COPYRIGHT NOTICE:
© 2019, 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 of 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 931532B, which corresponds to firmware version 1.1.0, was released on May 3, 2019 and has the following changes:

- Updates Figure 2-16, "Multicast Configuration Page"
- Updates Table 2-9, "Multicast Page Parameters"
- Adds Section A.3, "Disassemblies the Speaker"

Browsers Supported

The following browsers have been tested against firmware version 1.1.0:

- Internet Explorer (version: 11)
- Firefox (also called Mozilla Firefox) (version: 62.0)
- Chrome (version: 63.0.3239.132)
- Safari (version: 12)
- Microsoft Edge (version: 42.17134.1.0)
Pictorial Alert Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![General Alert Icon](image) | General Alert  
This pictoral alert indicates a potentially hazardous situation. This alert will be followed by a hazard level heading and more specific information about the hazard. |
| ![Ground Icon](image) | Ground  
This pictoral alert indicates the Earth grounding connection point. |

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.
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 Speaker enclosure is not rated for any AC voltages!**

<table>
<thead>
<tr>
<th>Warning</th>
<th><strong>Electrical Hazard:</strong> This product should be installed by a licensed electrician according to all local electrical and building codes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning</td>
<td><strong>Electrical Hazard:</strong> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</td>
</tr>
<tr>
<td>Warning</td>
<td>The PoE connector is intended for intra-building connections only and does not route to the outside plant.</td>
</tr>
<tr>
<td>Abbreviation or Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>A-law</td>
<td>A standard companding algorithm, used in European digital communications systems to optimize, i.e., modify, the dynamic range of an analog signal for digitizing.</td>
</tr>
<tr>
<td>AVP</td>
<td>Audio Video Profile</td>
</tr>
<tr>
<td>Cat 5</td>
<td>TIA/EIA-568-B Category 5</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per Second.</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PBX</td>
<td>Private Branch Exchange</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet (as per IEEE 802.3af standard)</td>
</tr>
<tr>
<td>RTFM</td>
<td>Reset Test Function Management</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiated Protocol</td>
</tr>
<tr>
<td>u-law</td>
<td>A companding algorithm, primarily used in the digital telecommunication</td>
</tr>
<tr>
<td>UC</td>
<td>Unified Communications</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
</tbody>
</table>
1 Product Overview

1.1 How to Identify This Product

To identify the Multicast Speaker, look for a model number label similar to the one shown in Figure 1-1. The model number on the label should be 011458.

Figure 1-1. Model Number Label
1.2 Typical Configuration

Figure 1-2 shows a typical configuration for the Multicast Speaker.

Figure 1-2. Typical Configuration
1.3 Product Features

- Plays audio from multicast
- Paging prioritization and background music
- Support for 10 multicast paging groups
- Network-adjustable speaker volume
- User upgradeable firmware via web interface or autoprovisioning
- 802.11q VLAN tagging
- Configurable event generation for device health and status monitoring
- Web-based configuration
- High efficiency speaker driver
- Small footprint
1.4 Supported Protocols

The Multicast Speaker supports:

- Multicast
- HTTP Web-based configuration
  Provides an intuitive user interface for easy system configuration and verification of speaker operations.
- DHCP Client
  Dynamically assigns IP addresses in addition to the option to use static addressing.
- HTTP TCP Post auto-updating event notification in XML format
- TFTP Client
  Facilitates hosting for the configuration file for Autoprovisioning.
- Audio Encodings
  PCMU (G.711 µ-law)
  PCMA (G.711 a-law)
  G.729
## 1.5 Product Specifications

### Table 1-1. Product Specifications

<table>
<thead>
<tr>
<th>Category</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Output</td>
<td>802.3af - SPL 105 dB @ 1 meter</td>
</tr>
<tr>
<td>Operating Range</td>
<td>Temperature: -40° C to 55° C (-40° F to 131° F)</td>
</tr>
<tr>
<td></td>
<td>Humidity: 5-95%, non-condensing</td>
</tr>
<tr>
<td>Storage Temperature</td>
<td>-40° C to 70° C (-40° F to 158° F)</td>
</tr>
<tr>
<td>Storage Altitude</td>
<td>Up to 15,000 ft. (4573 m)</td>
</tr>
<tr>
<td>Ethernet I/F</td>
<td>10/100 Mbps</td>
</tr>
<tr>
<td>Protocol</td>
<td>Multicast</td>
</tr>
<tr>
<td>Power Input</td>
<td>PoE 802.3af</td>
</tr>
<tr>
<td>Payload types</td>
<td>G.711 a-law, G.711µ-law, and G.729</td>
</tr>
<tr>
<td>Warranty</td>
<td>2 years limited</td>
</tr>
<tr>
<td>Dimensions</td>
<td>9 in. [228.6 mm] x 2.4 in. [60.96 mm]</td>
</tr>
<tr>
<td>Boxed Weight</td>
<td>4.0 lbs.</td>
</tr>
<tr>
<td>Compliance</td>
<td>CE; EMC Directive - Class A EN 55032 &amp; EN 55024, LV Safety Directive- EN 60950-1, RoHS Compliant, FCC; Part 15 Class A, Industry Canada; ICES-3 Class A, IEEE 802.3 Compliant</td>
</tr>
<tr>
<td>Part number</td>
<td>011458</td>
</tr>
</tbody>
</table>

## 1.6 Compliance

### 1.6.1 CE Testing

CE testing has been performed according to EN ISO/IEC 17050 for Emissions, Immunity, and Safety.

**Note** You can download the Declaration of Conformity document from the Downloads tab of the product’s webpage.

### 1.6.2 FCC Statement

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

2.1 Parts List

Table 2-1 illustrates the parts for each speaker and includes kits for the drop ceiling and drywall mounting.

**Note**  The installation template for the Multicast Speaker is located on the *Installation Quick Reference Guide* that is included in the packaging with each speaker.

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Part Name</th>
<th>Illustration</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Multicast Speaker Assembly</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Installation Quick Reference Guide</td>
<td></td>
</tr>
</tbody>
</table>

Table 2-1. Parts
2.2 Device Configuration

Set up and configure each speaker before you mount it.

CyberData delivers each speaker with the following factory default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addressing</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP Address&lt;sup&gt;a&lt;/sup&gt;</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Web Access Username</td>
<td>admin</td>
</tr>
<tr>
<td>Web Access Password</td>
<td>admin</td>
</tr>
<tr>
<td>Subnet Mask&lt;sup&gt;a&lt;/sup&gt;</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>Default Gateway&lt;sup&gt;a&lt;/sup&gt;</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

<sup>a</sup> Default if there is not a DHCP server present.
2.2.1 Connect Power to the Speaker

Figure 2-1 through Figure 2-2 illustrates how to connect power to the Multicast Speaker.

2.2.1.1 Multicast Speaker to a 802.3af Compliant PoE Switch

Figure 2-1 illustrates how to connect the Multicast Speaker to a 802.3af compliant PoE switch via a Cat 5 Ethernet cable.

Figure 2-1. Multicast Speaker to a 802.3af Compliant PoE Switch

2.2.1.2 Multicast Speaker (with PoE Injector) to a 802.3af Compliant PoE Switch

In Figure 2-2, if a PoE switch is not available, you will need a PoE Injector, part #010867A (ordered separately). A PoE Injector is a power supply solution for those who have a standard Non PoE Switch.

Figure 2-2. Multicast Speaker (with PoE Injector) to a Non PoE Switch
2.2.2 Confirm that the Speaker is Operational and Linked to the Network

After connecting the speaker to the 802.3af compliant Ethernet hub, the LEDs on the speaker face confirm that the speaker is operational and linked to the network.

**Figure 2-3. Status and Activity LEDs**


2.2.2.1 Link/Activity LED

After supplying power to the speaker:

1. The green Link/Activity LED comes on immediately to show that there is a good network connection, and then blinks to show network activity.

2. After about 23 seconds with a static IP address (or 27 seconds if the board is set to use DHCP), the speaker should be ready.

**Note**  If the board is set to use DHCP and there is not a DHCP server available on the network, it will try 12 times with a three second delay between tries and eventually fall back to the programmed static IP address (by default 10.10.10.10). This process will take approximately 80 seconds.

2.2.2.2 100 Mb LED

- The yellow **100 Mb** LED is illuminated when the network 100 Mb link to the speaker is established.
2.2.3 Confirm the IP Address and Test the Audio

2.2.3.1 Reset Test Function Management (RTFM) Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-4) on the speaker face to announce and confirm the speaker's IP Address and test that the audio is working.

**Figure 2-4. RTFM Button**

To announce a speaker's current IP address, use an instrument through the hole to press and release the RTFM button within a five second window.

**Note**  The speaker 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).

**Note**  Pressing and holding the RTFM button for longer than five seconds will restore the speaker to the factory default settings.
2.2.4 How to Set the Factory Default Settings

2.2.4.1 RTFM Button

When the speaker is operational and linked to the network, use the Reset Test Function Management (RTFM) button (Figure 2-5) on the speaker face to set the factory default settings.

Figure 2-5. RTFM Button

To set the factory default settings:

1. Press and hold the **RTFM** button for more than five seconds.

2. The speaker announces that it is restoring the factory default settings.

*Note* The speaker 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).
2.3 Configure the Multicast Speaker Parameters

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

Configure each Multicast Speaker and verify its operation before you mount it. When you are ready to mount a Multicast Speaker, refer to Appendix A, "Mounting the Speaker" for instructions.

2.3.1 Factory Default Settings

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

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

Table 2-3. Factory Default Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Factory Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addressing</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP Addressa</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Web Access Username</td>
<td>admin</td>
</tr>
<tr>
<td>Web Access Password</td>
<td>admin</td>
</tr>
<tr>
<td>Subnet Maska</td>
<td>255.0.0.0</td>
</tr>
<tr>
<td>Default Gatewaya</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

a. Default if there is not a DHCP server present.
### 2.3.2 Multicast Speaker Web Page Navigation

Table 2-4 shows the navigation buttons that you will see on every Multicast Speaker web page.

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>Link to the <strong>Home</strong> page.</td>
</tr>
<tr>
<td>Device</td>
<td>Link to the <strong>Device</strong> page.</td>
</tr>
<tr>
<td>Network</td>
<td>Link to the <strong>Network</strong> page.</td>
</tr>
<tr>
<td>SSL</td>
<td>Link to the <strong>SSL</strong> page.</td>
</tr>
<tr>
<td>Multicast</td>
<td>Link to the <strong>Multicast</strong> page.</td>
</tr>
<tr>
<td>Audiofiles</td>
<td>Link to the <strong>Audiofiles</strong> page.</td>
</tr>
<tr>
<td>Events</td>
<td>Link to the <strong>Events</strong> page.</td>
</tr>
<tr>
<td>Autoprovisioning</td>
<td>Link to the <strong>Autoprovisioning</strong> page.</td>
</tr>
<tr>
<td>Firmware</td>
<td>Link to the <strong>Firmware</strong> page.</td>
</tr>
</tbody>
</table>
2.3.3 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**

   ![Toggle Help Button](image)

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**

   ![Question Marks on Network Settings](image)
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**
2.3.4 Log in to the Configuration Home Page

1. Open your browser to the Multicast Speaker 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 Speaker.

**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:

https://www.cyberdata.net/pages/discovery

**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

CyberData Multicast Speaker

Current Status
- Serial Number: 458000001
- Mac Address: 00:20:70:ee:56:94
- Firmware Version: v1.0.0
- Partition 2: v1.0.0
- Booting From: partition 2
- IP Addressing: DHCP
- IP Address: 10.10.1.91
- Subnet Mask: 255.0.0.0
- Default Gateway: 10.0.0.1
- DNS Server 1: 10.0.1.56
- DNS Server 2: 
- Multicast Volume: 4
- Event Reporting: Disabled

Admin Settings
- Username: admin
- Password: 
- Confirm Password: 

Import Settings
- Browse...
- No file chosen
- Import Config

Export Settings
- Export Config

Save Reboot Toggle Help
3. On the **Home** page, review the setup details and navigation buttons described in Table 2-5.

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

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Username ?</td>
<td>The username to access the web interface. Enter up to 25 characters.</td>
</tr>
<tr>
<td>Password ?</td>
<td>The password to access the web interface. Enter up to 25 characters.</td>
</tr>
<tr>
<td>Confirm Password ?</td>
<td>Confirm the web interface password.</td>
</tr>
<tr>
<td><strong>Current Status</strong></td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>Shows the device serial number.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>Shows the device Mac address.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Shows the current firmware version.</td>
</tr>
<tr>
<td>Partition 2</td>
<td>Contains a complete copy of bootable software.</td>
</tr>
<tr>
<td>Partition 3</td>
<td>Contains an alternate, complete copy of bootable software.</td>
</tr>
<tr>
<td>Booting From</td>
<td>Indicates the partition currently used for boot.</td>
</tr>
<tr>
<td><strong>Boot From Other Partition</strong></td>
<td>Allows the user to boot from the alternate partition.</td>
</tr>
<tr>
<td>IP Addressing</td>
<td>Shows the current IP addressing setting (<strong>DHCP</strong> or <strong>static</strong>).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the current IP address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Shows the current subnet mask address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Shows the current default gateway address.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Shows the current DNS Server 1 address.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Shows the current DNS Server 2 address.</td>
</tr>
<tr>
<td>Multicast Volume</td>
<td>Shows the current Multicast volume level.</td>
</tr>
<tr>
<td>Event Reporting</td>
<td>Shows the current status of the Event Reporting mode.</td>
</tr>
<tr>
<td><strong>Import Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Browse...</strong></td>
<td>Use this button to select a configuration file to import.</td>
</tr>
<tr>
<td><strong>Import Config</strong></td>
<td>After selecting a configuration file, click Import to import the configuration from the selected file. Then, click Save and Reboot to store changes.</td>
</tr>
<tr>
<td><strong>Export Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Export Config</strong></td>
<td>Click Export to export the current configuration to a file.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>Click the <strong>Save</strong> button to save your configuration settings.</td>
</tr>
</tbody>
</table>
Table 2-5. Home Page Overview (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot</td>
<td>Click on the Reboot button to reboot the system.</td>
</tr>
<tr>
<td>Toggle Help</td>
<td>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 (<strong>Q</strong>) 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.</td>
</tr>
</tbody>
</table>
2.3.5 Configure the Device

1. Click the **Device** menu button to open the **Device** page. See *Figure 2-10*.

*Figure 2-10. Device Configuration Page*
2. On the **Device** page, you may enter values for the parameters indicated 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. Device Page Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Settings (0-9)</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Multicast Volume 2                | Set the speaker volume for multicast audio streams. A value of 0 will mute the speaker during multicasts.  
                                         **Note**: You can change this setting without rebooting the device. |
| **Clock Settings**                |                                                                             |
| Enable NTP 2                      | Sync device's local time with the specified NTP Server.                     |
| NTP Server 2                      | 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. |
| Timezone                          | Enter the tz database string of your timezone.                             |
|                                   | Examples:  
|                                   | America/Los_Angeles  
|                                   | America/New_Year  
|                                   | Europe/London  
|                                   | America/Toronto  
| Current Time                      | Displays the current time.                                                 |
| **Misc Settings**                 |                                                                             |
| Device Name 2                     | Type the device name. Enter up to 25 characters.                           |
| Disable HTTPS (NOT recommended) 2 | Disables the encrypted connection to the webpage. We do not recommend disabling HTTPS for security reasons. |
| **Test Audio**                    | Click on the **Test Audio** button to do an audio test. When the **Test Audio** button is pressed, you will hear a voice message for testing the device audio quality and volume. |
| **Save**                          | Click the **Save** button to save your configuration settings.              |
| **Reboot**                        | Click on the **Reboot** button to reboot the system.                       |
| **Toggle Help**                   | 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. |
2.3.6 Configure the Network Parameters

1. Click the **Network** menu button to open the **Network** page (Figure 2-11).

**Figure 2-11. Network Configuration Page**
2. On the **Network** page, 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. Network Configuration Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stored Network Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Addressing Mode</td>
<td>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 2.3.1, “Factory Default Settings” for factory default settings. Be sure to click <strong>Save</strong> and <strong>Reboot</strong> to store changes when configuring a Static address.</td>
</tr>
<tr>
<td>Hostname</td>
<td>This is the hostname provided by the DHCP server. See the DHCP/DNS server documentation for more information. Enter up to 64 characters.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the Static IPv4 network address in dotted decimal notation.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the Subnet Mask in dotted decimal notation.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the Default Gateway IPv4 address in dotted decimal notation.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Enter the primary DNS Server IPv4 address in dotted decimal notation.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Enter the secondary DNS Server IPv4 address in dotted decimal notation.</td>
</tr>
<tr>
<td><strong>Current Network Settings</strong></td>
<td>Shows the current network settings.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the current Static IP address.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Shows the current Subnet Mask address.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Shows the current Default Gateway address.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Shows the current DNS Server 1 address.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Shows the current DNS Server 2 address.</td>
</tr>
<tr>
<td><strong>VLAN Settings</strong></td>
<td></td>
</tr>
<tr>
<td>VLAN ID (0-4095)</td>
<td>Specify the IEEE 802.1Q VLAN ID number. Enter up to 4 digits. <strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>VLAN Priority (0-7)</td>
<td>Specify the IEEE 802.1p VLAN priority level. Enter 1 digit. A value of 0 may cause the VLAN ID tag to be ignored.</td>
</tr>
</tbody>
</table>

Click the **Save** button to save your configuration settings.

Click on the **Reboot** button to reboot the system.
Table 2-7. Network Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>You must click on the <strong>Save</strong> button and then the <strong>Reboot</strong> button for the changes to take effect.</td>
</tr>
<tr>
<td><strong>Toggle Help</strong></td>
<td>Click on the <strong>Toggle Help</strong> button to see a short description of some of the web page items. First click on the <strong>Toggle Help</strong> 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.</td>
</tr>
</tbody>
</table>
2.3.7 Configure the SSL Parameters

1. Click SSL menu button to open the SSL page (Figure 2-12).

Figure 2-12. SSL Configuration Page
Figure 2-13. SSL Configuration Page

<table>
<thead>
<tr>
<th>Certificate Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DigiCert_Trusted_Root_G4.crt</td>
</tr>
<tr>
<td>Equifax_Secure_CA.crt</td>
</tr>
<tr>
<td>Equifax_Secure_Global_eBusiness_CA.crt</td>
</tr>
<tr>
<td>Equifax_Secure_eBusiness_CA_1.crt</td>
</tr>
<tr>
<td>GeoTrust_Global_CA.crt</td>
</tr>
<tr>
<td>GeoTrust_Global_CA_2.crt</td>
</tr>
<tr>
<td>GeoTrust_Primary_Certification_Authority.crt</td>
</tr>
<tr>
<td>GeoTrust_Primary_Certification_Authority__G2.crt</td>
</tr>
<tr>
<td>GeoTrust_Primary_Certification_Authority__G3.crt</td>
</tr>
<tr>
<td>GeoTrust_Universal_CA.crt</td>
</tr>
<tr>
<td>GeoTrust_Universal_CA_2.crt</td>
</tr>
<tr>
<td>VeriSign_Class_3_Public_Primary_Certification_Authority__G4.crt</td>
</tr>
<tr>
<td>VeriSign_Class_3_Public_Primary_Certification_Authority__G5.crt</td>
</tr>
<tr>
<td>VeriSign_Universal_Root_Certification_Authority.crt</td>
</tr>
<tr>
<td>VeriSign_Class_1_Public_Primary_Certification_Authority.crt</td>
</tr>
<tr>
<td>VeriSign_Class_1_Public_Primary_Certification_Authority__G3.crt</td>
</tr>
<tr>
<td>VeriSign_Class_2_Public_Primary_Certification_Authority__G2.crt</td>
</tr>
<tr>
<td>VeriSign_Class_2_Public_Primary_Certification_Authority__G3.crt</td>
</tr>
<tr>
<td>VeriSign_Class_3_Public_Primary_Certification_Authority.crt</td>
</tr>
<tr>
<td>VeriSign_Class_3_Public_Primary_Certification_Authority__G3.crt</td>
</tr>
<tr>
<td>thawte_Primary_Root_CA.crt</td>
</tr>
<tr>
<td>thawte_Primary_Root_CA__G2.crt</td>
</tr>
<tr>
<td>thawte_Primary_Root_CA__G3.crt</td>
</tr>
</tbody>
</table>
2. On the **SSL** page, enter values for the parameters indicated in **Table 2-8**.

**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 2-8. SSL Configuration Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server CAs</strong></td>
<td>Use this button to select a configuration file to import.</td>
</tr>
<tr>
<td><img src="icon" alt="Browse..." /></td>
<td>Click <strong>Browse</strong> to select a CA certificate to import. After selecting a server certificate authority (CA), click <strong>Import CA Certificate</strong> to import it to the list of trusted CAs. CAs are used to validate the certificate presented by the server when establishing a TLS connection.</td>
</tr>
<tr>
<td><img src="icon" alt="Restore Defaults" /></td>
<td><strong>Restore Defaults</strong> will restore the default list of registered CAs and <strong>Remove All</strong> will remove all registered CAs.</td>
</tr>
<tr>
<td><img src="icon" alt="Remove All" /></td>
<td><strong>Restore Defaults</strong> will restore the default list of registered CAs and <strong>Remove All</strong> will remove all registered CAs.</td>
</tr>
<tr>
<td><strong>Client Certificate</strong></td>
<td>When doing mutual authentication this device will present a client certificate with these parameters.</td>
</tr>
<tr>
<td><img src="icon" alt="Client CA ?" /></td>
<td>Right click and <strong>Save Link As...</strong> to get the Cyberdata CA used to sign this client certificate.</td>
</tr>
<tr>
<td><strong>Test SSL Connection</strong></td>
<td>The ssl test server address as a fully qualified domain name or in IPv4 dotted decimal notation.</td>
</tr>
<tr>
<td><img src="icon" alt="Server ?" /></td>
<td>The ssl test server port. The supported range is 0-65536.</td>
</tr>
<tr>
<td><img src="icon" alt="Test TLS connection" /></td>
<td>Use this button to test a TLS connection to a remote server. This will attempt to make a socket connection to the configured test server and port and report the success or failure. This can be used to debug TLS connection issues.</td>
</tr>
<tr>
<td><strong>List of Trusted CAs</strong></td>
<td>Provides details of the certificate. After clicking on this button, the <strong>Certificate Info Window</strong> appears. See <strong>Section 2.3.7.1, &quot;Certificate Info Window&quot;</strong>.</td>
</tr>
<tr>
<td><img src="icon" alt="Info" /></td>
<td>Removes this certificate from the list of trusted certificates. After clicking on this button, the <strong>Remove Server Certificate Window</strong> appears. See <strong>Section 2.3.7.2, &quot;Remove Server Certificate Window&quot;</strong>.</td>
</tr>
</tbody>
</table>
2.3.7.1 Certificate Info Window

The Certificate Info Window provides details of the certificate. This window appears after clicking on the Info button. See Figure 2-14.

Figure 2-14. Certificate Info Window
2.3.7.2 Remove Server Certificate Window

The **Remove Server Certificate Window** will ask if the user wants to remove a certificate from the list of trusted certificates. This window appears after clicking on the **Remove** button. See Figure 2-15.

**Figure 2-15. Remove Server Certificate Window**
2.3.8 Configure the Multicast Parameters

The Multicast Configuration page allows the device to join up to ten paging zones for receiving ulaw/alaw encoded RTP audio streams.

A paging zone can consist of one or many CyberData multicast group-enabled products. There is no limit to how many speakers can be in a given paging zone. Each multicast group is defined by a multicast address and port number.

Each multicast group is assigned a priority, allowing simultaneously arriving pages to be serviced based on importance. Multicast groups are compatible with IGMP through version 3.

1. Click on the Multicast menu button to open the Multicast page. See Figure 2-16.

Figure 2-16. Multicast Configuration Page
2. On the **Multicast** page, enter values for the parameters indicated in Table 2-9.

**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>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Indicates the priority for the multicast group. Priority 9 is the highest (emergency streams). 0 is the lowest (background music).</td>
</tr>
<tr>
<td>Address</td>
<td>Enter the multicast IP Address for this multicast group (15 character limit).</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for this multicast group (5 character limit [range can be from 2000 to 65535]). <strong>Note:</strong> The multicast ports have to be even values. The webpage will enforce this restriction.</td>
</tr>
<tr>
<td>Name</td>
<td>Assign a descriptive name for this multicast group (25 character limit).</td>
</tr>
<tr>
<td>Beep</td>
<td>When selected, the device will play a beep before multicast audio is sent.</td>
</tr>
<tr>
<td>Polycom Default Channel</td>
<td>When a default Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <strong>Disabled</strong> to disable this channel.</td>
</tr>
<tr>
<td>Polycom Priority Channel</td>
<td>When a priority Polycom channel/group number is selected, the device will subscribe to the priority channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <strong>Disabled</strong> to disable this channel.</td>
</tr>
<tr>
<td>Polycom Emergency Channel</td>
<td>When an emergency Polycom channel/group number is selected, the device will subscribe to the default channel for one-way group pages. Group Numbers 1-25 are supported. Or, select <strong>Disabled</strong> to disable this channel.</td>
</tr>
</tbody>
</table>

Click the **Save** button to save your configuration settings.

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.
2.3.9 Configure the Audio Configuration Parameters

The **Audiofiles** page is used to add custom audio to the board. User uploaded audio will take precedence over the audio files shipped with the device.

1. Click on the **Audiofiles** menu button to open the **Audiofiles** page (Figure 2-17).

**Figure 2-17. Audiofiles Page**

![CyberData Multicast Speaker](image)

- **Available Space:** 1485MB
- **Currently set to:**
  - **Browse:** No file chosen
  - **Play**
  - **Delete**
  - **Save**

0:
1:
2:
3:
4:
5:
6:
7:
8:
9:
Dot:

**Audio Test:**

**Your IP Address:**

**Rebooting:**

**Restoring Default:**

No file chosen
Play
Delete
Save

No file chosen
Play
Delete
Save

No file chosen
Play
Delete
Save

No file chosen
Play
Delete
Save

No file chosen
Play
Delete
Save

No file chosen
Play
Delete
Save

No file chosen
Play
Delete
Save
2. On the **Audiofiles** page, enter values for the parameters indicated in **Table 2-10**.

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

**Table 2-10. Audiofiles Page Parameters**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Space</td>
<td>Shows the space available for the user to save custom audio files if they want to change the message when the door or sensor is triggered.</td>
</tr>
<tr>
<td><strong>Audio Files</strong></td>
<td></td>
</tr>
<tr>
<td>0-9</td>
<td>The name of the audio configuration option is the same as the spoken audio that plays on the board (24 character limit).</td>
</tr>
<tr>
<td></td>
<td>‘0’ corresponds to the spoken word “zero.”</td>
</tr>
<tr>
<td></td>
<td>‘1’ corresponds to the spoken word “one.”</td>
</tr>
<tr>
<td></td>
<td>‘2’ corresponds to the spoken word “two.”</td>
</tr>
<tr>
<td></td>
<td>‘3’ corresponds to the spoken word “three.”</td>
</tr>
<tr>
<td></td>
<td>‘4’ corresponds to the spoken word “four.”</td>
</tr>
<tr>
<td>Dot</td>
<td>Corresponds to the spoken word “dot.” (24 character limit)</td>
</tr>
<tr>
<td><strong>Audio Test</strong></td>
<td>Corresponds to the message “<strong>This is the CyberData IP speaker test message...</strong>” (24 character limit)</td>
</tr>
<tr>
<td>Your IP Address is</td>
<td>Corresponds to the message “Your IP address is...” (24 character limit).</td>
</tr>
<tr>
<td>Rebooting</td>
<td>Corresponds to the spoken word “Rebooting” (24 character limit).</td>
</tr>
<tr>
<td>Restoring Default</td>
<td>Corresponds to the message “Restoring default” (24 character limit).</td>
</tr>
<tr>
<td><strong>Browse</strong></td>
<td>Click on the <strong>Browse</strong> button to navigate to and select an audio file.</td>
</tr>
<tr>
<td><strong>Play</strong></td>
<td>The <strong>Play</strong> button will play that audio file.</td>
</tr>
<tr>
<td><strong>Delete</strong></td>
<td>The <strong>Delete</strong> button will delete any user uploaded audio and restore the stock audio file.</td>
</tr>
<tr>
<td><strong>Save</strong></td>
<td>The <strong>Save</strong> button will download a new user audio file to the board once you've selected the file by using the <strong>Browse</strong> button. The <strong>Save</strong> button will delete any pre-existing user-uploaded audio files.</td>
</tr>
</tbody>
</table>
2.3.9.1 User-created Audio Files

User created audio files should be saved in the following format:

RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, mono 8000 Hz

You can use the free utility Audacity to convert audio files into this format. See Figure 2-18 through Figure 2-20.

**Figure 2-18. Audacity 1**

[Image of Audacity interface]

**Figure 2-19. Audacity 2**

[Image of Audacity interface with metadata editor]
When you export an audio file with Audacity, save the output as:

- WAV (Microsoft) signed 16 bit PCM.

Figure 2-20. WAV (Microsoft) signed 16 bit PCM
2.3.10 Configure the Events Parameters

The **Events** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

1. Click on the **Events** menu button to open the **Events** page (Figure 2-21).

*Figure 2-21. Event Configuration Page*
2. On the **Events** page, enter values for the parameters indicated in Table 2-11.

**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>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Event Generation</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Events**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Multicast Start Events</td>
<td>When selected, the device will report when the device starts playing a multicast audio stream.</td>
</tr>
<tr>
<td>Enable Multicast Stop Events</td>
<td>When selected, the device will report when the device stops playing a multicast audio stream.</td>
</tr>
<tr>
<td>Enable Power On Events</td>
<td>When selected, the device will report when it boots.</td>
</tr>
<tr>
<td>Enable 60 Second Heartbeat</td>
<td>When enabled, the device will report a Heartbeat event every 60 seconds. SIP registration is not required to generate Heartbeat events.</td>
</tr>
</tbody>
</table>

**Event Server**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server IP Address</td>
<td>The IPv4 address of the event server in dotted decimal notation.</td>
</tr>
<tr>
<td>Server Port</td>
<td>Specify the event server port number. The supported range is 0-65536. Enter up to 5 digits.</td>
</tr>
<tr>
<td>Server URL</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Save**

Click the **Save** button to save your configuration settings.

**Reboot**

Click on the **Reboot** button to reboot the system.

**Toggle Help**

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.
2.3.10.1 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 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 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 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 Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
Installing the Multicast Speaker

Device Configuration

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 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 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 Device' MAC='0020f70015b6'>
<event>MULTICAST_START</event>
<index>8</index>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 233
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</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 Device' MAC='0020f70015b6'>
<event>MULTICAST_STOP</event>
<index>8</index>
</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 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 Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
Installing the Multicast Speaker

Device Configuration

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 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 Device' MAC='0020f70015b6'>
  <event>NIGHTRINGING</event>
</cyberdata>
2.3.11 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 2-22.

**Figure 2-22. Autoprovisioning Page**
2. On the **Autoprovisioning** page, you may enter values for the parameters indicated in **Table 2-12**.

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

### Table 2-12. Autoprovisioning Page Parameters

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Autoprovisioning</td>
<td>The device will automatically fetch a configuration file, also known as the 'autoprovisioning file', based on the configured settings below.</td>
</tr>
<tr>
<td>Autoprovisioning Server</td>
<td>Enter the IPv4 address of the provisioning server in dotted decimal notation.</td>
</tr>
<tr>
<td>Autoprovisioning Filename</td>
<td>The autoprovisioning filename is the configuration filename. The default autoprovisioning filename is in the format of <code>&lt;mac address&gt;.xml</code>. Supported filename extensions are .txt, and .xml. The current filename is denoted by an asterisk at the bottom of the <strong>Autoprovisioning Page</strong>. Enter up to 256 characters. 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.</td>
</tr>
<tr>
<td>Use tftp</td>
<td>The device will use TFTP (instead of http) to download autoprovisioning files.</td>
</tr>
<tr>
<td>Verify Server Certificate</td>
<td>When using ssl to download autoprovisioning files, reject connections where the server address doesn't match the server certificate's common name.</td>
</tr>
<tr>
<td>Username</td>
<td>The username used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>The password used to authenticate with an autoprovisioning server. Leave this field blank to disable authentication.</td>
</tr>
<tr>
<td>Autoprovisioning Autoupdate</td>
<td>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.</td>
</tr>
<tr>
<td>Autoprov at time (HHMMSS)</td>
<td>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.</td>
</tr>
<tr>
<td>Autoprov when idle</td>
<td>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.</td>
</tr>
</tbody>
</table>

Click the **Save** button to save your configuration settings.

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 (替补) 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 2.3.11.3, "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 for the changes to take effect.

2.3.11.1 Autoproposing

On boot, the device will look for an autoproposing server configured on the Autoproposing 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 autoproposing page.
2. A file named according to its 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 autoproposing server from the DHCP options. See Section 2.3.11.2, "Sample dhcpd.conf" for an example of how to configure dhcpd to offer autoproposing server addresses. If multiple options are set, the device will attempt to download autoproposing files from every server.

The DHCP option determines the protocol used to download the autoproposing 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 autoproposing template file from the Autoproposing Page using the Download Template button (see Table 2-12). This file contains every configuration option that can be set on the board.

Autoproposing files can contain the whole configuration or a subset of this file. The first autoproposing file can also contain links to other autoproposing files.

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

```xml
<DeviceName>CyberData VoIP Device</DeviceName>
<AutoprovFile>common.xml</AutoprovFile>
<AutoprovFile>sip_reg[macaddress].xml</AutoprovFile>
<AutoprovFile>audio[macaddress].xml</AutoprovFile>
<AutoprovFile>device[macaddress].xml</AutoprovFile>
</MiscSettings>
```

After downloading the first autoproposing file, the device will step through up to twenty additional <AutoprovFile> 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
<?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].xml</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 can contain a file, a file path, or a directory.

<table>
<thead>
<tr>
<th>Autoprovisioning Filename</th>
<th>Autoprovisioning Server</th>
<th>File Downloaded</th>
</tr>
</thead>
<tbody>
<tr>
<td>config.xml</td>
<td>10.0.1.3</td>
<td>10.0.1.3/config.xml</td>
</tr>
<tr>
<td>/path/to/config.xml</td>
<td>10.0.1.3</td>
<td>10.0.1.3/path/to/config.xml</td>
</tr>
<tr>
<td>subdirectory/path/</td>
<td>10.0.1.3</td>
<td>10.0.1.3/subdirectory/path/0020f7020002.xml</td>
</tr>
</tbody>
</table>

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.
Autoprosioning
Firmware Updates

< FirmwareSettings >
< FirmwareFile > 505-uImage-ceilingspeaker </ 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 autoprosioning server.

The device will use the filename to determine when to autoprosion firmware updates. The default configuration is blank, so the first time you set a value in your autoprosioning 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-uImage-[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 autoprosioning 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 00:20:17:02:00:01 and 00:20:17:02:00:02 (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

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

sip_common.xml

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

sip_0020f7020001.xml

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

sip_0020f7020002.xml

```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://autoprovtest.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 autoprovisioning 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 autoprovisioning 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)

Audio Files

Audio files are stored in non-volatile memory and an autoprovisioned 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 autoprovisioning 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 autoprovisioning 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 page or by changing the autoprovisioning file with “default” set as the file name.
2.3.11.2 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; }

2.3.11.3 Download Template Button

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

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

1. On the Autoprovisioning page, click on the Download Template button.

2. You will see a window prompting you to save a configuration file (.xml) to a location on your computer (Figure 2-23). The configuration file is the basis for the default configuration settings for your unit).

3. Choose a location to save the configuration file and click on OK. See Figure 2-23.

4. At this point, you can open and edit the autoprovisioning template to change the configuration settings in the template for the unit.

5. You can then upload the autoprovisioning file to a TFTP or HTTP server where the file can be loaded onto other devices.
2.4 Upgrade the Firmware and Reboot the Multicast Speaker

2.4.1 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/products/011458/

2. Unzip the firmware version file. This file may contain the following:
   - Firmware file
   - Release notes

3. Log in to the Multicast Speaker home page as instructed in Section 2.3.4, "Log in to the Configuration Home Page".

4. Click on the Firmware menu button to open the Firmware page. See Figure 2-24.

   **Caution**
   
   **Equipment Hazard**: CyberData strongly recommends that you first reboot the device before attempting to upgrade the firmware of the device. See Section 2.4.2, “Reboot the Device”.

   
   **Figure 2-24. Firmware Page**

   
   CyberData Multicast Speaker

   Browse... No file chosen

   Upload Progress

   Upload Post Processing

   Status Messages
   
   Socket connected

5. Click on the Browse button, and then navigate to the location of the firmware file.
6. Select the firmware file. This reveals the **Upload** button *(Figure 2-25).*

![Figure 2-25. Upload Button](image)

7. Click on the **Upload** button. After selecting the **Upload** button, you will see the progress of the upload in the **Upload Progress** bar.

8. When the upload is complete, you will see the words **Upload finished** under **Status Messages**.

9. At this point, you will see the progress of the upload's post processing in the **Upload Post Processing** bar.

**Note**  Do not reboot the device before the upgrading process is complete.

10. When the process is complete, you will see the words **SWUPDATE Successful** under **Status Messages**.

11. The device will reboot automatically.

12. The **Home** page will display the version number of the firmware and indicate which boot partition is active.
Table 2-14 shows the web page items on the **Firmware** page.

**Table 2-14. Firmware Page Parameters**

<table>
<thead>
<tr>
<th>Web Page Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse...</td>
<td>Use the <strong>Browse</strong> button to navigate to the location of the Intercom firmware file that you want to upload.</td>
</tr>
</tbody>
</table>
| Upload              | Click on the **Upload** button to automatically upload the selected firmware and reboot the system.  
                      | **Note**: This button only appears after the user has selected a firmware file. |
| Upload progress     | Status bar indicates the progress in uploading the file.                    |
| Upload Post Processing | Status bar indicates the progress of the software installation.             |
| Status Messages     | Messages relevant to the firmware update process appear here.               |
2.4.2 Reboot the Device

To reboot a Multicast Speaker, log in to the web page as instructed in Section 2.3.4, "Log in to the Configuration Home Page".

1. Click on the Reboot button on the Home page (Figure 2-26). A normal restart will occur.

Figure 2-26. Home Page
2.5 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in Table 2-15 use the free unix utility, wget, but any program that can send http POST commands to the device should work.

2.5.1 Command Interface Post Commands

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

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Commanda</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place call to extension (example: extension 130)</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;call=130&quot;</td>
</tr>
<tr>
<td>Terminate active call</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;terminate=yes&quot;</td>
</tr>
<tr>
<td>Force reboot</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;reboot=yes&quot;</td>
</tr>
<tr>
<td>Test Audio button</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;test_audio=yes&quot;</td>
</tr>
<tr>
<td>Announce IP address</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/command.cgi">https://10.0.3.71/cgi-bin/command.cgi</a>&quot; --post-data &quot;speak_ip_address=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;0&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_0=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;1&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_1=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;2&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_2=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;3&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_3=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;4&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_4=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;5&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_5=yes&quot;</td>
</tr>
</tbody>
</table>
### Table 2-15. Command Interface Post Commands (continued)

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play the &quot;6&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_6=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;7&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_7=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;8&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_8=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;9&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_9=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;Dot&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_d=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;Audio Test&quot; audio file (from Audio Config)</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_audiotest=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;Your IP Address Is&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_youripaddressis=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;Rebooting&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_rebooting=yes&quot;</td>
</tr>
<tr>
<td>Play the &quot;Restoring Default&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;play_restoringdefault=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;0&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_0=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;1&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_1=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;2&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_2=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;3&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_3=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;4&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_4=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;5&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_5=yes&quot;</td>
</tr>
<tr>
<td>Delete the &quot;6&quot; audio file</td>
<td>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;<a href="https://10.0.3.71/cgi-bin/audiofiles.cgi">https://10.0.3.71/cgi-bin/audiofiles.cgi</a>&quot; --post-data &quot;delete_6=yes&quot;</td>
</tr>
</tbody>
</table>
### Table 2-15. Command Interface Post Commands (continued)

<table>
<thead>
<tr>
<th>Device Action</th>
<th>HTTP Post Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete the &quot;7&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_7=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;8&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_8=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;9&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_9=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Audio Test&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_audiotest=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Your IP Address Is&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_youripaddressis=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Rebooting&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_rebooting=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Restoring Default&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_restoringdefault=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Ringback tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_ringback=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Ring tone&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_ringtone=yes&quot;</code></td>
</tr>
<tr>
<td>Delete the &quot;Night Ring&quot; audio file</td>
<td><code>wget --user admin --password admin --auth-no-challenge --no-check-certificate --quiet -O /dev/null &quot;https://10.0.3.71/cgi-bin/audiofiles.cgi&quot; --post-data &quot;delete_nightring=yes&quot;</code></td>
</tr>
</tbody>
</table>

---

*a. Type and enter all of each http POST command on one line.*
Appendix A: Mounting the Speaker

A.1 Mounting

See Figure A-1 to mount the speaker.

Figure A-1. Mounting the Speaker

Remove the Speaker Grill out of the Speaker Housing:

1. Turn and line up at least two of the flag nuts with their channel.
2. Grasp the speaker grill with your index, middle, and ring fingers.
3. Place your thumb over the flag nut. At the same time, slowly push out the speaker grill.

Tools Required for Installation:

- (1) Sheetrock Saw or Drywall Cutter
- (1) #2 Phillips Screw Driver or Powered Screw Driver with #2 Phillips Hex Bit

To mount the speaker:

1. Loosen the Four (4) flag nuts with a #2 Phillip Screw Driver or Powered Screw Driver.
2. Use the TEMPLATE on the back of this document to cut a hole in the wall* or ceiling.
   *Skip the seismic tether mounting when mounting it to the wall.
3. Tighten the Four (4) flag nuts with a #2 Phillip Screw Driver or Powered Screw Driver.
4. Replace the speaker grill to the speaker housing.

Operations Guide 931532B CyberData Corporation
A.2 Dimensions

Figure A-2 shows the dimensions for the Multicast Speaker.

Dimensions are in Inches [Millimeter]

- Ø7.93 [Ø201.5]
- 0.35 [8.9]
- 3.52 [89.4]
A.3 Disassembling the Speaker

Figure A-3 shows how to disassemble the Multicast Speaker.

Figure A-3. Disassembling the Speaker

Disassemble the Speaker

- Flagnut & Screw (4 Places)
- JSPKR
- PCBA (4 Places)
- Network Connector Through Network Port Cutout
- Speaker Grill
- Speaker Frame & Flagnuts
- Mounting Screw (4 Places)
- Speaker Back Housing
- Seismic Tether Bracket
Appendix C: Setting up a TFTP Server

C.1 Set up a TFTP Server

C.1.1 Autoprovisioning requires a TFTP server for hosting the configuration file.

C.1.2 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

C.1.3 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:

https://www.cyberdata.net/pages/solarwinds

To set up a TFTP server on Windows:

1. Install and start the software.


3. Make a note of the default directory name, and then move the firmware files to be uploaded to that directory.
Appendix C: Troubleshooting/Technical Support

C.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/products/011458/

C.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/products/011458/
C.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

C.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
address, configuration login 16
adjusting volume 11
announcing a speaker’s IP address 10, 11
audio configuration 32
audio configuration page 32
audio files, user-created 34
audio output 5
audio test 10, 11
autoprovision at time (HHMMSS) 42
autoprovision when idle (in minutes > 10) 42
autoprovisioning 42, 43
   download template button 42
autoprovisioning autoupdate (in minutes) 42
autoprovisioning configuration 41, 42
autoprovisioning filename 42
autoprovisioning server (IP Address) 42

C
changing
   the web access password 20
command interface 56
commands 56
configurable parameters 21, 23
configuration
   audio 32
   default IP settings 12
   device 7
   door sensor 25
   intrusion sensor 25
   network 22
configuration home page 16
configuration page
   configurable parameters 21, 23
confirming IP address 10, 11
contact information 64
contact information for CyberData 64
current network settings 23
CyberData contact information 64

D
default
   gateway 7, 12
   IP address 7, 12
   subnet mask 7, 12
   username and password 7, 12
web login username and password 16
default gateway 7, 12, 23
default IP settings 12
default login address 16
device configuration 7, 20
   device configuration parameters 42
   the device configuration page 41
device configuration page 20
device configuration parameters 21
device configuration password
   changing for web configuration access 20
dimensions 5
discovery utility program 16
DNS server 23
download autoprovisioning template button 42

E
export settings 18

F
factory default settings
   how to set 11
features 3
firmware
   where to get the latest firmware 52

G
get autoprovisioning template 42

H
home page 16
http POST command 56

I
identifying your product 1
import settings 18
import/export settings 18
IP address 7, 12, 23
IP addressing
  default
    IP addressing setting 7, 12

L

Linux, setting up a TFTP server on 62
log in address 16

M

MGROUP
  MGROUP Name 31
multicast configuration 30, 32
Multicast IP Address 31

N

navigation (web page) 13
navigation table 13
network configuration 22
network link activity, verifying 9
Nightringer 51
NTP server 21

O

overview 1

P

password
  login 16
    restoring the default 7, 12
polycom default channel 31
polycom emergency channel 31
polycom priority channel 31
POST command 56
power input (J1) 5
power requirement 5
power, connecting to speaker 8
product
  parts list 6
product features 3
product overview 1
  product features 3
R
reboot 54, 55
Reset Test Function Management (RTFM) button 10, 11
restoring the factory default settings 11
RTFM button 10, 11

S
sales 64
sensor setup page 25
sensor setup parameters 25
service 64
subnet mask 7, 12, 23

T
tech support 64
technical support, contact information 64
testing audio 10, 11
TFTP server 62

U
username
  changing for web configuration access 20
  default for web configuration access 16
  restoring the default 7, 12

V
verifying
  network link and activity 9
  power on to speaker 9
VLAN ID 23
VLAN Priority 23
VLAN tagging support 23
VLAN tags 23
volume
  multicast volume 21
volume, adjusting 11
W

warranty policy at CyberData 64
web access password 7, 12
web access username 7, 12
web configuration log in address 16
web page
   navigation 13
web page navigation 13
weight 5
wget, free unix utility 56
Windows, setting up a TFTP server on 62