log in to the Configuration GUI"](#).

Figure 2-12. Firmware Upgrade Page

CyberData Corporation
VOIP PAGING SERVER

Firmware Upgrade

System Configuration		Reboot System	
Bootname:	u-boot-1.X.X	<input type="button" value="Reboot"/>	
	Partition 1	Partition 2	
Kernel	xxx-image-at75.bin	▶xxx-image-at75.bin	
Application	xxx-romdisk-at75.img	▶xxx-romdisk-at75.img	

Load New Firmware to Partition 1

TFTP Server IP:

New Filename:

1. On the Home page, click **Upgrade Firmware** to open the **Firmware Upgrade** page. Go to the **Reboot** section on the right side of the page.
2. Click **Reboot**.

Appendix A: Setting Up a TFTP Server

A.1 Set up a TFTP Server

Upgrading the PoE VoIP Paging Server firmware requires a TFTP server on which you access the Web interface where you can upload the firmware files.

A.1.1 In a LINUX Environment

To set up a TFTP server on LINUX:

1. Create a directory dedicated to the TFTP server, and move the files to be uploaded to that directory.
2. Run the following command where `/tftpboot/` is the path to the directory you created in [Step 1](#): the directory that contains the files to be uploaded. For example:

```
in.tftpd -l -s /tftpboot/your_directory_name
```

A.1.2 In a Windows Environment

You can find several options online for setting up a Windows TFTP server. This example explains how to use the Solarwinds freeware TFTP server, which you can download at:

<http://www.cyberdata.net/support/voip/solarwinds.html>

To set up a TFTP server on Windows:

1. Install and start the software.
2. Select **File/Configure/Security tab/Transmit Only**.

Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.

Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

Go to the following URL to see CyberData's list of frequently asked questions:

<http://www.cyberdata.net/products/voip/digitalanalog/pagingserver/faqs.html>

B.1.1 Documentation

The documentation for this product is released in an English language version only. You can download PDF copies of CyberData product documentation at:

<http://www.cyberdata.net/products/voip/digitalanalog/pagingserver/docs.html>

B.2 Contact Information

Contact	<p>CyberData Corporation 3 Justin Court Monterey, CA 93940 USA www.CyberData.net Phone: 800-CYBERDATA (800-292-3732) Fax: 831-373-4193</p>
Sales	Sales 831-373-2601 Extension 334
Technical Support	<p>Phone: 831-373-2601 Extension 333 Web: http://www.cyberdata.net/support/contactsupportvoip.html</p>
Returned Materials Authorization	<p>To return the product, contact the CyberData Returned Materials Authorization (RMA) department at:</p> <p>Phone: 831-373-2601, Extension 136 Email: RMA@CyberData.net</p> <p>When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. No product will be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:</p> <p>CyberData Corporation 3 Justin Court Monterey, CA 93940 Attention: RMA "your RMA number"</p>

RMA Status Form If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:

<http://www.cyberdata.net/support/rmastatus.html>

B.3 Warranty

CyberData warrants its product against defects in material or workmanship for a period of two years from the date of purchase. Should the product fail within the warranty period, CyberData will repair or replace the product free of charge. This warranty includes all parts and labor.

Should the product fail out-of-warranty, a flat rate repair charge of one half of the purchase price of the product will be assessed. Repairs that are in warranty but are damaged by improper modifications or abuse, will be charged at the out-of-warranty rate. Products shipped to CyberData, both in and out-of-warranty, are shipped at the expense of the customer. Shipping charges for repaired products shipped back to the customer by CyberData, will be paid by CyberData.

CyberData shall not under any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use or malfunction of the products, loss of profits or revenues or costs of replacement goods, even if CyberData is informed in advance of the possibility of such damages.

B.3.1 Warranty & RMA Returns within the United States

If service is required, you must contact CyberData Technical Support prior to returning any products to CyberData. Our Technical Support staff will determine if your product should be returned to us for further inspection. If Technical Support determines that your product needs to be returned to CyberData, an RMA number will be issued to you at this point.

Your issued RMA number must be printed on the outside of the shipping box. No product will be accepted for return without an approved RMA number. The product in its original package should be sent to the following address:

CyberData Corporation

3 Justin Court.

Monterey, CA 93940

Attn: RMA "xxxxxx"

B.3.2 Warranty & RMA Returns Outside of the United States

If you purchased your equipment through an authorized international distributor or reseller, please contact them directly for product repairs.

B.3.3 Spare in the Air Policy

CyberData now offers a *Spare in the Air* no wait policy for warranty returns within the United States and Canada. More information about the *Spare in the Air* policy is available at the following web address:

<http://www.cyberdata.net/support/warranty/spareintheair.html>

B.3.4 Return and Restocking Policy

For our authorized distributors and resellers, please refer to your CyberData Service Agreement for information on our return guidelines and procedures.

For End Users, please contact the company that you purchased your equipment from for their return policy.

B.3.5 Warranty and RMA Returns Page

The most recent warranty and RMA information is available at the CyberData Warranty and RMA Returns Page at the following web address:

<http://www.cyberdata.net/support/warranty/index.html>

Appendix C: How to Use the Multicast Extensions

C.1 Sending IP Multicast Datagrams

Note The following information is also available at the following site:

<http://www.kohala.com/start/mcast.api.txt>

IP multicasting is currently supported only on AF_INET sockets of type SOCK_DGRAM and SOCK_RAW, and only on subnetworks for which the interface driver has been modified to support multicasting.

To send a multicast datagram, specify an IP multicast address in the range 224.0.0.0 to 239.255.255.255 as the destination address in a sendto() call.

By default, IP multicast datagrams are sent with a time-to-live (TTL) of 1, which prevents them from being forwarded beyond a single subnetwork. A new socket option allows the TTL for subsequent multicast datagrams to be set to any value from 0 to 255, in order to control the scope of the multicasts:

```
u_char ttl;
```

```
setsockopt(sock, IPPROTO_IP, IP_MULTICAST_TTL, &ttl, sizeof(ttl))
```

Multicast datagrams with a TTL of 0 will not be transmitted on any subnet, but may be delivered locally if the sending host belongs to the destination group and if multicast loopback has not been disabled on the sending socket (see below). Multicast datagrams with TTL greater than one may be delivered to more than one subnet if there are one or more multicast routers attached to the first-hop subnet. To provide meaningful scope control, the multicast routers support the notion of TTL "thresholds", which prevent datagrams with less than a certain TTL from traversing certain subnets. The thresholds enforce the following convention:

multicast datagrams with initial TTL 0 are restricted to the same host

multicast datagrams with initial TTL 1 are restricted to the same subnet

multicast datagrams with initial TTL 32 are restricted to the same site

multicast datagrams with initial TTL 64 are restricted to the same region

multicast datagrams with initial TTL 128 are restricted to the same continent

multicast datagrams with initial TTL 255 are unrestricted in scope.

"Sites" and "regions" are not strictly defined, and sites may be further subdivided into smaller administrative units, as a local matter. An application may choose an initial TTL other than the ones listed above. For example, an application might perform an "expanding-ring search" for a network resource by sending a multicast query, first with a TTL of 0, and then with larger and larger TTLs, until a reply is received, perhaps using the TTL sequence 0, 1, 2, 4, 8, 16, 32.

The multicast router accompanying this release refuses to forward any multicast datagram with a destination address between 224.0.0.0 and 224.0.0.255, inclusive, regardless of its TTL. This range of addresses is reserved for the use of routing protocols and other low-level topology discovery or

maintenance protocols, such as gateway discovery and group membership reporting. The current specification for IP multicasting requires this behavior only for addresses 224.0.0.0 and 224.0.0.1; the next revision of the specification is expected to contain this more general restriction.

Each multicast transmission is sent from a single network interface, even if the host has more than one multicast-capable interface. (If the host is also serving as a multicast router, a multicast may be FORWARDED to interfaces other than originating interface, provided that the TTL is greater than 1.) The system manager establishes the default interface to be used for multicasting as part of the installation procedure, described below. A socket option is available to override the default for subsequent transmissions from a given socket:

```
struct in_addr addr;
```

setsockopt(sock, IPPROTO_IP, IP_MULTICAST_IF, &addr, sizeof(addr)) where "addr" is the local IP address of the desired outgoing interface. An address of INADDR_ANY may be used to revert to the default interface. The local IP address of an interface can be obtained via the SIOCGIFCONF ioctl. To determine if an interface supports multicasting, fetch the interface flags via the SIOCGIFFLAGS ioctl and see if the IFF_MULTICAST flag is set. (Normal applications should not need to use this option; it is intended primarily for multicast routers and other system services specifically concerned with internet topology.)

If a multicast datagram is sent to a group to which the sending host itself belongs (on the outgoing interface), a copy of the datagram is, by default, looped back by the IP layer for local delivery. Another socket option gives the sender explicit control over whether or not subsequent datagrams are looped back:

```
u_char loop;
```

```
setsockopt(sock, IPPROTO_IP, IP_MULTICAST_LOOP, &loop, sizeof(loop))
```

where "loop" is 0 to disable loopback, and 1 to enable loopback. This option provides a performance benefit for applications that may have no more than one instance on a single host (such as a router or a mail demon), by eliminating the overhead of receiving their own transmissions. It should generally not be used by applications for which there may be more than one instance on a single host (such as a conferencing program) or for which the sender does not belong to the destination group (such as a time querying program).

A multicast datagram sent with an initial TTL greater than 1 may be delivered to the sending host on a different interface from that on which it was sent, if the host belongs to the destination group on that other interface. The loopback control option has no effect on such delivery.

C.2 Receiving IP Multicast Datagrams

Before a host can receive IP multicast datagrams, it must become a member of one or more IP multicast groups. A process can ask the host to join a multicast group by using the following socket option:

```
struct ip_mreq mreq;

setsockopt(sock, IPPROTO_IP, IP_ADD_MEMBERSHIP, &mreq, sizeof(mreq))
```

where "mreq" is the following structure:

```
struct ip_mreq {
    struct in_addr imr_multiaddr; /* multicast group to join */
    struct in_addr imr_interface; /* interface to join on */
}
```

Every membership is associated with a single interface, and it is possible to join the same group on more than one interface. "imr_interface" should be INADDR_ANY to choose the default multicast interface, or one of the host's local addresses to choose a particular (multicast-capable) interface. Up to IP_MAX_MEMBERSHIPS (currently 20) memberships may be added on a single socket.

To drop a membership, use:

```
struct ip_mreq mreq;

setsockopt(sock, IPPROTO_IP, IP_DROP_MEMBERSHIP, &mreq, sizeof(mreq))
```

where "mreq" contains the same values as used to add the membership. The memberships associated with a socket are also dropped when the socket is closed or the process holding the socket is killed. However, more than one socket may claim a membership in a particular group, and the host will remain a member of that group until the last claim is dropped.

The memberships associated with a socket do not necessarily determine which datagrams are received on that socket. Incoming multicast packets are accepted by the kernel IP layer if any socket has claimed a membership in the destination group of the datagram; however, delivery of a multicast datagram to a particular socket is based on the destination port (or protocol type, for raw sockets), just as with unicast datagrams. To receive multicast datagrams sent to a particular port, it is necessary to bind to that local port, leaving the local address unspecified (i.e., INADDR_ANY).

More than one process may bind to the same SOCK_DGRAM UDP port if the bind() is preceded by:

```
int one = 1;

setsockopt(sock, SOL_SOCKET, SO_REUSEADDR, &one, sizeof(one))
```

In this case, every incoming multicast or broadcast UDP datagram destined to the shared port is delivered to all sockets bound to the port. For backwards compatibility reasons, THIS DOES NOT APPLY TO INCOMING UNICAST DATAGRAMS -- unicast datagrams are never delivered to more than one socket, regardless of how many sockets are bound to the datagram's destination port. SOCK_RAW sockets do not require the SO_REUSEADDR option to share a single IP protocol type.

The definitions required for the new, multicast-related socket options are found in <netinet/in.h>. All IP addresses are passed in network byte-order.

A final multicast-related extension is independent of IP: two new ioctls, SIOCADDMULTI and SIOCDELMULTI, are available to add or delete link-level (e.g., Ethernet) multicast addresses accepted by a particular interface. The address to be added or deleted is passed as a sockaddr structure of family AF_UNSPEC, within the standard ifreq structure. These ioctls are for the use of protocols other than IP, and require superuser privileges. A link-level multicast address added via SIOCADDMULTI is not automatically deleted when the socket used to add it goes away; it must be explicitly deleted. It is inadvisable to delete a link-level address that may be in use by IP. (These ioctls already exist in SunOS and Ultrix; they are new to BSD Unix.)

Drivers that have been modified to support multicasting also support the IFF_PROMISC and IFF_ALLMULTI interface flags, to the degree possible.

The kernel modification required to support Van Jacobson's traceroute program is also included in this release.

Examples of usage of the above facilities can be found in the programs accompanying this distribution, such as "ping", "mtest" and "rwhod".

C.3 Establishing a Default Multicast Interface

Selection of the default multicast interface is controlled via the kernel (unicast) routing table. If there is no multicast route in the table, all multicasts will, by default, be sent on the interface associated with the default gateway. If that interface does not support multicast, attempts to send will receive an ENETUNREACH error.

A route may be added for a particular multicast address or for all multicast addresses, to direct them to a different default interface. For example, to specify that multicast datagrams addressed to 224.0.1.3 should, by default, be sent on the interface with local address 36.2.0.8, use the following:

```
/etc/route add 224.0.1.3 36.2.0.8 0
```

To set the default for all multicast addresses, other than those with individual routes, to be the interface with local address 36.11.0.1, use:

```
/etc/route add 224.0.0.0 36.11.0.1 0
```

If you point a multicast route at an interface that does not support multicasting, an attempt to multicast via that route will receive an ENETUNREACH error.

If needed, these commands normally would be added to the /etc/rc.ip or /etc/rc.local file, to take effect every time the system is booted.

C.4 Mtest

The mtest directory contains a small program for testing the multicast membership sockopts and ioctls. It accepts the following commands, interactively:

```
j g.g.g g.i.i.i.i - join IP multicast group
l g.g.g g.i.i.i.i - leave IP multicast group
a ifname e.e.e.e.e - add ether multicast address
d ifname e.e.e.e.e - del ether multicast address
m ifname 1/0      - set/clear ether allmulti flag
p ifname 1/0      - set/clear ether promisc flag
q                 - quit
```

where g.g.g.g is an IP multicast address, e.g., 224.0.2.1

i.i.i.i is the IP address of a local interface or 0.0.0.0

ifname is an interface name, e.g., qe0

e.e.e.e.e is an Ethernet address in hex, e.g., 1.0.5e.0.2.1

1/0 is a 1 or a 0, to turn the flag on or off

The "p" command to change the promiscuous flag does not work under SunOS, because it uses a different ioctl for that purpose.

Mtest is useful for establishing targets for multicast ping testing. The results of mtest filter manipulation can be seen by using the "netstat -nia" command (see next section).

Index

Symbols

+48V DC power supply 5

Numerics

100 Mbps indicator light 6

A

act light 6
 address, login 8
 addressing
 DHCP 8, 12
 static 8, 12
 admin settings button 12
 admin username and password 9
 administrator settings page 12, 13
 asterisk 11, 13, 16
 Audio Codec 2
 authenticate ID and password for SIP server
 registration 16

B

baseT ethernet connection 1
 baud rate
 specification 2
 verifying 6
 blue status light 6
 bypass DTMF 18

C

cat 5 ethernet cable 5
 changing default username and password for
 configuration GUI 12
 configurable parameters 9, 11, 15, 21
 configuration information 8
 contact information 24
 contact information for CyberData 24

current settings, reviewing 10
 CyberData contact information 24

D

default
 gateway 7
 IP address 7
 subnet mask 7
 username and password 7
 default gateway 7, 11
 default gateway for static addressing 12
 default password for configuration GUI 9
 default settings, restoring 7
 default username and password for configuration GUI 9
 DHCP addressing 8, 12
 DHCP Client 2
 DHCP IP addressing 11
 dimensions 2
 DNS server 9, 11
 DTMF detection 2
 dual speeds 6

E

ethernet port 5
 expiration time for SIP server lease 15, 16

F

features 1
 firmware
 where to get the latest firmware 21
 firmware upgrade page 21, 22
 firmware, upgrade 10, 20

G

GUI username and password 12

H

http web-based configuration 2

I

IP address 7, 11, 21
SIP server 16

IP addressing 11
default
IP addressing setting 7

L

lease, SIP server expiration time 15, 16
link light 6
Linux, setting up a TFTP server on 23
local SIP port 15, 16
log in address 8
logging in to configuration GUI 8

M

MGROUP 17
MGROUP Name 18
Multicast IP Address 18
multicast TTL 18, 27
multi-zone paging 1

N

network activity, verifying 6
network configuration page 10
network parameters, configuring 10
network setup button 10
network, connecting to 5

O

orange link light 6

P

paging light 6

paging server
configuration 8
part number 2
parts list 3
password
configuration GUI 8, 12
for SIP server login 15
restoring the default 7
SIP server authentication 16
pgroups 17
pgroups configuration 10
port
ethernet 5
local SIP 15, 16
remote SIP 15, 16
power
connecting to 5
requirement 2
product overview 1

R

reboot 21
paging server 22
unregistering from SIP server during 16
registration and expiration, SIP server
lease expiration 16
registration and expiration, SIP server lease 15
regulatory compliance 2
remote SIP port 15, 16
required configuration for web access username and
password 8, 14
requirements for upgrading firmware 20
resetting the IP address to the default 24
restoring factory default settings 7
return and restocking policy 26
RMA returned materials authorization 24
RMA status 25
RTP Audio Version 2 2

S

sales 24
server
SIP 10
TFTP 20, 23
server address, SIP 15
service 24
SIP configuration
SIP Server 15
SIP configuration page 14
SIP registration 15

- SIP server 15
- SIP server configuration 10
- SIP server parameters, configuring 8
- SIP setup button 10, 14
- Spare in the Air Policy 26
- speaker configuration page
 - configurable parameters 9, 11, 15, 21
- specifications 2
- static addressing 8, 12
- static IP addressing 11
- status light 6
- subnet mask 7, 11
- subnet mask static addressing 12
- supported protocols 2

T

- tech support 24
- technical support, contact information 24
- TFTP server 2, 20, 23
- TFTP server IP 21

U

- unregister from SIP server 16
- unregister, from SIP server 15
- upgrade firmware 10, 20
- upgrade firmware button 10, 21, 22
- upload file button 21
- user ID
 - for SIP server login 15
- user ID for SIP server registration 16
- user ID, SIP 15
- username
 - restoring the default 7
- username for configuration GUI 8, 12

V

- verifying
 - baud rate 6
 - network activity 6
 - network connectivity 6
- VoIP phone in typical installation 4

W

- warranty 25
- warranty & RMA returns outside of the United States 25

- warranty & RMA returns within the United States 25
- warranty and RMA returns page 26
- warranty policy at CyberData 25
- web configuration log in address 8
- weight 2
- Windows, setting up a TFTP server on 23

Y

- yellow act light 6
- yellow link light 6