



Multicast VoIP Microphone Operations Guide

Part #011446
Document Part #931431A
for Firmware Version 1.0.0

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

Multicast VoIP Microphone Operations Guide 931431A
Part # 011446

COPYRIGHT NOTICE:

© 2017, 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.



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

<http://support.cyberdata.net/>

Phone: (831) 373-2601, Ext. 333

Email: support@cyberdata.net

Fax: (831) 373-4193

Company and product information is at www.cyberdata.net.

Revision Information

Revision 931431A, which corresponds to firmware version 1.0.0, was released on October 9, 2017, and has the following changes:

Browsers Supported




The following browsers have been tested against firmware version 1.0.0:

- Chrome (version 57.0.2987.98)
- Firefox: (version 55.0.2)
- Internet Explorer (version 11.0.9600.18314)



Important Safety Instructions

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
13. Prior to installation, consult local building and electrical code requirements.

14. WARNING: The Multicast VoIP Microphone enclosure is not rated for any AC voltages!

 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
 <p>GENERAL ALERT</p>	<p>Warning</p> <p><i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
 <p>GENERAL ALERT</p>	<p>Warning</p> <p>The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>

Pictorial Alert Icons

	<p>General Alert</p> <p>This pictorial alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard.</p>
	<p>Ground</p> <p>This pictorial alert indicates the Earth grounding connection point.</p>

Hazard Levels

Danger: Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury. This is limited to the most extreme situations.

Warning: Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

Caution: Indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury. It may also alert users against unsafe practices.

Notice: Indicates a statement of company policy (that is, a safety policy or protection of property).

The safety guidelines for the equipment in this manual do not purport to address all the safety issues of the equipment. It is the responsibility of the user to establish appropriate safety, ergonomic, and health practices and determine the applicability of regulatory limitations prior to use. Potential safety hazards are identified in this manual through the use of words Danger, Warning, and Caution, the specific hazard type, and pictorial alert icons.

Abbreviations and Terms

Abbreviation or Term	Definition
A-law	A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing.
AVP	Audio Video Profile
Cat 5	TIA/EIA-568-B Category 5
DHCP	Dynamic Host Configuration Protocol
LAN	Local Area Network
LED	Light Emitting Diode
Mbps	Megabits per Second.
NTP	Network Time Protocol
PBX	Private Branch Exchange
PoE	Power over Ethernet (as per IEEE 802.3af standard)
RTFM	Reset Test Function Management
SIP	Session Initiated Protocol
u-law	A companding algorithm, primarily used in the digital telecommunication
UC	Unified Communications
VoIP	Voice over Internet Protocol

Contents

Chapter 1 Product Overview	1
1.1 How to Identify This Product	1
1.2 Typical System Installation	2
1.3 Product Features	3
1.4 Supported Protocols	3
1.5 Specifications	4
Chapter 2 Installing the Multicast VoIP Microphone	5
2.1 Parts List	5
2.1.1 Multicast VoIP Microphone Connectors	6
2.1.2 Activity and Link LEDs	8
2.1.3 Restoring the Factory Default Settings	9
2.1.4 Call Button and the Call Button LED	10
2.2.1 Factory Default Settings	11
2.2.2 Multicast VoIP Microphone Web Page Navigation	12
2.2.3 Using the Toggle Help Button	13
2.2.4 Log in to the Configuration Home Page	15
2.2.5 Configure the Device	18
2.2.6 Configure the Network Parameters	24
2.2.7 Configure the Event Parameters	27
2.2.8 Configure the Autoprovisioning Parameters	31
2.2.9 Downloading the Firmware	43
2.2.10 Reboot the Device	45
2.3.1 Command Interface Post Commands	46
Appendix A Mounting the Multicast VoIP Microphone	47
A.1 Mount the Multicast VoIP Microphone	47
Appendix B Troubleshooting/Technical Support	50
B.1 Frequently Asked Questions (FAQ)	50
B.2 Documentation	50
B.3 Contact Information	51
B.4 Warranty and RMA Information	51
Index	52

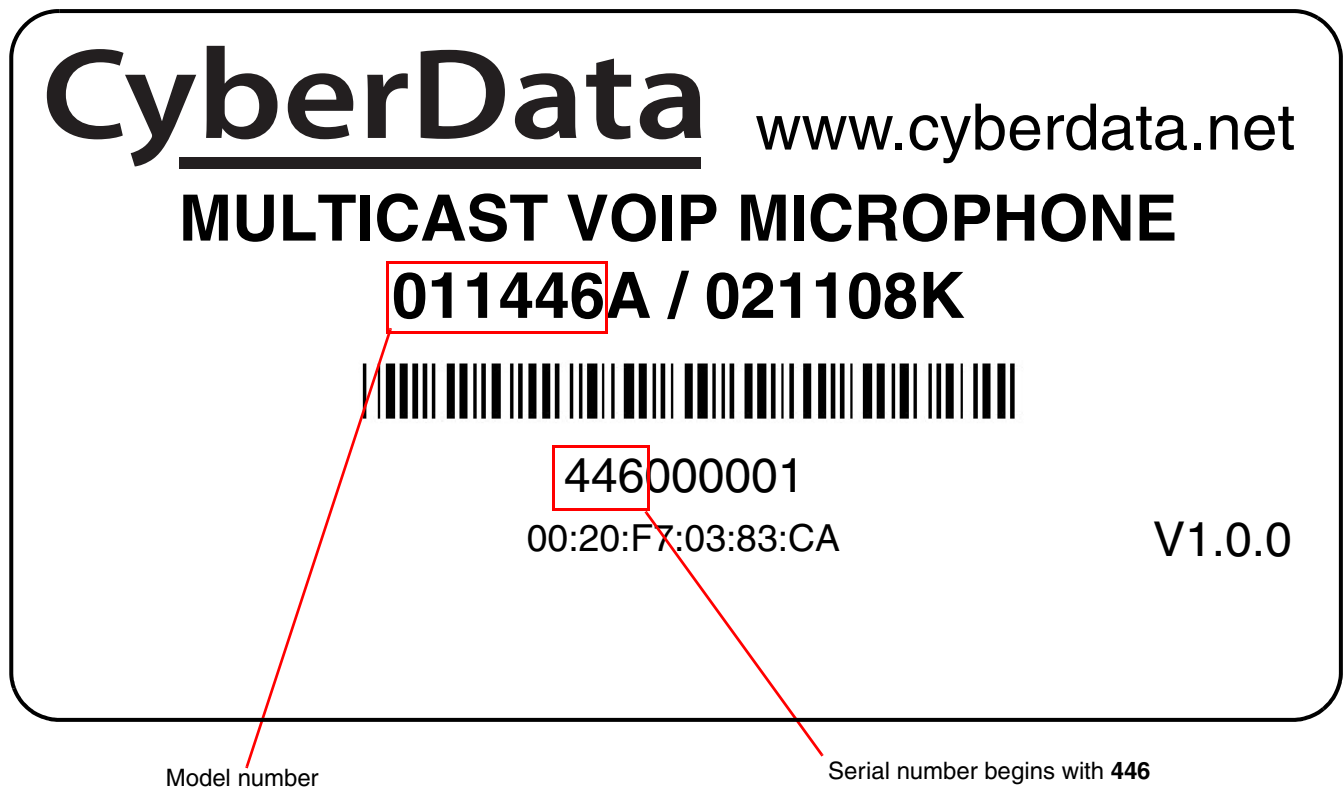
1 Product Overview

1.1 How to Identify This Product

To identify the Multicast VoIP Microphone, look for a model number label similar to the one shown in [Figure 1-1](#). Confirm the following:

- The model number on the label should be **011446**.
- The serial number on the label should begin with **446**.

Figure 1-1. Model Number Label¹

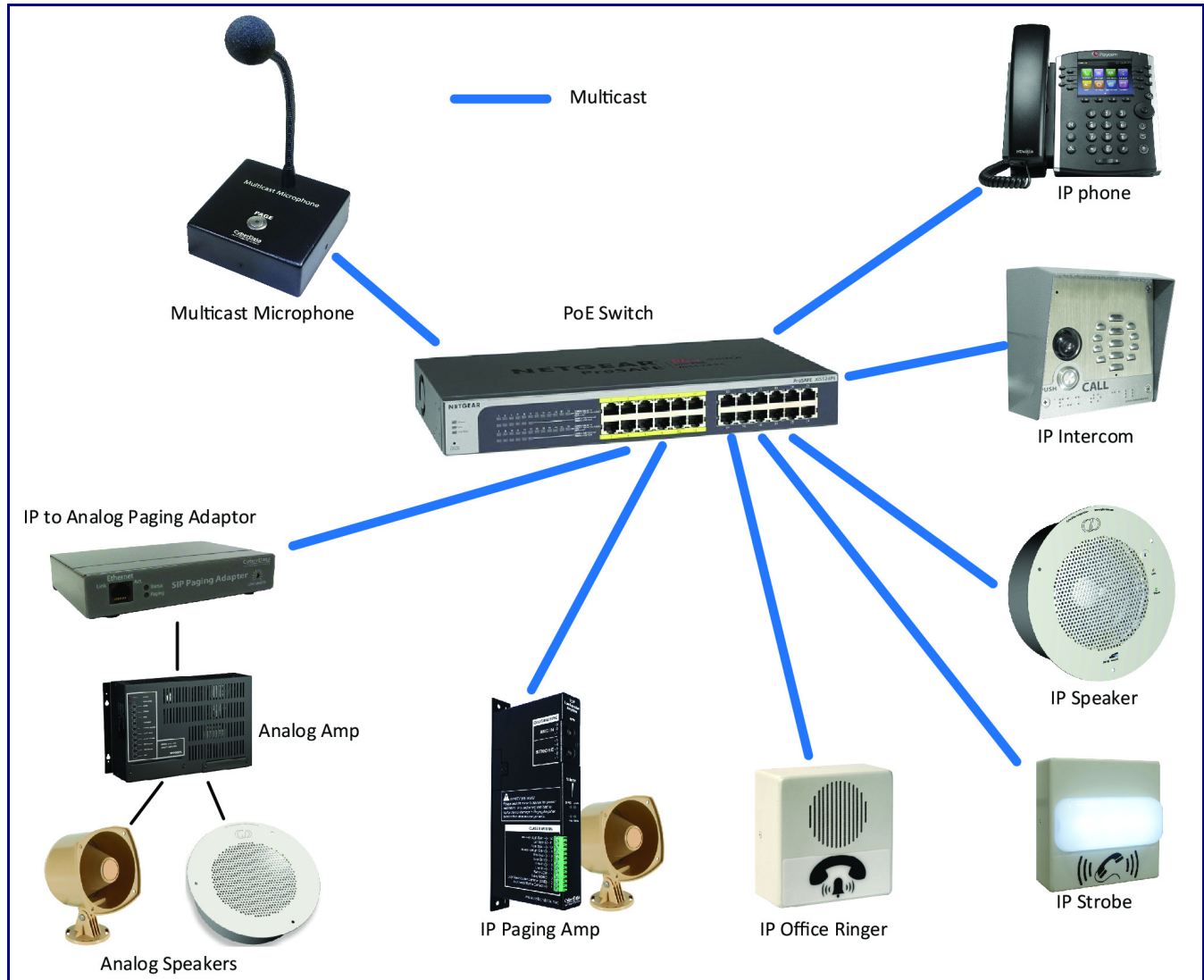


1. This figure is just an example. The information on the labels may be different.

1.2 Typical System Installation

The following figures illustrate how the Multicast VoIP Microphone can be installed as part of a VoIP phone system.

Figure 1-2. Paging to Multicast Enabled Endpoints



1.3 Product Features

The Multicast VoIP Microphone has the following features:

- Multicast Transmit
- Compatible with CyberData endpoints that receive multicast
- Page to Polycom phones
- Delayed page support (up to 60 seconds)
- Web-based configuration and firmware upload
- Autoprovision support
- PoE 802.3af enabled (Power-over-Ethernet)
- G711 codec
- 12-inch flexible shaft microphone
- Desktop Design
- Wall mountable

1.4 Supported Protocols

The Multicast VoIP Microphone supports the following protocols:

- HTTP Web-based configuration
Provides an intuitive user interface for easy system configuration and verification of Multicast VoIP Microphone operations.
- DHCP Client
Dynamically assigns IP addresses in addition to the option to use static addressing.
- TFTP Client
Facilitates hosting for the Autoprovisioning configuration file.
- RTP
- Facilitates autoprovisioning configuration values on boot
- Audio Encodings
PCMU (G.711 mu-law)

1.5 Specifications

Table 1-1. Specifications

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	Multicast
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply ^a
Microphone Length	12 inches
Operating Range	Temperature: -40° C to 55° C (-40° F to 131° F) Humidity: 5-95%, non-condensing
Storage Temperature	-40° C to 70° C (-40° F to 158° F)
Storage Altitude	Up to 15,000 ft. (4573 m)
Payload Types	G711, A-law and μ -law
Dimensions ^b (without Microphone Boom)	4.53 inches [115 mm] Length 1.58 inches [40.2 mm] Width 4.53 inches [115 mm] Height
Weight	1.0 lbs. (0.45 kg)
Boxed Weight	2.0 lbs. (0.90 kg)
Part Number	011446

a. Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.


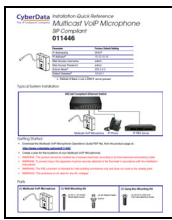

b. Dimensions are measured from the perspective of the product being upright with the front of the product facing you.

2 Installing the Multicast VoIP Microphone

2.1 Parts List

Table 2-1 illustrates the Multicast VoIP Microphone parts.

Table 2-1. Parts List

Quantity	Part Name	Picture
1	Multicast VoIP Microphone Assembly	
1	Installation Quick Reference Guide	
1	Multicast VoIP Microphone Mounting Accessory Kit	

2.1.1 Multicast VoIP Microphone Connectors

See the following figures and tables to identify the connectors and functions of the Multicast VoIP Microphone.

Figure 2-1. Connector Locations

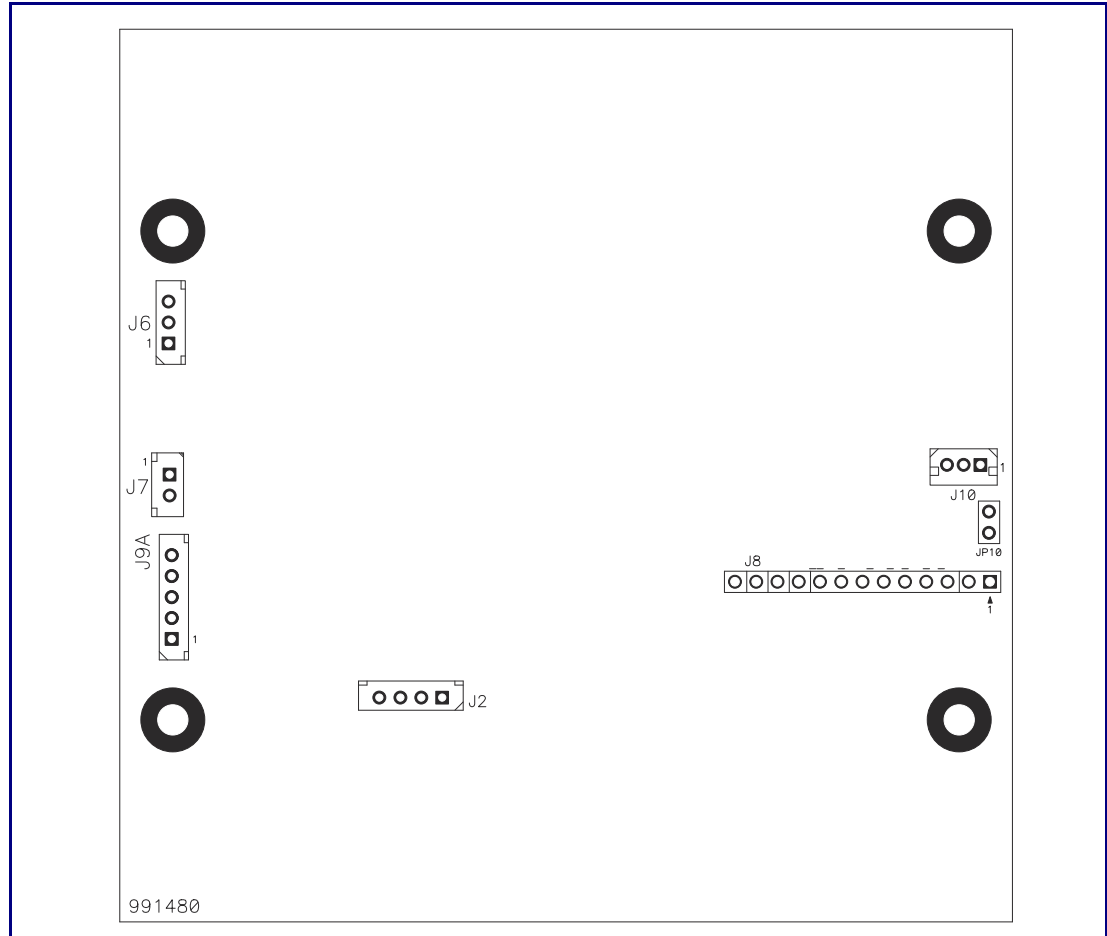


Table 2-2. Connector Functions

Connector	Function
J2	Push Button
J6	Microphone Interface

Figure 2-2. Connector Locations

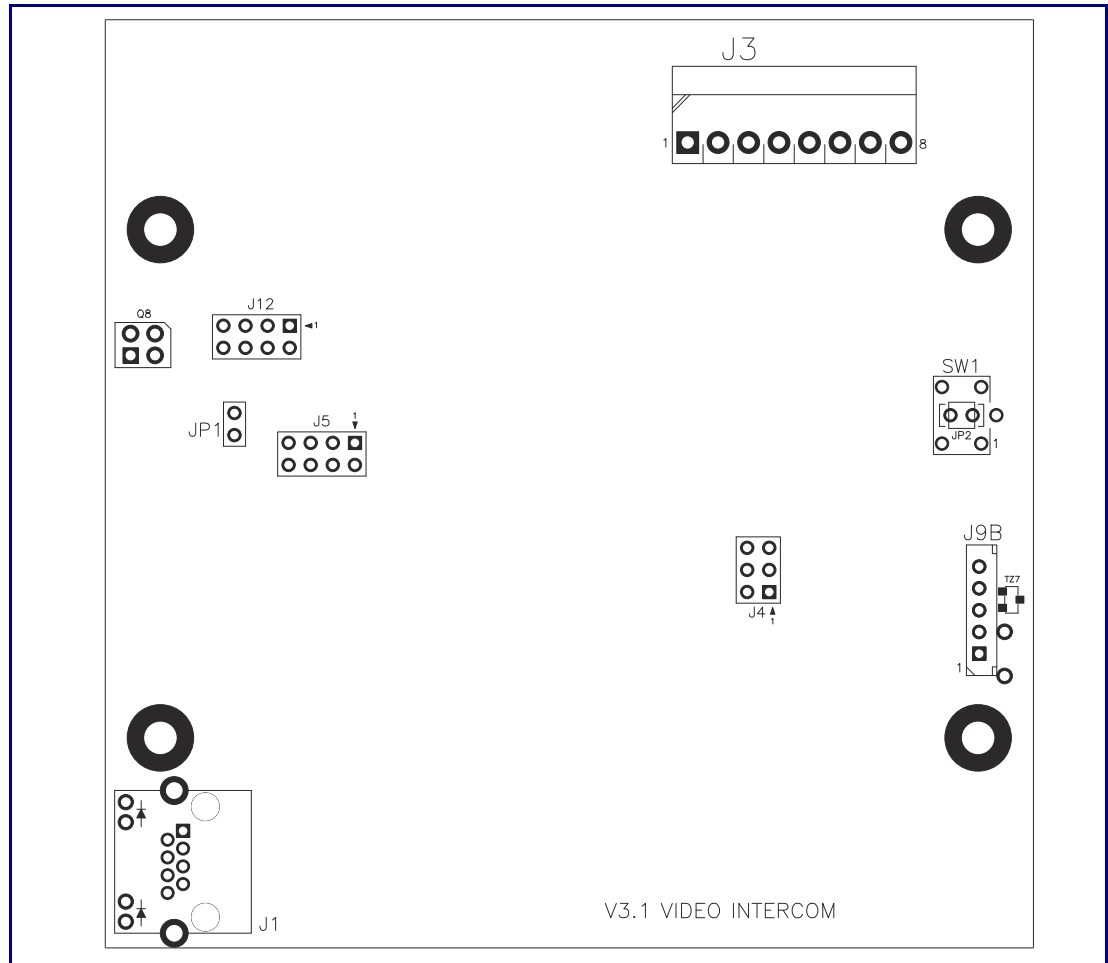


Table 2-3. Connector Functions

Connector	Function
J1	PoE Network Connection (RJ-45 ethernet)

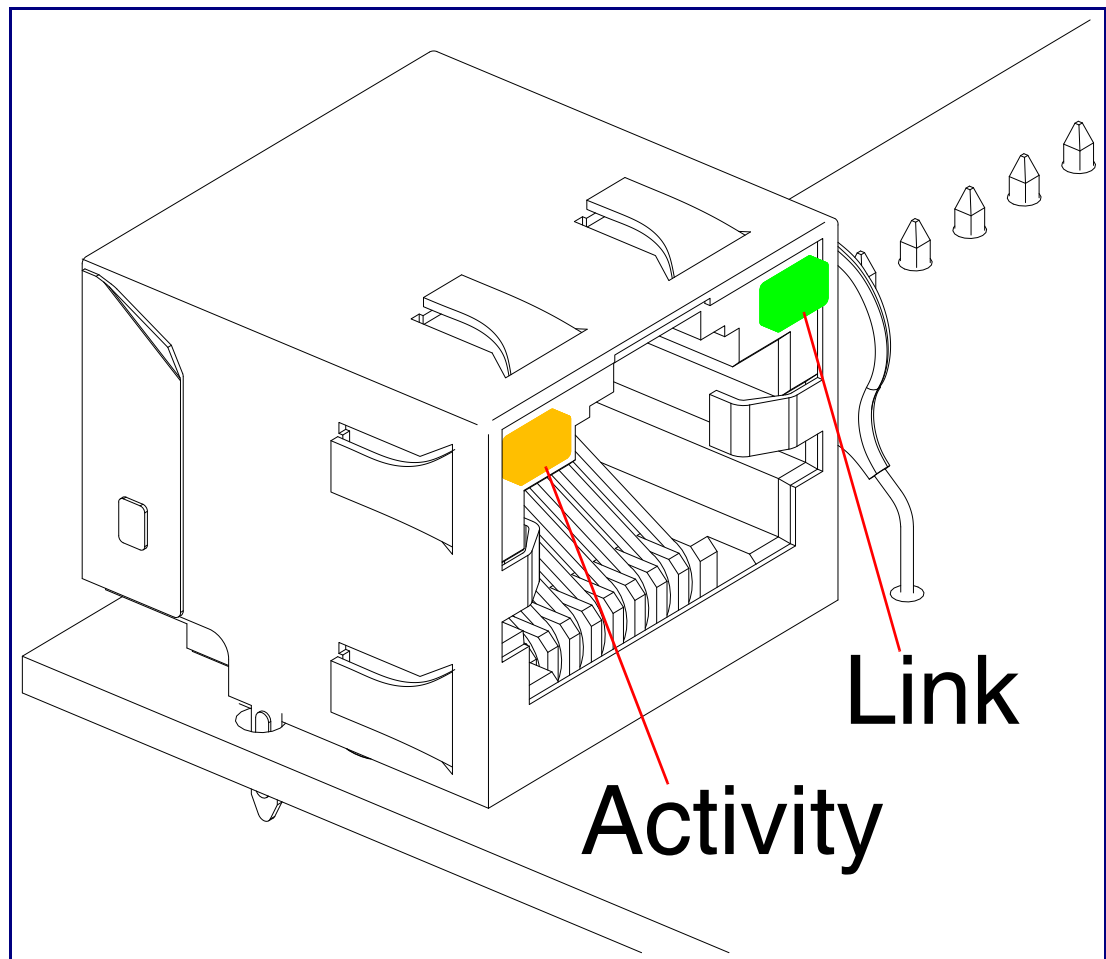
2.1.2 Activity and Link LEDs

2.1.2.1 Verifying the Network Connectivity and Data Rate

When you plug in the Ethernet cable or power supply to the device, the following occurs:

- The square, **AMBER Link/Activity** LED blinks when there is network activity (see [Figure 2-3](#)).
- The square, **GREEN 100Mb Link** LED above the Ethernet port indicates that the network connection has been established (see [Figure 2-3](#)).

Figure 2-3. Activity and Link LED



2.1.3 Restoring the Factory Default Settings

When troubleshooting configuration problems, it is sometimes convenient to restore the device to the factory default settings.

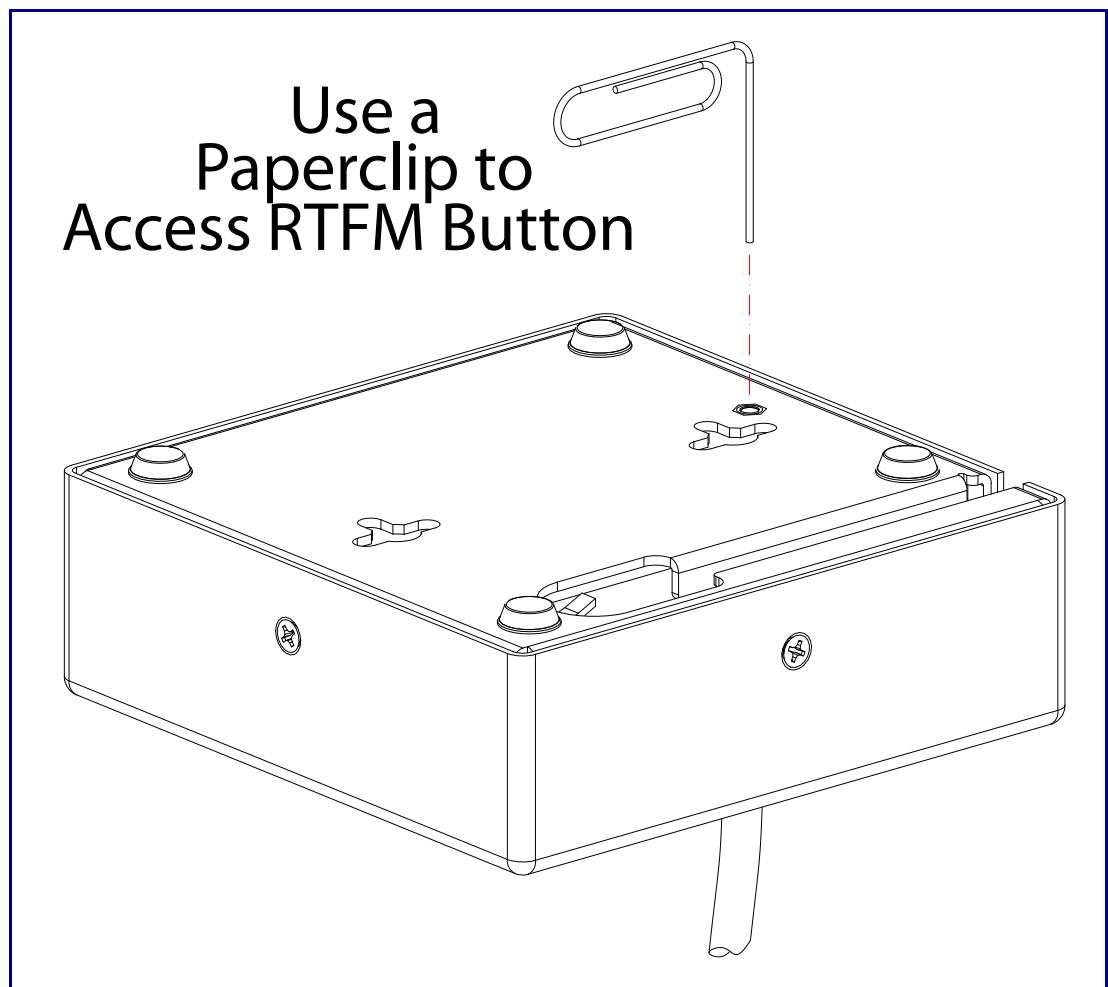
Note Each Multicast VoIP Microphone is delivered with factory set default values.

To restore the factory default settings:

1. Press and hold the **RTFM button** (see **SW1** in [Figure 2-4](#)) for more than five seconds.

Note The device will use DHCP to obtain the new IP address (DHCP-assigned address or default to 10.10.10.10 if a DHCP server is not present).

Figure 2-4. RTFM Button



2.1.4 Call Button and the Call Button LED

2.1.4.1 Call Button LED Function

- Upon initial power or reset, the Call Button LED will illuminate.
- On boot, the Call Button LED will flash ten times a second while setting up the network and downloading autoprovisioning files.
- The device “autoprovisions” by default, and the initial process may take several minutes as the device searches for and downloads updates. The Call Button LED will blink during this process. During the initial provisioning, or after the factory defaults have been reset, the device may download firmware twice. The device will blink, remain solid for 10 to 20 seconds, and then resume blinking.
- When the software has finished initialization, the Call Button LED will blink twice.
- On the [Device Configuration Page](#) (see [Section 2.2.5, "Configure the Device"](#)), there is an option called [Button Lit When Idle](#). This option sets the normal state for the indicator LED. The Call Button LED will still blink during initialization.
- After the RTFM button is pressed, the call button LED will turn off for several seconds. It lights for approximately 25 seconds, fast blinks for 10 seconds, and then stays on while the device is in operation.

Figure 2-5. Call Button and Call Button LED



2.2 Configure the Multicast VoIP Microphone Parameters

To configure the Multicast VoIP Microphone online, use a standard web browser.

Configure each Multicast VoIP Microphone and verify its operation *before* you mount it. When you are ready to mount an Multicast VoIP Microphone, refer to [Appendix A, "Mounting the Multicast VoIP Microphone"](#) for instructions.

2.2.1 Factory Default Settings

All Multicast VoIP Microphones are initially configured with the following default IP settings:

When configuring more than one Multicast VoIP Microphone, attach the Multicast VoIP Microphones to the network and configure one at a time to avoid IP address conflicts.

Table 2-4. Factory Default Settings

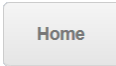
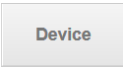

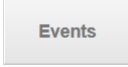
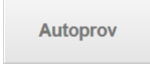

Parameter	Factory Default Setting
IP Addressing	DHCP
IP Address ^a	10.10.10.10
Web Access Username	admin
Web Access Password	admin
Subnet Mask ^a	255.0.0.0
Default Gateway ^a	10.0.0.1

a. Default if there is not a DHCP server present.

2.2.2 Multicast VoIP Microphone Web Page Navigation

Table 2-5 shows the navigation buttons that you will see on every Multicast VoIP Microphone web page.

Table 2-5. Web Page Navigation

Web Page Item	Description
	Link to the Home page.
	Link to the Device page.
	Link to the Network page.
	Link to the Events page.
	Link to the Autoprovisioning page.
	Link to the Firmware page.

2.2.3 Using the Toggle Help Button

The **Toggle Help** button allows you to see a short description of some of the settings on the webpage. To use the **Toggle Help** button, do the following:

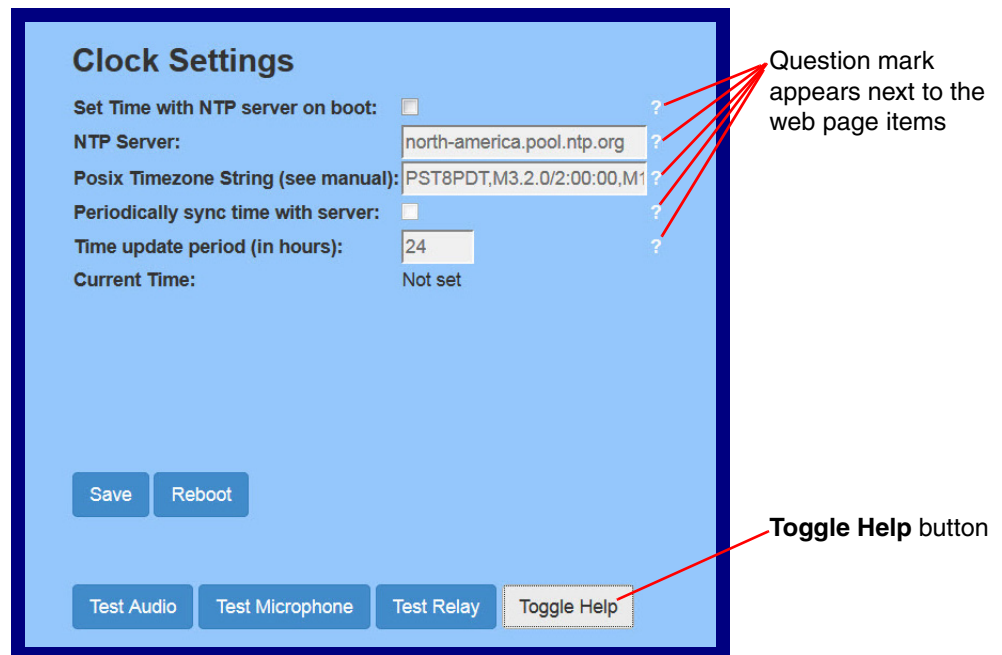
1. Click on the **Toggle Help** button that is on the UI webpage. See [Figure 2-6](#) and [Figure 2-7](#).

Figure 2-6. Toggle/Help Button



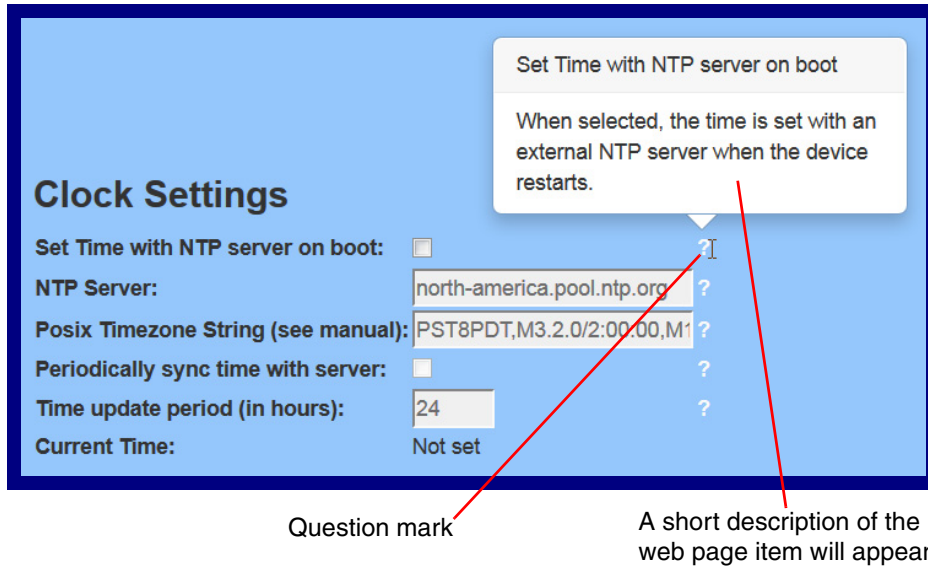
2. You will see a question mark (?) appear next to each web page item that has been provided with a short description by the Help feature. See [Figure 2-7](#).

Figure 2-7. Toggle Help Button and Question Marks



3. Move the mouse pointer to hover over the question mark (?), and a short description of the web page item will appear. See Figure 2-8.

Figure 2-8. Short Description Provided by the Help Feature



2.2.4 Log in to the Configuration Home Page

1. Open your browser to the Multicast VoIP Microphone IP address.

Note If the network does not have access to a DHCP server, the device will default to an IP address of 10.10.10.10.

Note Make sure that the PC is on the same IP network as the Multicast VoIP Microphone.

Note You may also download CyberData's VoIP Discovery Utility program which allows you to easily find and configure the default web address of the CyberData VoIP products.

CyberData's VoIP Discovery Utility program is available at the following website address:

<http://www.cyberdata.net/assets/common/discovery.zip>

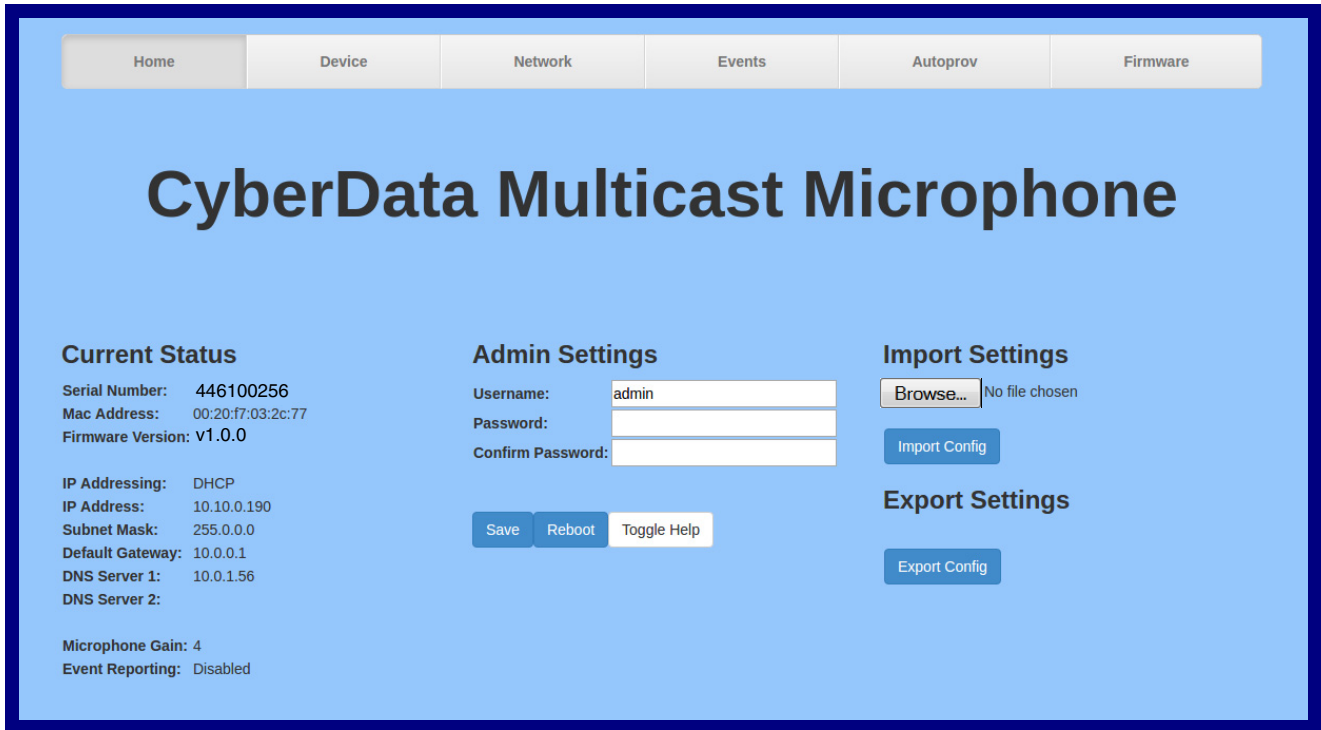
Note The device ships in DHCP mode. To get to the **Home** page, use the discovery utility to scan for the device on the network and open your browser from there.

2. When prompted, use the following default **Web Access Username** and **Web Access Password** to access the **Home Page** (Figure 2-9):

Web Access Username: **admin**

Web Access Password: **admin**

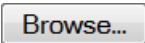




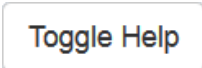
Figure 2-9. Home Page



3. On the **Home** page, review the setup details and navigation buttons described in [Table 2-6](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-6. Home Page Overview

Web Page Item	Description
Admin Settings	
Username ?	The username to access the web interface. Enter up to 25 characters.
Password ?	The password to access the web interface. Enter up to 25 characters.
Confirm Password ?	Confirm the web interface password.
Current Status	
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
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 current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
Microphone Gain	Shows the current level of the Microphone Gain
Event Reporting	Shows the current status of the Event Reporting mode.
Import Settings	
	Use this button to select a configuration file to import.
	After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.
Export Settings	
	Click Export to export the current configuration to a file.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

2.2.5 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See [Figure 2-10](#).

Figure 2-10. Device Configuration Page

The screenshot shows the 'Device Configuration' page for a CyberData Multicast Microphone. The page features a navigation bar with tabs for Home, Device, Network, Events, Autoprovisioning, and Firmware. The main heading is 'CyberData Multicast Microphone'. The settings are organized into four sections:

- Multicast Settings:** Multicast Address: 224.5.5.5; Multicast Port: 5050; Buffer Multicast: ; Enable Polycom Paging on Multicast: ; Polycom Transmit Channel: 1 (dropdown).
- Microphone Settings (0-9):** Microphone Gain: 4.
- Clock Settings:** Set Time with NTP server on boot: ; NTP Server: north-america.pool.ntp.org; Posix Timezone String (see manual): PST8PDT,M3.2.0/2:00:00,M11.1.0; Periodically sync time with server: ; Time update period (in hours): 24; Current Time: 07:01:56.
- Misc Settings:** Device Name: Multicast Microphone; Button Lit when Idle: ; Button Brightness (0-255): 255; Disable HTTPS (NOT recommended): .

At the bottom of the page, there are 'Save' and 'Reboot' buttons, and a 'Toggle Help' button.










2. On the **Device** page, you may enter values for the parameters indicated in [Table 2-7](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-7. Device Configuration Parameters

Web Page Item	Description
Multicast Settings	
Multicast Address ?	The multicast address used for multicasting live audio. Note: The Multicast Address setting requires a reboot for the changes to take effect.
Multicast Port ?	The multicast port used for multicasting live audio. The port must be an even number. Note: The Multicast Port setting requires a reboot for the changes to take effect.
Buffer Multicast ?	When enabled, this setting will record audio picked up by the mic into a buffer while the button is held, and multicast it when the button is released. Maximum message length is 60 seconds.
Enable Polycom Paging on Multicast ?	Enabling Polycom Paging will result in a standard RTP multicast being sent to the specified address and port and a Polycom Group Paging multicast being sent to the specified address and port+1. Note: The Enabling Polycom Paging setting requires a reboot for the changes to take effect. Note: To make a multicast page, press the call button. The microphone should generally be used at a distance of 6 inches, but may be adjusted to suit your environment.
Polycom Transmit Channel ?	Destination channel for Polycom Group Paging multicast.
Clock Settings	
Set Time with NTP Server on boot ?	When selected, the time is set with an external NTP server when the device restarts.
NTP Server ?	Use this field to set the address (in IPv4 dotted decimal notation or as a canonical name) for the NTP Server. This field can accept canonical names of up to 64 characters in length. Note: The NTP Server setting needs to be restarted to spawn NTP or to change the server.
Posix Timezone String ?	See Section 2.2.5.1, "Time Zone Strings" for information about how to use the Posix Timezone String to specify time zone and daylight savings time where applicable. Enter up to 63 characters.
Periodically sync time with server ?	When selected, the time is periodically updated with the NTP server at the configured interval below.
Time update period (in hours) ?	The time interval after which the device will contact the NTP server to update the time. Enter up to 4 digits. Note: Syncing and changing the Time update period (in hours) setting does not require a reboot for the changes to take effect.
Current Time	Displays current time (6 character limit).
Microphone Settings	

Table 2-7. Device Configuration Parameters (continued)

Web Page Item	Description
Microphone Gain 	Set the microphone gain level. Note: The Microphone Gain setting does not require a reboot for the changes to take effect.
Misc Settings	
Device Name 	Type the device name. Enter up to 25 characters.
Button Lit When Idle 	When selected, the Call button LED is illuminated while the device is idle (a call is not in progress).
Button Brightness (0-255) 	The desired Call button LED brightness level. Acceptable values are 0-255, where 0 is the dimmest and 255 is the brightest. Enter up to three digits.
Disable HTTPS (NOT recommended) 	Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons. Note: The Disable HTTPS (NOT recommended) setting requires a reboot for the changes to take effect.
	Click the Save button to save your configuration settings. Note: You must click on the Save button and then the Reboot button for the changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark () appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

Note To make a multicast page, press the call button. The microphone should generally be used at a distance of 6 inches, but may be adjusted to suit your environment.

2.2.5.1 Time Zone Strings

The posix time zone string tells the internal date and time utilities how to handle daylight savings time for different time zones. [Table 2-8](#) shows some common strings.

Table 2-8. Common Time Zone Strings

Time Zone	Time Zone String
US Pacific time	PST8PDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Mountain time	MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
US Eastern Time	EST5EDT,M3.2.0/2:00:00,M11.1.0/2:00:00
Phoenix Arizona ^a	MST7
US Central Time	CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00

a. Phoenix, Arizona does not use daylight savings time.

[Table 2-9](#) shows a breakdown of the parts that constitute the following time zone string:

- ***CST6DST,M3.2.0/2:00:00,M11.1.0/2:00:00***

Table 2-9. Time Zone String Parts

Time Zone String Part	Meaning
CST6CDT	The time zone offset from GMT and three character identifiers for the time zone.
CST	Central Standard Time
6	The (hour) offset from GMT/UTC
CDT	Central Daylight Time
M3.2.0/2:00:00	The date and time when daylight savings begins.
M3	The third month (March)
.2	The 2nd occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change
M11.1.0/2:00:00	The date and time when daylight savings ends.
M11	The eleventh month (November)
.1	The 1st occurrence of the day (next item) in the month
.0	Sunday
/2:00:00	Time of day to change

Time Zone String Examples [Table 2-10](#) has some more examples of time zone strings.

Table 2-10. Time Zone String Examples

Time Zone	Time Zone String
Tokyo ^a	IST-9
Berlin ^b	CET-1MET,M3.5.0/1:00,M10.5.0/1:00

a. Tokyo does not use daylight savings time.

b. For Berlin, daylight savings time starts on the last Sunday in March at 01:00 UTC, and ends on the last Sunday in October at 01:00 UTC, and is one hour ahead of UTC.

Time Zone Identifier A user-definable three or four character time zone identifier (such as PST, EDT, IST, MUT, etc) is needed at the beginning of the posix time zone string to properly set the time. However, the specific letters or numbers used for the time zone identifier are not important and can be any three or four letter or number combination that is chosen by the user. However, the time zone identifier cannot be blank.

Figure 2-11. Three or Four Character Time Zone Identifier

You can also use the following URL when a certain time zone applies daylight savings time:

<http://www.timeanddate.com/time/dst/2011.html>

World GMT Table [Table 2-11](#) has information about the GMT time in various time zones.

Table 2-11. World GMT Table

Time Zone	City or Area Zone Crosses
GMT-12	Eniwetok
GMT-11	Samoa
GMT-10	Hawaii
GMT-9	Alaska
GMT-8	PST, Pacific US
GMT-7	MST, Mountain US
GMT-6	CST, Central US
GMT-5	EST, Eastern US
GMT-4	Atlantic, Canada
GMT-3	Brazilia, Buenos Aries
GMT-2	Mid-Atlantic
GMT-1	Cape Verdes
GMT	Greenwich Mean Time, Dublin
GMT+1	Berlin, Rome
GMT+2	Israel, Cairo
GMT+3	Moscow, Kuwait
GMT+4	Abu Dhabi, Muscat

Table 2-11. World GMT Table (continued)

Time Zone	City or Area Zone Crosses
GMT+5	Islamabad, Karachi
GMT+6	Almaty, Dhaka
GMT+7	Bangkok, Jakarta
GMT+8	Hong Kong, Beijing
GMT+9	Tokyo, Osaka
GMT+10	Sydney, Melbourne, Guam
GMT+11	Magadan, Soloman Is.
GMT+12	Fiji, Wellington, Auckland

2.2.6 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-12).

Figure 2-12. Network Configuration Page

The screenshot shows the Network Configuration page for a CyberData Multicast Microphone. The page has a blue background and a navigation bar at the top with buttons for Home, Device, Network (selected), Events, Autoprovisioning, and Firmware. The main heading is "CyberData Multicast Microphone".

Stored Network Settings

Addressing Mode: Static DHCP

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

DNS Server 1:

DNS Server 2:

DHCP Timeout in seconds*:

* A value of -1 will retry forever

VLAN Settings

VLAN ID (0-4095):

VLAN Priority (0-7):

Current Network Settings

IP Address: 10.10.0.190

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.1.56

DNS Server 2:

Buttons: Save, Reboot, Toggle Help




2. On the **Network** page, enter values for the parameters indicated in [Table 2-12](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-12. Network Configuration Parameters

Web Page Item	Description
Stored Network Settings	
Addressing Mode ?	Select either DHCP IP Addressing or Static Addressing by marking the appropriate radio button. DHCP Addressing mode is enabled on default and the device will attempt to resolve network addressing with the local DHCP server upon boot. If DHCP Addressing fails, the device will revert to the last known IP address or the factory default address if no prior DHCP lease was established. See Section 2.2.1, "Factory Default Settings" for factory default settings. Be sure to click Save and Reboot to store changes when configuring a Static address.
Hostname ?	This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.
IP Address ?	Enter the Static IPv4 network address in dotted decimal notation.
Subnet Mask ?	Enter the Subnet Mask in dotted decimal notation.
Default Gateway ?	Enter the Default Gateway IPv4 address in dotted decimal notation.
DNS Server 1 ?	Enter the primary DNS Server IPv4 address in dotted decimal notation.
DNS Server 2 ?	Enter the secondary DNS Server IPv4 address in dotted decimal notation.
DHCP Timeout in seconds ?	Specify the desired time-out duration (in seconds) that the device will wait for a response from the DHCP server before reverting back to the stored static IP address. The stored static IP address may be the last known IP address or the factory default address if no prior DHCP lease was established. Enter up to 8 characters. A value of -1 will retry forever.
Current Network Settings	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
VLAN Settings	
VLAN ID (0-4095) ?	Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. Note: The device supports 802.1Q VLAN tagging support. The switch port connected to the device will need to be in "trunking mode" for the VLAN tags to propagate.
VLAN Priority (0-7) ?	Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.

Table 2-12. Network Configuration Parameters (continued)

Web Page Item	Description
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.2.7 Configure the Event Parameters

1. Click the **Event Config** button to open the **Event Configuration** page (Figure 2-13). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-13. Event Configuration Page

Home Device Network **Events** Autoprovisioning Firmware

CyberData Multicast Microphone

Enable Event Generation:

Events

Enable Button Events:

Enable Power On Events:

Enable 60 Second Heartbeat:

[Check All](#) [Uncheck All](#)

Event Server

Server IP Address: 10.0.0.250

Server Port: 8080




Server URL: xmlparse_engine

[Save](#) [Reboot](#) [Toggle Help](#)

2. On the **Events** page, enter values for the parameters indicated in [Table 2-13](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-13. Events Configuration Parameters

Web Page Item	Description
Enable Event Generation ?	The device will send HTTP POST events to the specified remote server and port number whenever a certain action takes place. Select an event type below to generate an HTTP POST event.
Events	
Enable Button Events ?	When selected, the device will report Call button presses.
Enable Power On Events ?	When selected, the device will report when it boots.
Enable 60 Second Heartbeat Events ?	When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.
Check All	Click on Check All to select all of the events on the page.
Uncheck All	Click on Uncheck All to de-select all of the events on the page.
Event Server	
Server IP Address ?	The IPv4 address of the event server in dotted decimal notation.
Server Port ?	Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.
Server URL ?	Generally, the destination URL is the name of the application that receives the events and the string in the HTTP POST command. It can be a script used to parse and process the HTTP POST events. Enter up to 127 characters.
	Click the Save button to save your configuration settings. Note: You need to reboot for changes to take effect.
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.2.7.1 Example Packets for Events

The server and port are used to point to the listening server and the 'Remote Event Server URL' is the destination URL (typically the script running on the remote server that's used to parse and process the POST events).

Note The XML is URL-encoded before transmission so the following examples are not completely accurate.

Here are example packets for every event:

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>POWERON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 199
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>HEARTBEAT</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 196
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>BUTTON</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 201
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>CALL_TERMINATED</event>
</cyberdata>
```

```
POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 197
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>RINGING</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>RELAY_DEACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded
<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>NIGHTRINGING</event>
</cyberdata>
```

2.2.8 Configure the Autoprovisioning Parameters

Autoprovisioning can be used to automatically configure your device. The autoprovisioning file is an xml file with the device configuration. Values found in this file will override values stored in on-board memory.

Note By default, the device will try to set up its configuration with autoprovisioning.

1. Click the **Autoprov** menu button to open the **Autoprovisioning** page. See [Figure 2-14](#).

Figure 2-14. Autoprovisioning Page

Home Device Network Events Autoprov Firmware

CyberData Multicast Microphone

Disable Autoprovisioning:

Autoprovisioning Server:

Autoprovisioning Filename:

Use tftp:

Username:

Password:

Autoprovisioning autoupdate (in minutes):

Autoprovision at time (HHMMSS):

Autoprovision when idle (in minutes > 10):

See the manual to learn how to use autoprovisioning to configure your device.

Autoprovisioning happens on boot.

The device will first look for a configured server address and filename.

If these haven't been configured, it will look for an autoprovisioning server in your list of DHCP options and try to download '0020f7032c77.xml' and if this fails, '000000cd.xml'.

Save Reboot Toggle Help

Download Template

Autoprovisioning log

```
16:55 Autoprovisioning Device...
16:56 Autoprov found option 43 in DHCP server="http://10.0.0.242"
16:56 Autoprov looking for 0020f7032c77.xml at http://10.0.0.242
16:56 Autoprov: didn't find autoprov file
16:56 Autoprov looking for 000000cd.xml at http://10.0.0.242
16:56 Autoprov: didn't find autoprov file
16:56 Failed to fetch autoprov file
16:56 Autoprov found option 72 in DHCP server="10.0.0.252"
16:56 Autoprov looking for 0020f7032c77.xml at 10.0.0.252
16:56 Autoprov: didn't find autoprov file
```

- On the **Autoprovisioning** page, you may enter values for the parameters indicated in [Table 2-14](#).

Note The question mark icon (?) in the following table shows which web page items will be defined after the **Toggle Help** button is pressed.

Table 2-14. Autoprovisioning Configuration Parameters





Web Page Item	Description
Disable Autoprovisioning ?	Prevent the device from automatically trying to download a configuration file. See Section 2.2.8.1, "Autoprovisioning" for more information.
Autoprovisioning Server ?	Enter the IPv4 address of the provisioning server in dotted decimal notation.
Autoprovisioning Filename ?	<p>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <mac address>.xml.</p> <p>Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the Autoprovisioning Page. Enter up to 256 characters.</p> <p>A file may have any name with an xml extension. If a file name is entered, the device will look for the specified file name, and only that file.</p>
Use tftp ?	The device will use TFTP (instead of http) to download autoprovisioning files.
Username ?	The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Password ?	The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.
Autoprovisioning Autoupdate (in minutes) ?	<p>The reoccurring time (in minutes) the device will wait before checking for new autoprovisioning files. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page page (see Table 2-7).</p>
Autoprovision at time (HHMMSS) ?	<p>The time of day the device will check for a new autoprovisioning file. The time must be 6 characters in length and in HHMMSS format. An empty value will disable this option.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page page (see Table 2-7).</p>
Autoprovision when idle (in minutes > 10) ?	<p>The idle time (in minutes greater than 10) after which the device will check for a new autoprovisioning file. Enter up to 6 digits. A value of 0 will disable this option.</p> <p>Note: To use the auto update options, enable the Set Time with NTP Server on boot setting on the Device Configuration Page page (see Table 2-7).</p>
	<p>Click the Save button to save your configuration settings.</p> <p>Note: You need to reboot for changes to take effect.</p>

Table 2-14. Autoprovisioning Configuration Parameters (continued)

Web Page Item	Description
	Click on the Reboot button to reboot the system.
	Click on the Toggle Help button to see a short description of some of the web page items. First click on the Toggle Help button, and you will see a question mark (?) appear next to some of the web page items. Move the mouse pointer to hover over a question mark to see a short description of a specific web page item.
	Press the Download Template button to create an autoprovisioning file for the device. See Section 2.2.8.3, "Download Template Button"
Autoprovisioning log	The autoprovisioning log provides information about the latest autoprovisioning attempt (i.e. dhcp options and server accessed and files parsed or not found).

Note You must click on the **Save** button and then the **Reboot** button for the changes to take effect.

2.2.8.1 Autoprovisioning

On boot, the device will look for an autoprovisioning server configured on the [Autoprovisioning Page](#) or specified as a DHCP option. When it finds a server, it will try to download the following (in order of preference):

1. The file configured on the autoprovisioning page.
2. A file named according to it's mac address (for example: 0020f7350058.xml).
3. The file 000000cd.xml

The file can be hosted using a standard web server (like apache, IIS, or nginx), and the device can download over SSL. The file server can be an ipv4 address in dotted decimal notation or a fully qualified domain name.

By default, the device will get its autoprovisioning server from the DHCP options. See [Section 2.2.8.2, "Sample dhcpd.conf"](#) for an example of how to configure dhcpd to offer autoprovisioning server addresses. If multiple options are set, the device will attempt to download autoprovisioning files from every server.

The DHCP option determines the protocol used to download the autoprovisioning file. The device looks for DHCP options in the following order:

1. Option 43 - a FQDN or an IP address to an http server
2. Option 72 - an IP address to an http server
3. Option 150 - an IP address to a tftp server
4. Option 66 - an IP address to a tftp server or if the entry starts with 'http', a FQDN to a http server.

You can download an auto provisioning template file from the [Auto provisioning Page](#) using the **Download Template** button (see [Table 2-14](#)). This file contains every configuration option that can be set on the board.

Auto provisioning files can contain the whole configuration or a subset of this file. The first auto provisioning file can also contain links to other auto provisioning files.

The <MiscSettings> section contains some examples of additional auto provisioning files:

```
<MiscSettings>
  <DeviceName>CyberData VoIP Intercom</DeviceName>
<!-- <AutoproFile>common.xml</AutoproFile>-->
<!-- <AutoproFile>sip_reg [macaddress] .xml</AutoproFile>-->
<!-- <AutoproFile>audio [macaddress] </AutoproFile>-->
<!-- <AutoproFile>device [macaddress] .xml</AutoproFile>-->
</MiscSettings>
```

After downloading the first auto provisioning file, the device will step through up to twenty additional <AutoproFile> entries and try to download these files from the same server.

When the device finds a filename with the string **[macaddress]**, it will replace this string with the mac address.

As an example, the user has configured option 43 on their DHCP server to “http://example.com,” and on their server, they have a file named **0020f7123456.xml** (the same as the mac address of the device).

The file 0020f7123456.xml contains:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
  <MiscSettings>
    <DeviceName>Newname</DeviceName>
    <AutoprovFile>common.xml</AutoprovFile>
    <AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>
    <AutoprovFile>audio[macaddress]</AutoprovFile>
    <AutoprovFile>device.xml</AutoprovFile>
  </MiscSettings>
</specific>
```

1. The device will first set its name to 'Newname'.
2. It will try to download <http://example.com/common.xml>.
3. It will try to download http://example.com/sip_reg0020f7123456.xml.
4. It will try to download <http://example.com/audio0020f7123456>.
5. It will try to download <http://example.com/device.xml>.

The device is reconfigured every time it downloads a new file so if two files configure the same option the last one will be the one that is saved.

It is possible to autoprovision autoprovisioning values (for example, to disable autoprovisioning or to configure a time to check for new files).

Checking for New
Autoprovisioning
Files after Boot

The device will always check for an autoprovisioning files on boot but it can be configured to also check after a periodic delay, when idle, or at a specified time. When one of these options is set, the device will download its autoprovisioning files again, and if it finds any differences from the files it downloaded on boot, it will force a reboot and reconfigure.

The
Autoprovisioning
Filename

The autoprovisioning filename can contain a file, a file path, or a directory.

Table 2-15. Autoprovisioning File Name

Autoprovisioning Filename	Autoprovisioning Server	File Downloaded
config.xml	10.0.1.3	10.0.1.3/config.xml
/path/to/config.xml	10.0.1.3	10.0.1.3/path/to/config.xml
subdirectory/path/	10.0.1.3	10.0.1.3/subdirectory/path/0020f7020002.xml

TFTP options may not support subdirectories. If a directory is set in the filename field, firmware and audio files will also be downloaded from this subdirectory.

If the filename ends with a forward slash “/,” the device will treat it as a subdirectory.

For example:

The autoprovisioning server is set to “https://www.example.com”

The autoprovisioning filename is set to “cyberdata/”

On boot, the device will try to download:

https://www.example.com/cyberdata/0020f7123456.xml

...and if this fails:

https://www.example.com/cyberdata/000000cd.xml

Audio files and firmware files will also add “cyberdata” to the URL before downloading.

```

Autoprovisioning <FirmwareSettings>
Firmware Updates <FirmwareFile>505-uImage-ceiling-speaker</FirmwareFile>
                  <FirmwareServer>10.0.1.3</FirmwareServer>
                  <OutdoorIntercom30>firmware_file_v9.3.0</OutdoorIntercom30>
                  <OutdoorIntercom31>firmware_file_v10.3.0</OutdoorIntercom31>
                  <CallButton31>firmware_file_v10.3.0</CallButton31>
                  </FirmwareSettings>

```

In the <FirmwareSettings> section, the <FirmwareServer> element can be used to specify a different server for hosting firmware files. When this element is not available, the device will try to download the file from the autoprovisioning server.

The device will use the filename to determine when to autoprovision firmware updates. The default configuration is blank, so the first time you set a value in your autoprovisioning file, it may force a firmware update even if the firmware version has not changed.

The <FirmwareFile> name can contain path elements (i.e. /path/to/firmware/10.3.0-ulmage-[device_file_name]).

The device also supports product strings for downloading firmware. If the <FirmwareFile> option is not set, the device will look for its particular product string for a firmware filename. In this way, a generic autoprovisioning file can specify unique firmware for a range of products.

The list of valid product strings:

```

<ProductString>CallButton31</ProductString>
<ProductString>EmergencyIntercom31</ProductString>
<ProductString>EmergencyIntercom31SW</ProductString>
<ProductString>IndoorIntercom31</ProductString>
<ProductString>IndoorIntercom31SW</ProductString>
<ProductString>IndoorKeypad31</ProductString>
<ProductString>IndoorKeypad31SW</ProductString>
<ProductString>OfficeRinger31</ProductString>
<ProductString>OfficeRinger31SW</ProductString>
<ProductString>OutdoorIntercom31</ProductString>
<ProductString>OutdoorIntercom31SW</ProductString>
<ProductString>OutdoorKeypad31</ProductString>
<ProductString>OutdoorKeypad31SW</ProductString>
<ProductString>Strobe31</ProductString>
<ProductString>Strobe31SW</ProductString>

```

Autoprovisioning
Example 1

Here's a simple example using four autoprovisioning files to configure two devices:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2).

The devices are set to use DHCP and that server provides an autoprovisioning server address with option 43. The address is "https://autoprovtest.server.net." The files on this server are as follows:

000000cd.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
<AutoprovFile>sip_common.xml</AutoprovFile>
<AutoprovFile>sip_[macaddress].xml</AutoprovFile>
</MiscSettings>
```

sip_common.xml

```
<SIPSettings>
<SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

sip_0020f7020001.xml

```
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

sip_0020f7020002.xml

```
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

On boot, Device1 tries to fetch the file **0020f7023614.xml** from "https://autoprovtest.server.net". This file is not available, so device1 then tries to fetch the file **000000cd.xml**. This file exists, and Device1 parses the three elements.

1. Device1 changes its device name to **CyberData Autoprovisioned**.
2. Device1 finds an AutoprovFile element containing the filename **sip_common.xml**. The device downloads **sip_common.xml** from "https://autoprovtest.server.net," and imports this configuration, setting the sip server to **10.0.0.253** and the remote port to **5060.3**.
3. Device1 finds another AutoprovFile element containing the filename **sip_[macaddress].xml**. The device replaces the **[macaddress]** with its own mac address value creating **sip_0020f7020001.xml**, downloads this file from "https://autoprovtest.server.net," and imports this configuration. This sets the user ID to **198**, the password to **ext198**, and the dialout extension to **204**. Device1 is now finished with autoprovisioning.

Device2 goes through the same steps by setting its device name to **CyberData Autoprovisioned**, its SIP server to **10.0.0.253**, and its port to **5060**. When Device2 “sees” **sip_[macaddress].xml**, Device2 replaces it with its own mac address and downloads **sip_0020f7020002.xml** from “https://autoprovttest.server.net.” Device2 sets the SIP User ID to **500**, the password to **ext500**, and the dialout extension to **555**.

Autoprovisioning Example 2

Here is another example of setting up your autoprovisioning files:

We boot up two devices with mac addresses **00:20:f7:02:00:01** and **00:20:f7:02:00:02** (Device1 and Device2) and boot them on a network with a DHCP server configured with an autoprovisioning server at **10.0.1.3** on option **150**. Our TFTP server has three files:

0020f7020001.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>198</SIPUserID>
<SIPAuthPassword>ext198</SIPAuthPassword>
<DialoutExtension0>204</DialoutExtension0>
</SIPSettings>
```

0020f7020002.xml

```
<MiscSettings>
<AutoprovFile>common_settings.xml</AutoprovFile>
</MiscSettings>
<SIPSettings>
<SIPUserID>500</SIPUserID>
<SIPAuthPassword>ext500</SIPAuthPassword>
<DialoutExtension0>555</DialoutExtension0>
</SIPSettings>
```

common_settings.xml

```
<MiscSettings>
<DeviceName>CyberData Autoprovisioned</DeviceName>
</MiscSettings>
<SIPSettings> <SIPServer>10.0.0.253</SIPServer>
<RemoteSIPPort>5060</RemoteSIPPort>
</SIPSettings>
```

1. On boot, Device1 downloads **0020f7020001.xml** from **10.0.1.3** and imports these values. The SIP User ID is **198**, the password is **ext198**, and the dialout extension is **204**.

2. Device1 then gets the filename **common_settings.xml** from the AutoprovFile element and downloads this file from the TFTP server at **10.0.1.3**. and imports these settings. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

Device2 does the same except it downloads **0020f7020002.xml** on boot and imports these values instead. The Sip User ID is **500**, password is **ext500**, and dialout extension is **555**. Device2 then downloads the **common_settings.xml** file and imports those values. The device name is set to **CyberData Autoprovisioned**, the SIP server is set to **10.0.0.253**, and the port is set to **5060**.

XML Files

XML files can contain <AutoprovFile> elements. If multiple DHCP options are specified, the device will try to download auto provisioning files from each in turn. The device will only look for <AutoprovFile> elements in the first file downloaded from each server. You can specify up to 20 <AutoprovFile> elements in the first auto provisioning file.

There are numerous ways to change an element of the **configuration(xml)** file. Using **sip ext** as an example, the extension can be changed:

Within the device-specific xml, i.e. **[macaddress].xml**, via the AutoprovFile element:<SIPSettings>/<SIPExt>

From the device specific xml, a pointer to a sip_common file

From the device specific xml, a pointer to the device specific sip_[macaddress].xml

From the common file, a pointer to sip_common.xml

From the common file, a pointer to the device specific (sip_[macaddress].xml)

Autoprovisioned Audio Files

Audio files are stored in non-volatile memory and an auto provisioned audio file will only have to be downloaded once for each device. Loading many audio files to the device from the web page could cause it to appear unresponsive. If this happens, wait until the transfer is complete and then refresh the page.

The device uses the file name to determine when to download a new audio file. This means that if you used auto provisioning to upload a file and then changed the contents of this file at the TFTP server, the device will not recognize that the file has changed (because the file name is the same).

Since audio files are stored in non-volatile memory, if auto provisioning is disabled after they have been loaded to the board, the audio file settings will not change. You can force a change to the audio files on the board by clicking **Restore Default** on the **Audio Configuration** page or by changing the auto provisioning file with “**default**” set as the file name.

2.2.8.2 Sample dhcpd.conf

```
#
# Sample configuration file for ISC dhcpd for Debian
#

ddns-update-style none;

option domain-name "voiplab";
option domain-name-servers 10.0.0.252;
option option-150 code 150 = ip-address;
option ntp-servers north-america.pool.ntp.org;
option space VendorInfo;
option VendorInfo.text code 10 = { text };
authoritative;
log-facility local7;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 3600;
    default-lease-time 3600;

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

    option domain-name            "voiplab";
    option domain-name-servers    10.0.0.252;

    option time-offset            -8;                # Pacific Standard Time

#    option www-server             99.99.99.99;        # OPTION 72

#    option tftp-server-name       "10.0.1.52";        # OPTION 66
#    option tftp-server-name       "http://test.cyberdata.net"; # OPTION 66

#    option option-150             10.0.0.252;        # OPTION 150

# These two lines are needed for option 43
#    vendor-option-space VendorInfo;                # OPTION 43
#    option VendorInfo.text "http://test.cyberdata.net"; # OPTION 43

    range 10.10.0.1 10.10.2.1; }
}
```

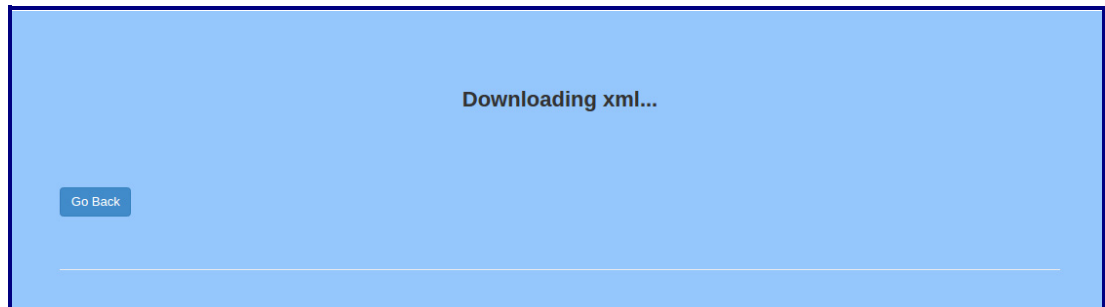

2.2.8.3 Download Template Button

The **Download Template** button allows the user to generate, download, edit, and then store an auto provisioning template on the server that serves the auto provisioning files for devices.

To generate an auto provisioning template directly from the device, complete the following steps:

1. On the **Auto provisioning** page, click on the **Download Template** button.
2. You will see a window that displays the words **Downloading xml...** (Figure 2-15). The template that downloads is the basis for the default configuration settings for your unit. The file will be saved in the location specified in your web browser for downloaded files.

Figure 2-15. Configuration File



3. At this point, you can open and edit the auto provisioning template to change the configuration settings in the template for the unit. Save this file as the mac address of your device .xml to use DHCP auto provisioning options.
4. You can then upload the auto provisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.

2.2.9 Downloading the Firmware

To download the firmware to your computer:

1. Download the latest firmware file from the **Downloads** tab at the following webpage:
<http://www.cyberdata.net/voip/011446/>
2. Unzip the firmware version file. This file may contain the following:
 - Firmware file
 - Release notes
3. Log in to the Multicast VoIP Microphone home page as instructed in [Section 2.2.4, "Log in to the Configuration Home Page"](#).
4. Click on the **Firmware** menu button to open the **Firmware** page. See [Figure 2-16](#).

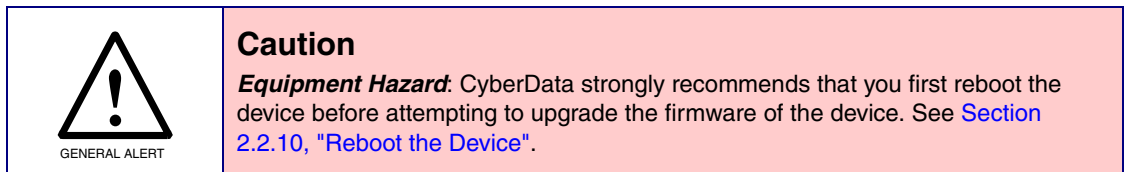


Figure 2-16. Firmware Page





5. Click on the **Browse** button, and then navigate to the location of the firmware file.
6. Select the firmware file.
7. Click on the **Upload** button.

Note Do not reboot the device after clicking on the **Upload** button.

Note This starts the upgrade process. Once the Multicast VoIP Microphone has uploaded the file, the **Uploading Firmware** countdown page appears, indicating that the firmware is being written to flash. The Multicast VoIP Microphone will automatically reboot when the upload is complete. When the countdown finishes, the **Firmware** page will refresh. The uploaded firmware filename should be displayed in the system configuration (indicating a successful upload and reboot).

8. [Table 2-16](#) shows the web page items on the **Firmware** page.

Table 2-16. Firmware Parameters

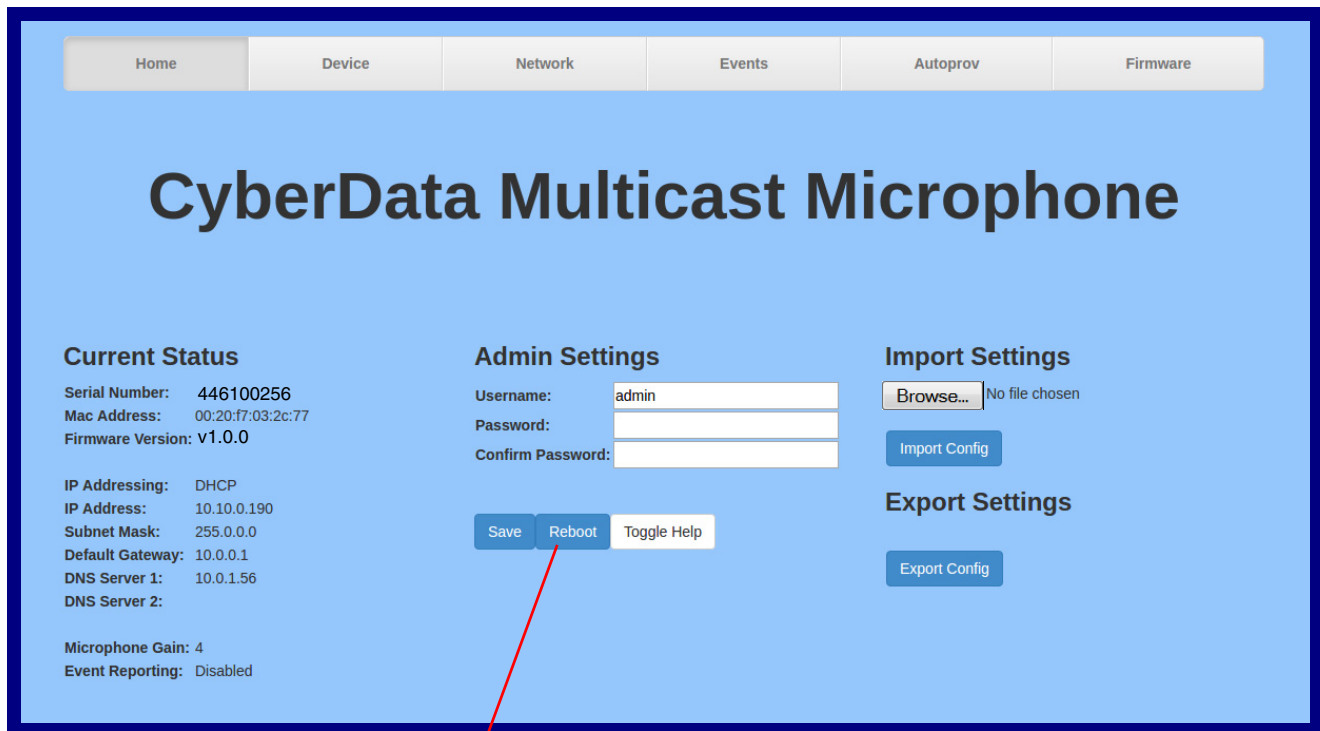
Web Page Item	Description
Current Firmware Version	Shows the current firmware version.
	Use the Browse button to navigate to the location of the firmware file that you want to upload.
	Click on the Upload button to automatically upload the selected firmware and reboot the system.

2.2.10 Reboot the Device

To reboot a Multicast VoIP Microphone, log in to the web page as instructed in [Section 2.2.4, "Log in to the Configuration Home Page"](#).

1. Click on the **Reboot** button on the **Home** page ([Figure 2-17](#)). A normal restart will occur.

Figure 2-17. Home Page



Reboot

2.3 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-17](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

2.3.1 Command Interface Post Commands

Note These commands require an authenticated session (a valid username and password to work).

Table 2-17. Command Interface Post Commands

Device Action	HTTP Post Command ^a
Force reboot	wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null "https://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"

a. Type and enter all of each http POST command on one line.

Appendix A: Mounting the Multicast VoIP Microphone

A.1 Mount the Multicast VoIP Microphone

Before you mount the Multicast VoIP Microphone, make sure that you have received all the parts for each Multicast VoIP Microphone. Refer to [Table A-1](#).

Table A-1. Wall Mounting Components (Part of the Accessory Kit)

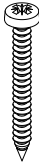
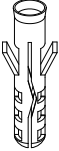
Quantity	Part Name	Illustration
2	#6 x 1.25 inches Sheet Metal Screw	
2	#6 Ribbed Plastic Anchor	

Figure A-1 shows the dimensions of the Multicast VoIP Microphone.

Figure A-1. Dimensions

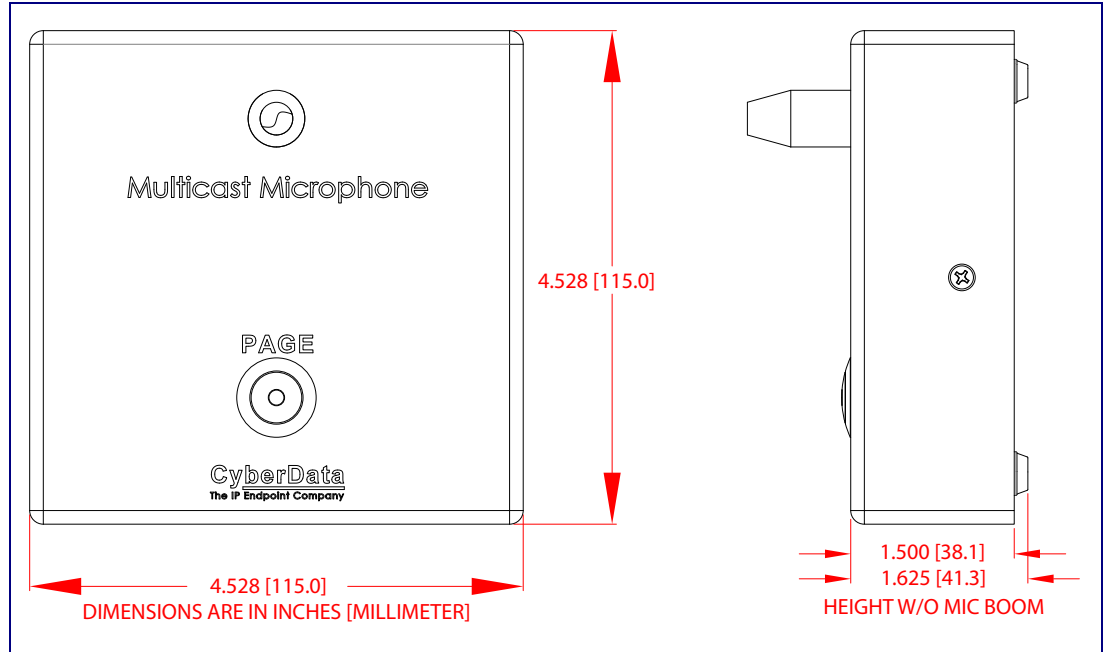


Figure A-1 shows how to connect the network cable to the Multicast VoIP Microphone.

Figure A-1. Network Cable Connection

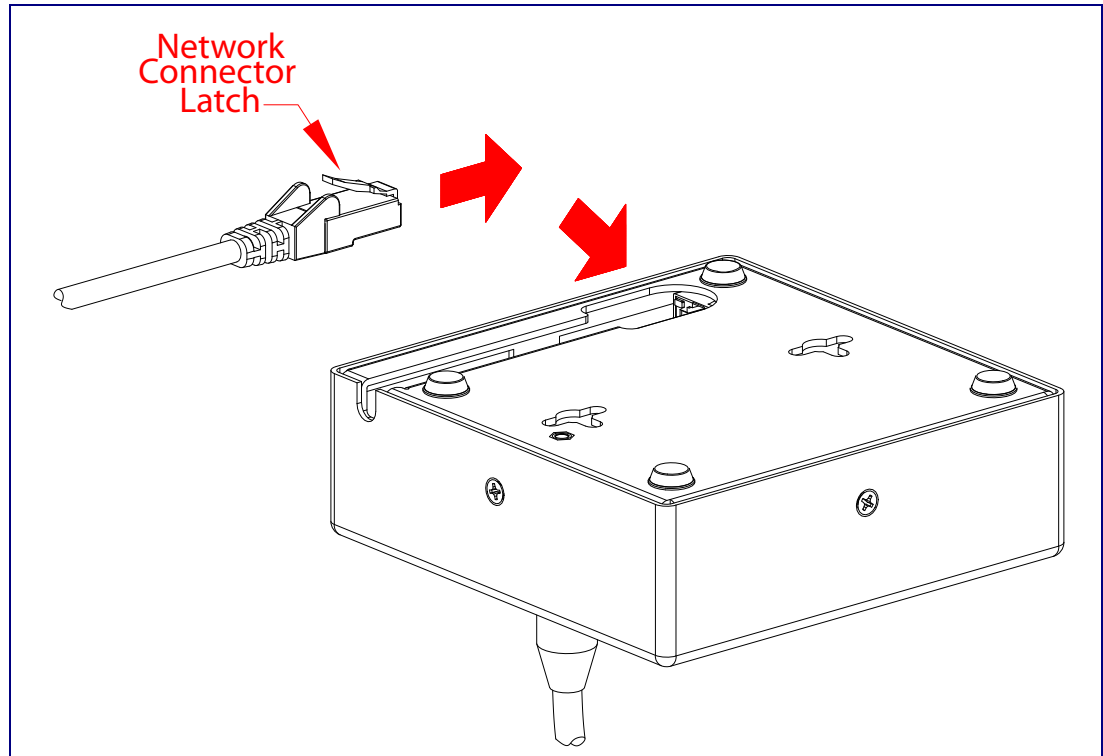


Figure A-2 shows the wall mounting option for the Multicast VoIP Microphone.

Figure A-2. Wall Mounting Options

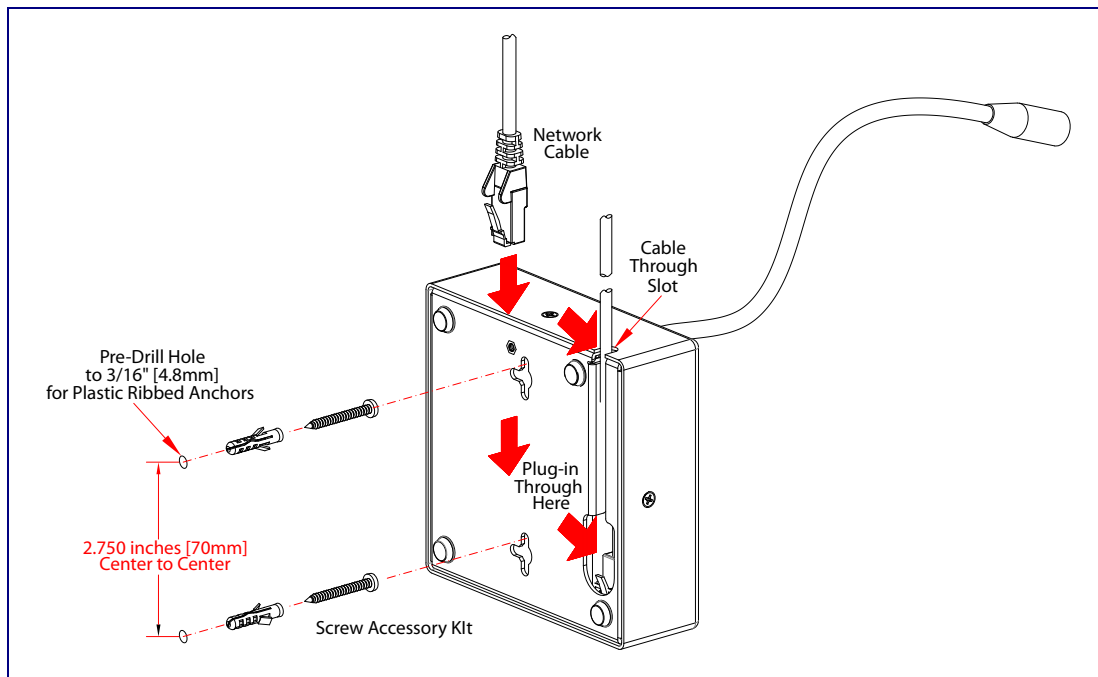
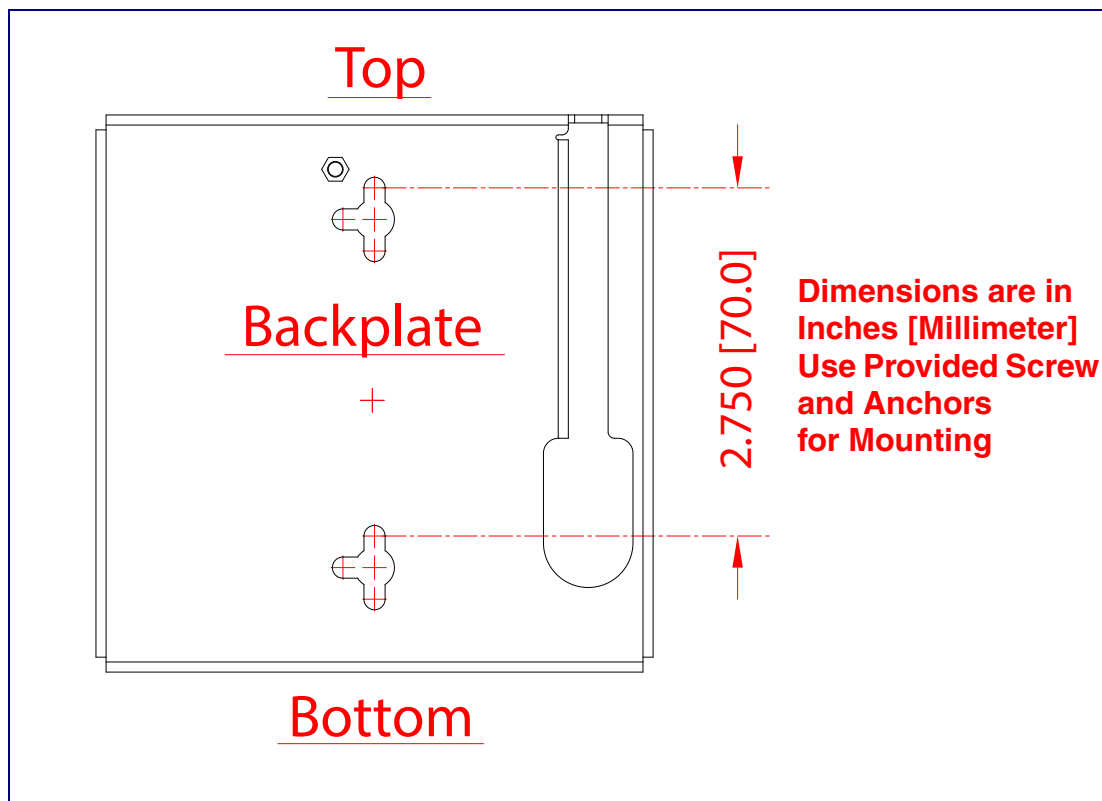


Figure A-3 shows the keyhole details of the Multicast VoIP Microphone.

Figure A-3. Keyhole Details



Appendix B: Troubleshooting/Technical Support

B.1 Frequently Asked Questions (FAQ)

To see a list of frequently asked questions for your product, click on the **FAQs** tab at the following webpage:

<http://www.cyberdata.net/voip/011446/>

B.2 Documentation

The documentation for this product is released in an English language version only.

To download PDF copies of CyberData product documentation, click on the **Downloads** tab at the following webpage:

<http://www.cyberdata.net/voip/011446/>

B.3 Contact Information

Contact CyberData Corporation
 3 Justin Court
 Monterey, CA 93940 USA
 www.CyberData.net
 Phone: 800-CYBERDATA (800-292-3732)
 Fax: 831-373-4193

Sales Sales 831-373-2601, Extension 334

Technical Support The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:

<http://support.cyberdata.net/>

The Support Form initiates a ticket which CyberData uses for tracking customer requests. Most importantly, the Support Form tells us which PBX system and software version that you are using, the make and model of the switch, and other important information. This information is essential for troubleshooting. Please also include as much detail as possible in the **Comments** section of the Support Form.

Phone: (831) 373-2601, Extension 333

B.4 Warranty and RMA Information

The most recent warranty and RMA information is available at the following website address:

<http://support.cyberdata.net/>

Index

A

- activity LED 8
- address, configuration login 15
- alternative power input 4
- audio encodings 3
- autoprovision at time (HHMMSS) 32
- autoprovision when idle (in minutes > 10) 32
- autoprovisioning 33
 - download template button 33
- autoprovisioning autoupdate (in minutes) 32
- autoprovisioning configuration 31, 32
- autoprovisioning filename 32
- autoprovisioning server (IP Address) 32

C

- call button configuration
 - default IP settings 11
- call button LED 10
- changing
 - the web access password 18
- command interface 46
- commands 46
- configurable parameters 19, 25
- configuration
 - default IP settings 11
 - network 24
 - using Web interface 11
- configuration home page 15
- configuration page
 - configurable parameters 19, 25
- contact information 51
- contact information for CyberData 51
- Current Network Settings 25
- current network settings 25
- CyberData contact information 51

D

- default
 - device settings 52
 - gateway 11
 - IP address 11
 - subnet mask 11
 - username and password 11
 - web login username and password 15
- default gateway 11, 25
- default IP settings 11
- default login address 15

- default settings 9
- device configuration 18
 - device configuration parameters 32
 - the device configuration page 31
- device configuration page 18
- device configuration parameters 19
- device configuration password
 - changing for web configuration access 18
- DHCP Client 3
- dimensions 4
- discovery utility program 15
- DNS server 25
- download autoprovisioning template button 33

E

- ethernet I/F 4
- export settings 17

F

- factory default settings 9
- firmware
 - where to get the latest firmware 43

G

- gang box mounting 49
- get autoprovisioning template 33
- GMT table 22
- GMT time 22

H

- home page 15
- http POST command 46
- http web-based configuration 3

I

- identifier names (PST, EDT, IST, MUT) 22
- identifying your product 1
- import settings 17
- import/export settings 17
- installation, typical intercom system 2

- IP address 11, 25
- IP addressing
 - default
 - IP addressing setting 11

L

- LED
 - green link LED 8
 - yellow activity LED 8
- link LED 8
- log in address 15

M

- mounting the device 47

N

- navigation (web page) 12
- navigation table 12
- network configuration 24
- Network Setup 24
- Nightringer 42
- NTP server 19

P

- part number 4
- parts list 5
- password
 - login 15
 - restoring the default 11
- payload types 4
- posix timezone string
 - timezone string 19
- POST command 46
- power input 4
 - alternative 4
- product
 - configuring 11
 - parts list 5
- product features 3
- product overview
 - product features 3
 - product specifications 4
 - supported protocols 3
 - supported SIP servers 4
 - typical system installation 2

- product specifications 4
- protocol 4
- protocols supported 3

R

- reboot 44, 45
- resetting the IP address to the default 47, 50
- restoring factory default settings 9, 52
- RJ-45 7
- RTFM jumper 9
- RTP/AVP 3

S

- sales 51
- service 51
- set time with external NTP server on boot 19
- settings, default 9
- SIP server
 - SIP servers supported 4
- subnet mask 11, 25
- supported protocols 3

T

- tech support 51
- technical support, contact information 51
- TFTP server 3
- time zone string examples 22

U

- username
 - changing for web configuration access 18
 - default for web configuration access 15
 - restoring the default 11

V

- VLAN ID 25
- VLAN Priority 25
- VLAN tagging support 25
- VLAN tags 25

W

- warranty policy at CyberData 51
- web access password 11
- web access username 11
- web configuration log in address 15
- web page
 - navigation 12
- web page navigation 12
- web-based configuration 11
- wget, free unix utility 46