

# *SIP Strobe Operations Guide*

Part #011087

Document Part #930425J  
for Firmware Version 8.0.1

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

---

---

**SIP Strobe Operations Guide 930425J**  
**Part # 011087**

**COPYRIGHT NOTICE:**

© 2015, CyberData Corporation, ALL RIGHTS RESERVED.

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

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

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

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

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



Technical Support

The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:  
<http://support.cyberdata.net/>

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

Email: [support@cyberdata.net](mailto:support@cyberdata.net)

Fax: (831) 373-4193




Company and product information is at [www.cyberdata.net](http://www.cyberdata.net).

---

# Important Safety Instructions


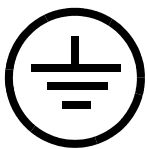
1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near 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 SIP Strobe enclosure is not rated for any AC voltages!**

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

---

## Pictorial Alert Icons

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

---

## Hazard Levels

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

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

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

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

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

---

# Abbreviations and Terms

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

---

# Revision Information

Revision 930425J, which corresponds to firmware version 8.0.1, was released on October 30, 2015 and has the following changes:

- Updates the following specifications in [Table 1-1, "Specifications"](#):
  - Power Input: PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply
  - Speaker Output: 1 Watt Peak Power
  - On-Board Relay: 1A at 30 VDC
  - Dimensions: 5.118 inches [130 mm] Length, 2.252 inches [57.21 mm] Width, 5.118 inches [130 mm] Height
  - Weight: 1.0 lbs. (0.45 kg)
  - Boxed Weight: 2.0 lbs. (0.90 kg)
- Updates [Figure 2-3, "SIP Strobe Connections"](#)

# Contents

---

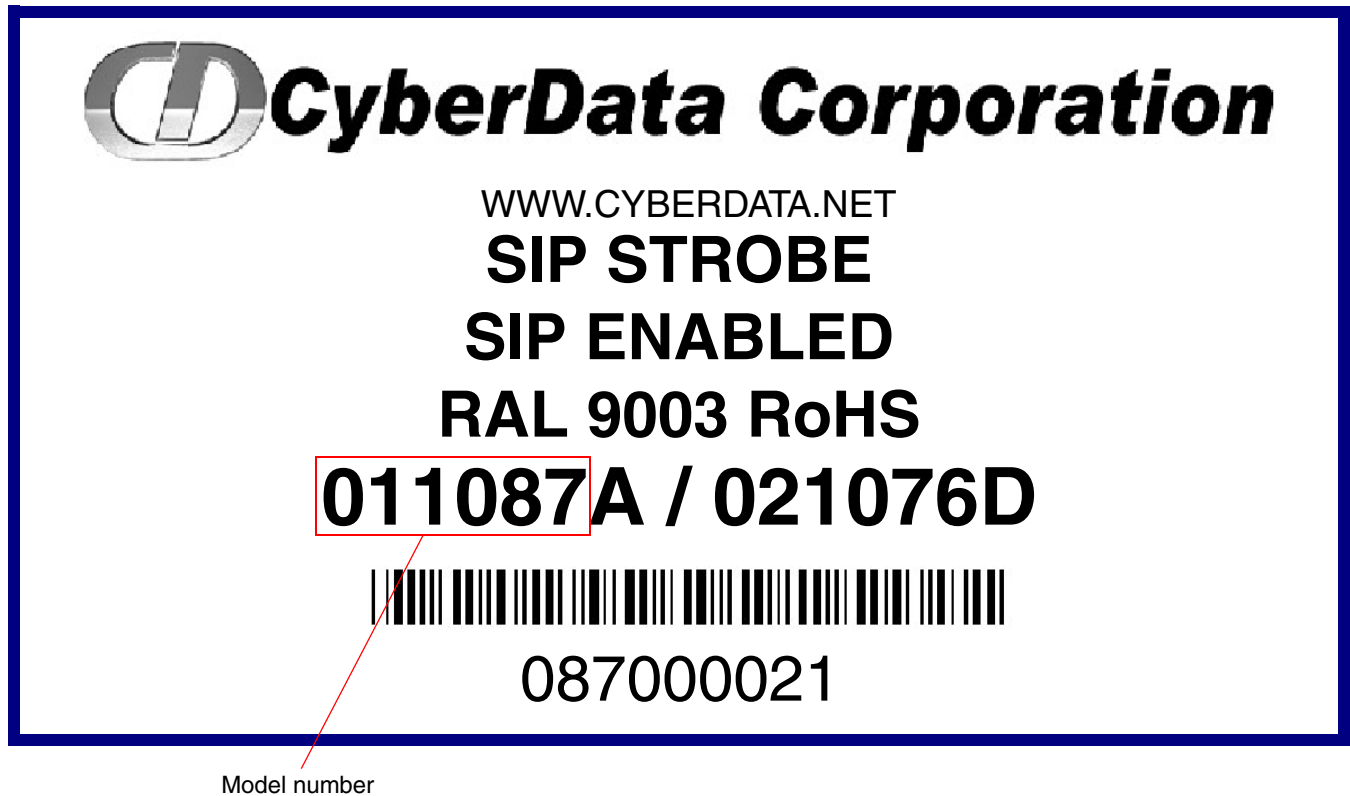
<b>Chapter 1 Product Overview</b>	<b>1</b>
1.1 How to Identify This Product .....	1
1.2 Typical System Installation .....	2
1.3 Product Features .....	3
1.4 Supported Protocols .....	3
1.5 Supported SIP Servers .....	3
1.6 Specifications .....	4
 <b>Chapter 2 Installing the SIP Strobe</b>	 <b>5</b>
2.1 Parts List .....	5
2.1 SIP Strobe Setup .....	6
2.1.1 SIP Strobe Connections .....	6
2.1.2 Connecting the SIP Strobe to the On-Board Relay .....	7
2.1.3 Identifying the SIP Strobe Connectors and Jumpers .....	9
2.1.4 Network Connectivity, and Data Rate .....	11
2.1.5 RTFM Switch .....	13
2.1.6 Restore the Factory Default Settings .....	14
2.2.1 SIP Strobe Web Page Navigation .....	16
2.2.2 Log in to the Configuration Home Page .....	17
2.2.3 Configure the Device .....	20
2.2.4 Configure the Network Parameters .....	22
2.2.5 Configure the SIP Parameters .....	24
2.2.6 Configure the Night Ringer Parameters .....	27
2.2.7 Configure the Sensor Configuration Parameters .....	29
2.2.8 Configure the Multicast Parameters .....	31
2.2.9 Configure the Event Parameters .....	33
2.2.10 Configure the Autoprovisioning Parameters .....	38
2.3.1 Reboot the SIP Strobe .....	45
2.4.1 Command Interface Post Commands .....	46
 <b>Appendix A Mounting the SIP Strobe</b>	 <b>47</b>
A.1 Important Safety Instructions .....	47
A.2 Mount the SIP Strobe .....	48
 <b>Appendix B Troubleshooting/Technical Support</b>	 <b>53</b>
B.1 Frequently Asked Questions (FAQ) .....	53
B.2 Documentation .....	53
B.3 Contact Information .....	54
B.4 Warranty and RMA Information .....	54
 <b>Index</b>	 <b>55</b>

# 1 Product Overview

## 1.1 How to Identify This Product

To identify the SIP Strobe, look for a model number label similar to the one shown in [Figure 1-1](#). The model number on the label should be **011087**.

Figure 1-1. Model Number Label



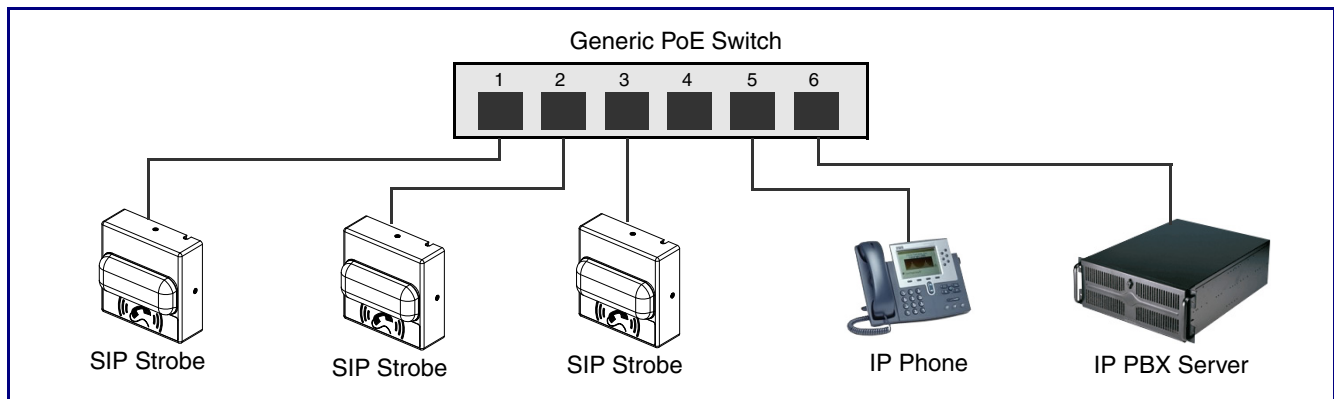


## 1.2 Typical System Installation

The Session Initiation Protocol (SIP) SIP Strobe is a SIP endpoint designed to provide VoIP phone connectivity in a tamper proof and secure package.

Figure 1-2 illustrate how the SIP Strobes can be installed as part of a VoIP phone system.

**Figure 1-2. Typical Installation**



### Warning

*Electrical Hazard:* The SIP Strobe enclosure is not rated for any AC voltages.



### Warning

*Electrical Hazard:* This product should be installed by a licensed electrician according to all local electrical and building codes.



### Warning

*Electrical Hazard:* To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.



### Warning

The PoE connector is intended for intra-building connections only and does not route to the outside plant.

---

## 1.3 Product Features

- Meets ADA requirements for telephony signaling and notification
- Program or listen to up to 10 multicast addresses
- SIP activation
- Mailbox message waiting indication
- Multicast activation
- Cisco SRST support
- Event-controlled relay

**Note:** The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.

- Tamper sensor
- Web-based setup
- PoE-powered

---

## 1.4 Supported Protocols

The SIP Strobe supports:

- SIP
- HTTP Web-based configuration

Provides an intuitive user interface for easy system configuration and verification of SIP Strobe operations.

- DHCP Client

Dynamically assigns IP addresses in addition to the option to use static addressing.

- RTP
- RTP/AVP - Audio Video Profile
- Audio Encodings

PCMU (G.711 mu-law)

PCMA (G.711 A-law)

Packet Time 20 ms

---

## 1.5 Supported SIP Servers

Go to the following link to find the SIP Strobe product page which will have information on how to configure the SIP Strobe for various supported SIP servers:

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

## 1.6 Specifications

**Table 1-1. Specifications**

Specifications	
Ethernet I/F	10/100 Mbps
Protocol	SIP RFC 3261 Compatible
Power Input	PoE 802.3af compliant or +8 to +12VDC @ 1000mA Regulated Power Supply <sup>a</sup>
Light power	Up to 90 candela (user-selectable)
Flash rate	5 user-defined scenes
LED MTBF	100,000 Hours
On-Board Relay	1A at 30 VDC
Operating Temperature	-10° C to 50° C (14° F to 122° F)
Payload Types	G711, A-law and $\mu$ -law
Dimensions	4.5 inches [115 mm] Length 2.1 inches [55 mm] Width 4.5 inches [115 mm] Height
Weight	1.0 lbs. (0.45 kg)
Boxed Weight	2.0 lbs. (0.90 kg)
Part Number	011087

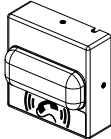


a. Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.

# 2 Installing the SIP Strobe

## 2.1 Parts List

Table 2-2 illustrates the SIP Strobe parts.

Table 2-2. Parts List

Quantity	Part Name	Illustration
1	SIP Strobe Assembly	
1	Installation Quick Reference Guide	
1	SIP Strobe Mounting Accessory Kit	

## 2.1 SIP Strobe Setup

### 2.1.1 SIP Strobe Connections

Figure 2-3 shows the pin connections on the J3 (terminal block). This terminal block can accept 16 AWG gauge wire.

**Note** As an alternative to using PoE power, you can supply +8 to +12VDC @ 1000mA Regulated Power Supply into the terminal block.


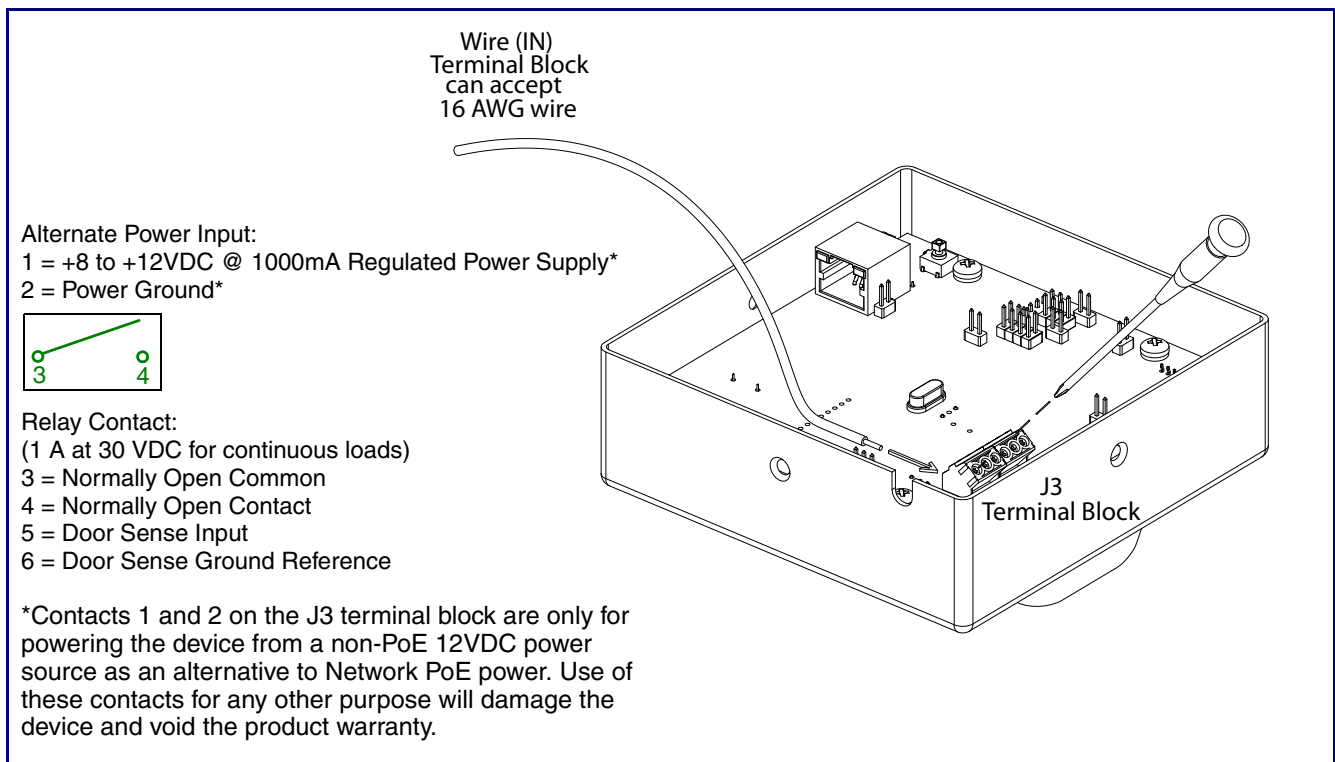





 GENERAL ALERT	<p><b>Caution</b></p> <p><i>Equipment Hazard:</i> Contacts 1 and 2 on the J3 terminal block are only for powering the device from a non-PoE 12 VDC power source as an alternative to Network PoE power. Use of these contacts for any other purpose will damage the device and void the product warranty.</p>
--	---

Figure 2-3. SIP Strobe Connections



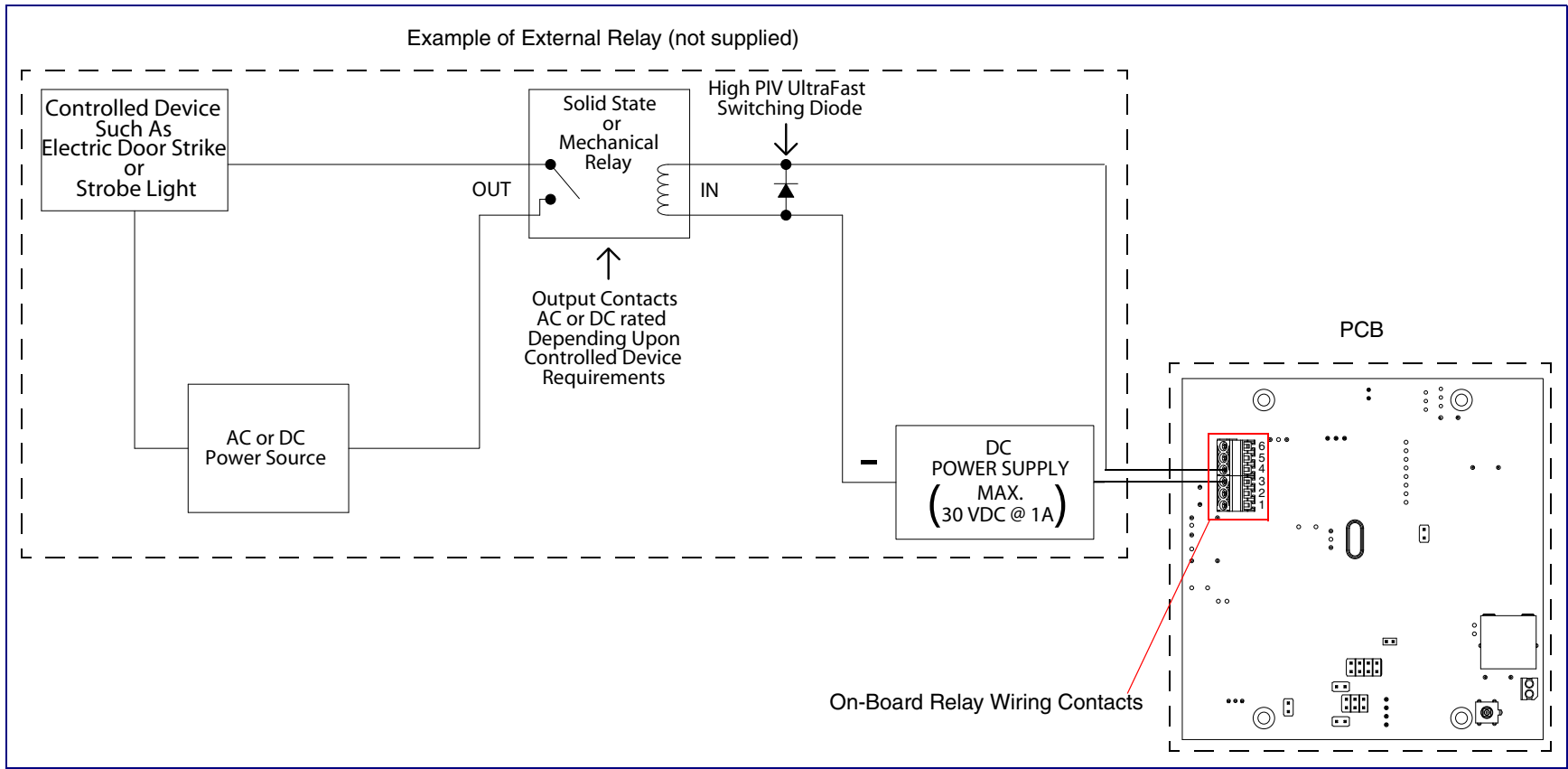
## 2.1.2 Connecting the SIP Strobe to the On-Board Relay

 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The SIP Strobe enclosure is not rated for any AC voltages.</p>
 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Electrical Hazard:</i> This product should be installed by a licensed electrician according to all local electrical and building codes.</p>
 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Electrical Hazard:</i> To prevent injury, this apparatus must be securely attached to the floor/wall in accordance with the installation instructions.</p>
 GENERAL ALERT	<p><b>Warning</b></p> <p><i>Electrical Hazard:</i> The relay contacts are dry and provided for a normally open and momentarily closed configuration. Neither the alternate power input nor PoE power can be used to drive a door strike.</p>
 GENERAL ALERT	<p><b>Warning</b></p> <p>The PoE connector is intended for intra-building connections only and does not route to the outside plant.</p>

The device incorporates an on-board relay which enables users to control an external relay for activating an auxiliary device such as an electric door strike (see [Figure 2-4, "Wiring Diagram"](#)).

The relay contacts are limited to 1A at 30 VDC. The relay activation time is selectable through the web interface and is controlled by DTMF tones generated from the phone being called. The DTMF tones are selectable from the web interface as well.

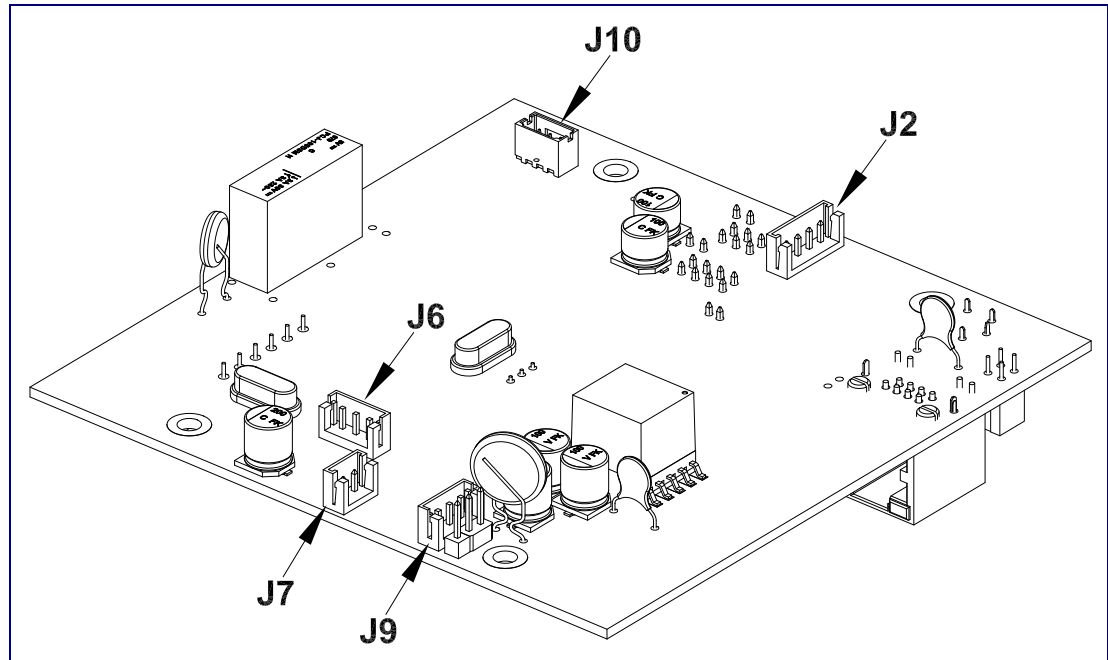
Figure 2-4. Wiring Diagram



### 2.1.3 Identifying the SIP Strobe Connectors and Jumpers

See the following figures and tables to identify the SIP Strobe connector locations and functions.

**Figure 2-5. Connector Locations**

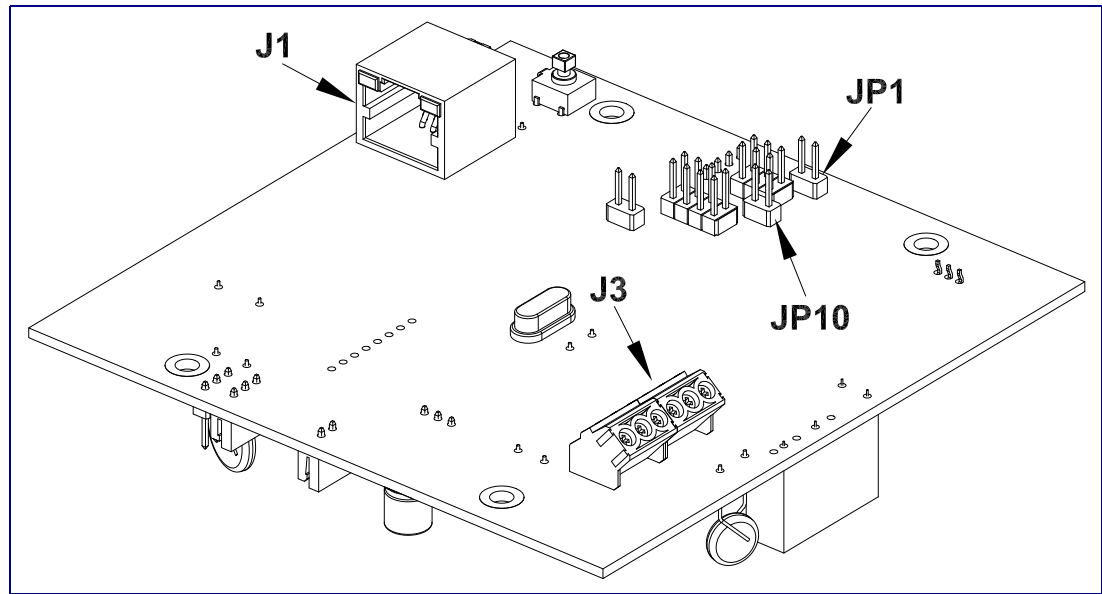


**Table 2-3. Connector Functions**

Connector	Function
J2	Call Button Interface — Not Used
J6	Microphone Interface — Not Used
J7	Speaker Interface — Not Used
J9	Strobe Power Interface
J10	Proximity Sensor Interface — Not Used



**Figure 2-6. Connector Locations**



**Table 2-4. Connector Functions**

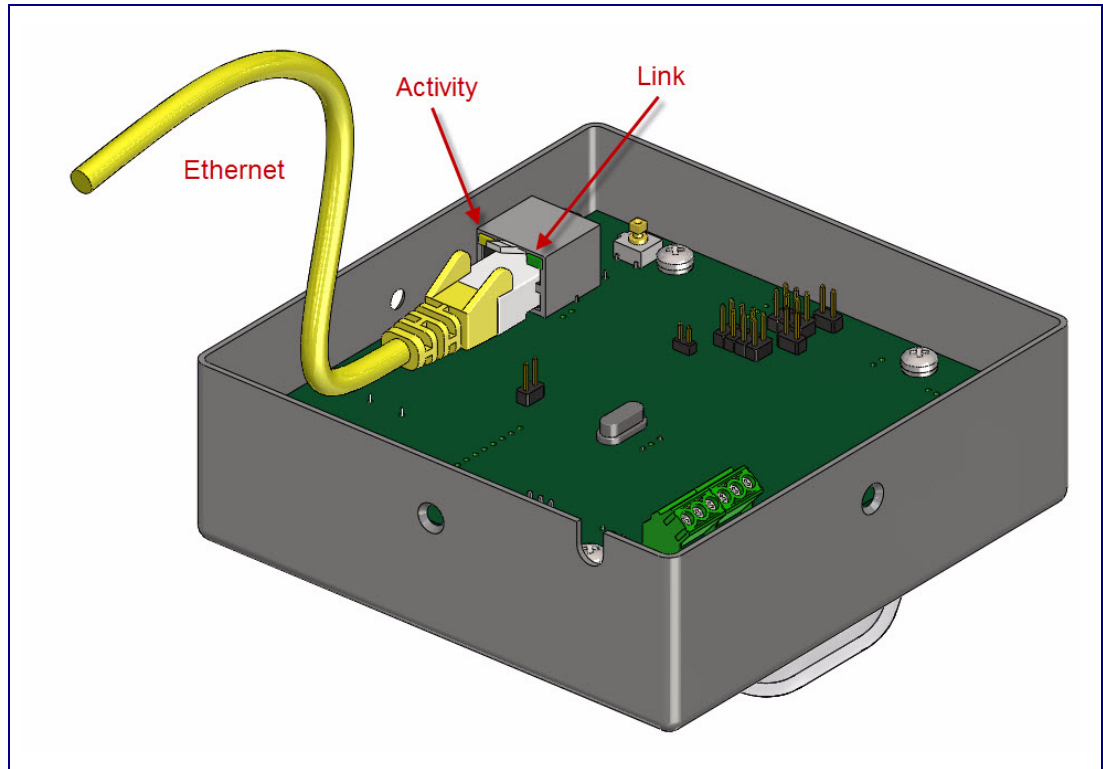
Connector	Function
J1	Ethernet Connector
J3	User Terminal Block Interface
JP1	Manual Reset — Factory only
JP10	Intrusion Sensor Disable. Place jumper on to disable.

## 2.1.4 Network Connectivity, and Data Rate

When you plug in the Ethernet cable or power supply:

- The square, green **Link** light above the Ethernet port indicates that the network connection has been established (see [Figure 2-7](#)).

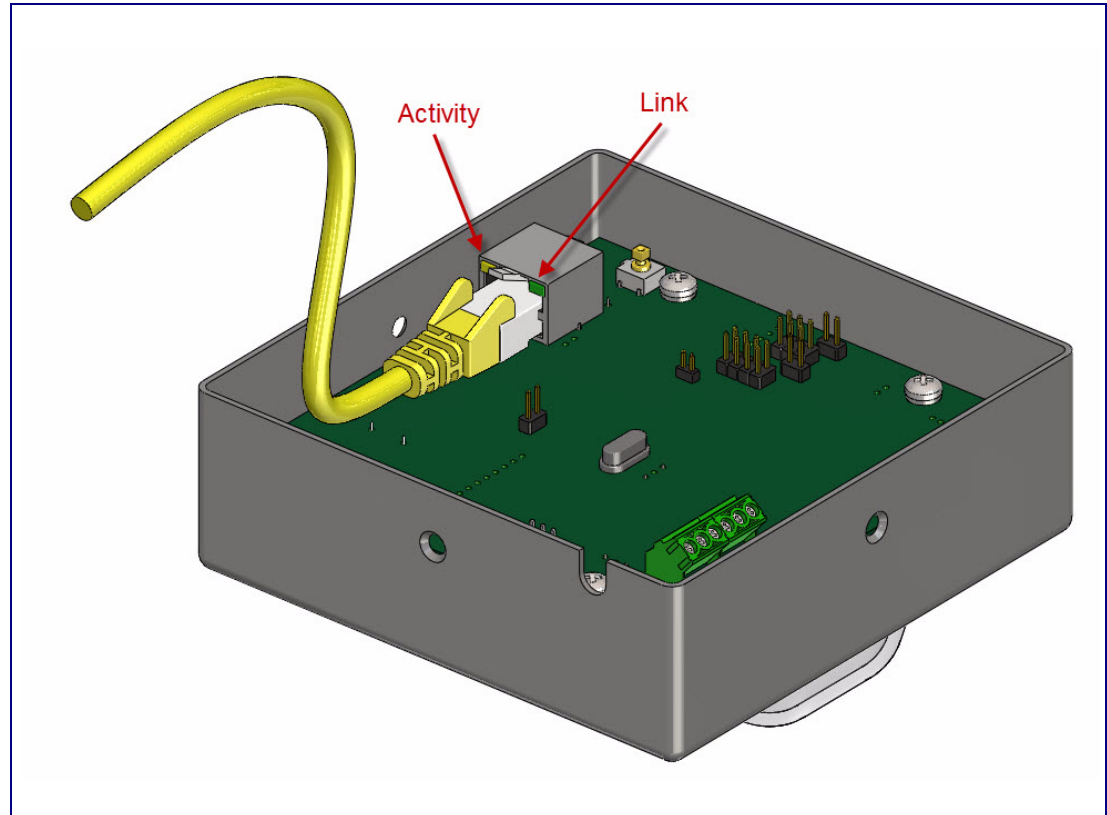
**Figure 2-7. Network Connector Prior to Installation**



### 2.1.4.1 Verify Network Activity

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

**Figure 2-8. Network Connector**

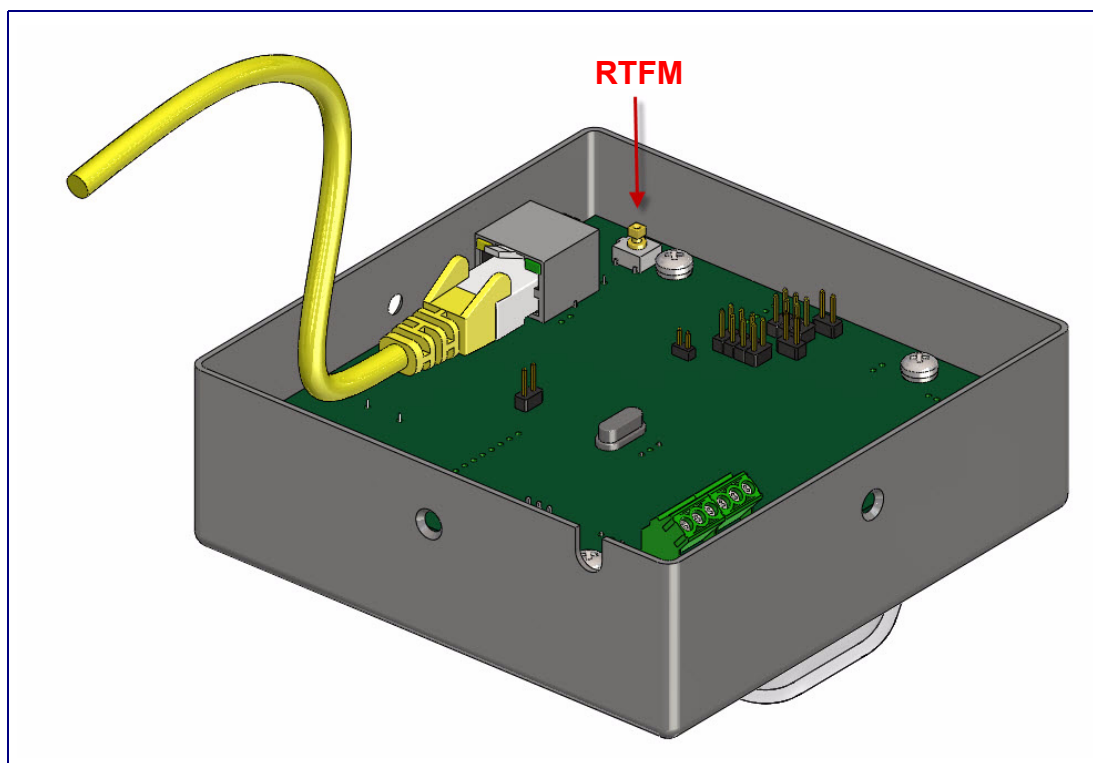


---

## 2.1.5 RTFM Switch

When the SIP Strobe is operational and linked to the network, use the Reset Test Function Management (**RTFM**) switch (Figure 2-9) on the SIP Strobe board to restore the unit to the factory default settings.

Figure 2-9. RTFM Switch



---

## 2.1.6 Restore the Factory Default Settings

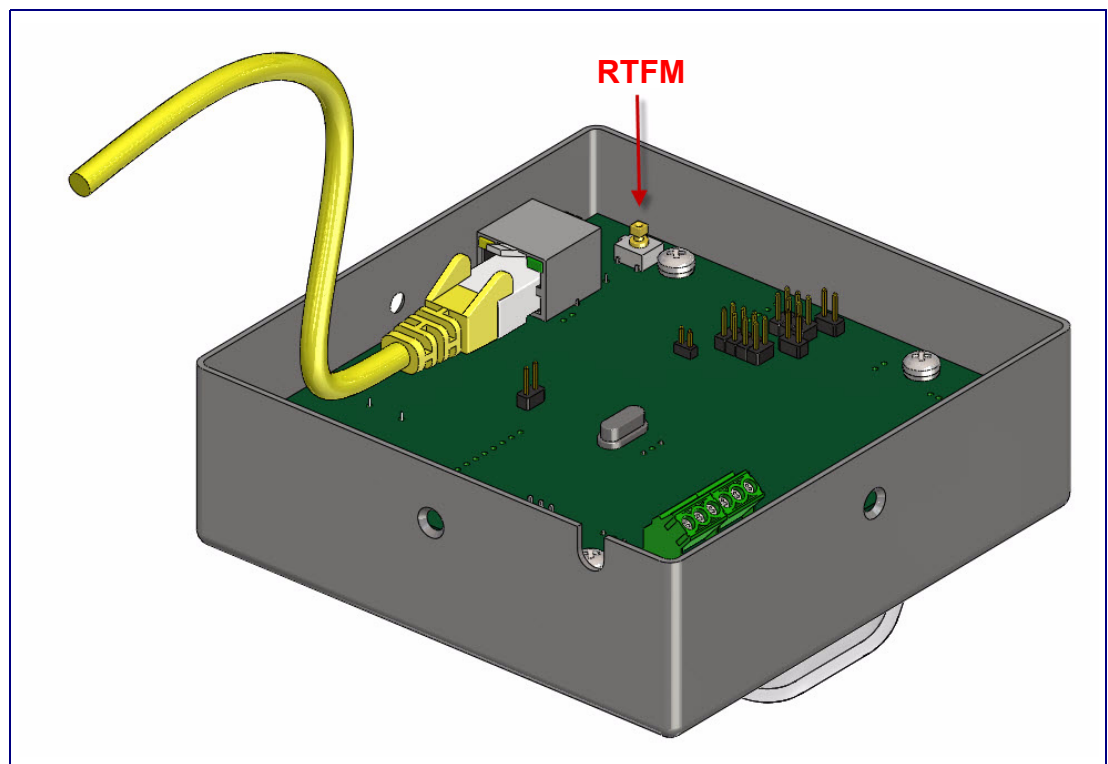
### 2.1.6.1 RTFM Switch

When the SIP Strobe is operational and linked to the network, use the Reset Test Function Management (RTFM) switch ([Figure 2-10](#)) to set the factory default settings.

**Note** Each SIP Strobe is delivered with factory set default values.

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

**Figure 2-10. RTFM Switch**



To set the factory default settings:

1. Press and hold the RTFM switch for seven seconds, and then release the RTFM switch.

---

## 2.2 Configure the SIP Strobe Parameters

To configure the SIP Strobe online, use a standard web browser.

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

All SIP Strobes are initially configured with the following default IP settings:

When configuring more than one SIP Strobe, attach the SIP Strobes to the network and configure one at a time to avoid IP address conflicts.

**Table 2-5. Factory Default Settings**

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











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

---

## 2.2.1 SIP Strobe Web Page Navigation

Table 2-6 shows the navigation buttons that you will see on every SIP Strobe web page.

**Table 2-6. Web Page Navigation**

Web Page Item	Description
	Link to the <b>Home</b> page.
	Link to the <b>Device Configuration</b> page.
	Link to the <b>Networking</b> page.
	Link to go to the <b>SIP Configuration</b> page.
	Link to go to the <b>Nightringer</b> page.
	Link to the <b>Sensor Configuration</b> page.
	Link to the <b>Multicast Configuration</b> page.
	Link to the <b>Event Configuration</b> page.
	Link to the <b>Autoprovisioning Configuration</b> page.
	Link to the <b>Update Firmware</b> page.

---

## 2.2.2 Log in to the Configuration Home Page

1. Open your browser to the SIP Strobe 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 SIP Strobe.

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

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

[http://www.cyberdata.net/support/voip/discovery\\_utility.html](http://www.cyberdata.net/support/voip/discovery_utility.html)

**Note** The SIP Strobe 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 2-11):

Web Access Username: **admin**

Web Access Password: **admin**

**Figure 2-11. Home Page**

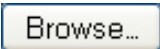
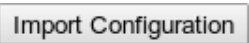
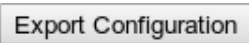
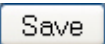
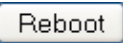
The screenshot displays the 'CyberData Strobe' web interface. On the left is a vertical menu with buttons for: Home, Device Config, Networking, SIP Config, Nightringer, Sensor Config, Multicast Config, Event Config, Autoprovisioning, and Update Firmware. The main content area is divided into three sections:

- Device Settings:** Includes fields for 'Device Name' (CyberData VoIP Strobe), 'Change Username' (admin), 'Change Password' (empty), and 'Re-enter Password' (empty).
- Current Settings:** Displays various system parameters:
  - Part Number: 011087
  - Serial Number: 087000011
  - Mac Address: 00:20:f7:00:e4:b7
  - Firmware Version: v8.0.1
  - IP Addressing: dhcp
  - IP Address: 192.168.70.20
  - Subnet Mask: 255.255.240.0
  - Default Gateway: 192.168.64.1
  - DNS Server 1: 192.168.65.20
  - DNS Server 2: 192.168.65.10
  - SIP Mode is: enabled
  - Multicast Mode is: disabled
  - Event Reporting is: disabled
  - Nightringer is: disabled (NOT Registered with SIP Server)
  - Primary SIP Server: (NOT Registered with SIP Server)
  - Backup Server 1: (NOT Registered with SIP Server)
  - Backup Server 2: (NOT Registered with SIP Server)
- Import/Export Settings:** Includes a text input for 'Please specify a configuration file:', a 'Browse...' button, an 'Import Configuration' button, and an 'Export Configuration' button.

At the bottom, a note states: '\* You need to reboot for changes to take effect'. Below this note are 'Save' and 'Reboot' buttons.

3. On the **Home Page**, review the setup details and navigation buttons described in [Table 2-7](#).

**Table 2-7. Home Page Overview**

Web Page Item	Description
<b>Device Settings</b>	
Device Name	Shows the device name.
Change Username	Type in this field to change the username.
Change Password	Type in this field to change the password.
Re-enter Password	Type the password again in this field to confirm the new password.
<b>Current Settings</b>	
Part Number	Shows the device 01 part number.
Serial Number	Shows the device serial number.
Mac Address	Shows the device Mac address.
Firmware Version	Shows the current firmware version.
IP Addressing	Shows the current IP addressing setting ( <b>DHCP</b> or <b>static</b> ).
IP Address	Shows the current IP address.
Subnet Mask	Shows the current subnet mask address.
Default Gateway	Shows the current default gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
SIP Mode is	Shows the current status of the SIP mode.
Multicast Mode is	Shows the current status of the Multicast mode.
Event Reporting is	Shows the current status of the Event Reporting mode.
Nightringer is	Shows the current status of the Nightringer mode.
Primary SIP Server	Shows the current status of the Primary SIP Server.
Backup Server 1	Shows the current status of Backup Server 1.
Backup Server 2	Shows the current status of Backup Server 2.
<b>Import/Export Settings</b>	
	Press the <b>Browse</b> button to select a configuration file to import.
	Press the <b>Import Configuration</b> button to save a board configuration to the board. <b>Note:</b> The board will have to be reset before changes will take effect.
	Press the <b>Export Configuration</b> button to download the current board configuration.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

## 2.2.3 Configure the Device

1. Click the **Device Configuration** button to open the **Device Configuration** page. See [Figure 2-12](#).

**Figure 2-12. Device Configuration Page**

**CyberData Strobe**

**Device Configuration**

Home  
Device Config  
Networking  
SIP Config  
Nightringer  
Sensor Config  
Multicast Config  
Event Config  
Autoprovisioning  
Update Firmware

**Relay Settings**

Activate Relay During Ring: ☐  
Activate Relay During Night Ring: ☐

**Miscellaneous Settings**

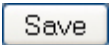


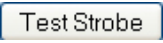
Blink Strobe On Ring: ☒  
Blink Strobe On Message Waiting (MWI): ☐

\* You need to reboot for changes to take effect

Save Reboot  
TestRelay TestStrobe

2. On the **Device Configuration** page, you may enter values for the parameters indicated in [Table 2-8](#).

**Table 2-8. Device Configuration Parameters**

Web Page Item	Description
<b>Relay Settings</b>	
Activate Relay During Ring	When selected, the relay will be activated for as long as the call is active.
Activate Relay During Night Ring	Check this box to activate the relay for as long as a Night Ring tone is ringing.
<b>Miscellaneous Settings</b>	
Blink Strobe on Ring	When selected, the strobe light will blink during an incoming call.
Blink Strobe on Message Waiting (MWI)	When selected, the strobe light will blink if there is a message waiting.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.
	Click on the <b>Test Relay</b> button to do a relay test.
	Click on the <b>Test Strobe</b> button to do a strobe test.

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

## 2.2.4 Configure the Network Parameters

1. Click the **Networking** button to open the **Network Configuration** page (Figure 2-13).

Figure 2-13. Network Configuration Page

**CyberData Strobe**

**Network Configuration**

Home  
Device Config  
**Networking**  
SIP Config  
Nightringer  
Sensor Config  
Multicast Config  
Event Config  
Autoprovisioning  
Update Firmware

**Stored Network Settings**

IP Addressing: ☐ Static ☒ DHCP

IP Address: 10.10.10.10

Subnet Mask: 255.0.0.0

Default Gateway: 10.0.0.1

DNS Server 1: 10.0.0.1

DNS Server 2: 10.0.0.1

**DHCP Timeout**

DHCP Timeout in seconds\*: 60

\* A value of -1 will retry forever

**Current Network Settings**

IP Address: 192.168.70.20

Subnet Mask: 255.255.240.0

Default Gateway: 192.168.64.1

DNS Server 1: 192.168.65.20


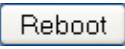
DNS Server 2: 192.168.65.10

\* You need to reboot for changes to take effect

Save Reboot

2. On the **Network Configuration** page, enter values for the parameters indicated in [Table 2-9](#).

**Table 2-9. Network Configuration Parameters**

Web Page Item	Description
IP Addressing	Select either <b>DHCP IP Addressing</b> or <b>Static IP Addressing</b> by marking the appropriate radio button. If you select <b>Static</b> , configure the remaining parameters indicated in <a href="#">Table 2-9</a> . If you select <b>DHCP</b> , go to <a href="#">Step 3</a> .
<b>Stored Network Settings</b>	
IP Address	Enter the Static IP address.
Subnet Mask	Enter the Subnet Mask address.
Default Gateway	Enter the Default Gateway address.
DNS Server 1	Enter the DNS Server 1 address.
DNS Server 2	Enter the DNS Server 2 address.
<b>DHCP Timeout</b>	
DHCP Timeout in seconds	Enter the desired timeout duration (in seconds) that the device will wait for a response from the DHCP server before defaulting back to the stored static IP address.  <b>Note:</b> A value of <b>-1</b> will cause the device to retry indefinitely and a value of <b>0</b> will cause the device to reset to a default of 60 seconds.
<b>Current Network Settings</b>	
IP Address	Shows the current Static IP address.
Subnet Mask	Shows the current Subnet Mask address.
Default Gateway	Shows the current Default Gateway address.
DNS Server 1	Shows the current DNS Server 1 address.
DNS Server 2	Shows the current DNS Server 2 address.
	Click the <b>Save</b> button to save your configuration settings.  <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

3. After changing the parameters, click **Save Settings**. This updates the changed parameters and reboots the SIP Strobe if appropriate.
4. Connect the SIP Strobe to the target network.
5. From a system on the same network as the SIP Strobe, open a browser with the new IP address of the SIP Strobe.

## 2.2.5 Configure the SIP Parameters

1. Click **SIP Config** to open the **SIP Configuration** page (Figure 2-14).

**Note** For specific server configurations, go to the following website address:

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

**Figure 2-14. SIP Configuration Page**

**CyberData Strobe**

**SIP Configuration**

Enable SIP operation: ☒

**SIP Settings**

Primary SIP Server (**NOT Registered**): 10.0.0.253  
Primary SIP User ID: 199  
Primary SIP Auth ID: 199  
Primary SIP Auth Password: ••••••

Backup SIP Server 1 (**NOT Registered**):  
Backup SIP User ID 1:  
Backup SIP Auth ID 1:  
Backup SIP Auth Password 1:

Backup SIP Server 2 (**NOT Registered**):  
Backup SIP User ID 2:  
Backup SIP Auth ID 2:  
Backup SIP Auth Password 2:

Use Cisco SRST: ☐

Remote SIP Port: 5060  
Local SIP Port: 5060  
Outbound Proxy:  
Outbound Proxy Port: 0

Register with a SIP Server: ☒  
Re-registration Interval (in seconds): 360  
NAT ping (check box if PBX is not local): ☐

**RTP Settings**

RTP Port (even): 10500

\* You need to reboot for changes to take effect

Save Reboot

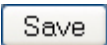
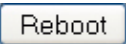
2. On the **SIP Configuration** page, enter values for the parameters indicated in [Table 2-10](#).

**Table 2-10. SIP Configuration Parameters**

Web Page Item	Description
Enable SIP Operation	Enables or disables SIP operation.
<b>SIP Settings</b>	
Primary SIP Server	Use this field to set the address (in dotted decimal notation or as a canonical name) for the Primary SIP Server. This field can accept canonical names of up to 255 characters in length.
Primary SIP User ID	Type the <b>SIP User ID</b> for the Primary SIP Server (up to 64 alphanumeric characters).
Primary Auth ID	Type the <b>Authenticate ID</b> for the Primary SIP Server (up to 64 alphanumeric characters).
Primary Auth Password	Type the <b>Authenticate Password</b> for the Primary SIP Server (up to 64 alphanumeric characters).
Backup SIP Server 1 Backup SIP Server 2	<ul style="list-style-type: none"> <li>If all of the <b>Primary SIP Server</b> and <b>Backup SIP Server</b> fields are populated, the device will attempt to stay registered with all three servers all of the time. You can leave the <b>Backup SIP Server 1</b> and <b>Backup SIP Server 2</b> fields blank if they are not needed.</li> <li>In the event of a registration failure on the <b>Primary SIP Server</b>, the device will use the next highest priority server for outbound calls (<b>Backup SIP Server 1</b>). If <b>Backup SIP Server 1</b> fails, the device will use <b>Backup SIP Server 2</b>.</li> <li>If a higher priority SIP Server comes back online, the device will switch back to this server.</li> </ul>
Backup SIP User ID 1 Backup SIP User ID 2	Type the <b>SIP User ID</b> for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth ID 1 Backup SIP Auth ID 2	Type the <b>SIP Authenticate ID</b> for the Backup SIP Server (up to 64 alphanumeric characters).
Backup SIP Auth Password 1 Backup SIP Auth Password 2	Type the <b>SIP Authenticate Password</b> for the Backup SIP Server (up to 64 alphanumeric characters).
Use Cisco SRST	When selected, the backup servers are handled according to Cisco SRST (Survivable Remote Site Telephony).
Remote SIP Port	Type the <b>Remote SIP Port</b> number (default 5060) (8 character limit).
Local SIP Port	Type the <b>Local SIP Port</b> number (default 5060) (8 character limit).
Outbound Proxy	Type the Outbound Proxy as either a numeric IP address in dotted decimal notation or the fully qualified host name (255 character limit [FQDN]).
Outbound Proxy Port	Type the Outbound Proxy Port number (8 character limit).
Register with a SIP Server	Check this box to enable SIP Registration.
Re-registration Interval (in seconds)	Type the SIP Registration lease time (in seconds)




**Table 2-10. SIP Configuration Parameters (continued)**

Web Page Item	Description
Re-registration Interval (in seconds)	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)
NAT ping (check box if PBX is not local)	Check this box if the PBX server is remote and you are experiencing problems establishing calls with the PBX.
<b>RTP Settings</b>	
RTP Port (even)	Specify the port number used for the RTP stream after establishing a SIP call. This port number has to be an even number and defaults to 10500.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

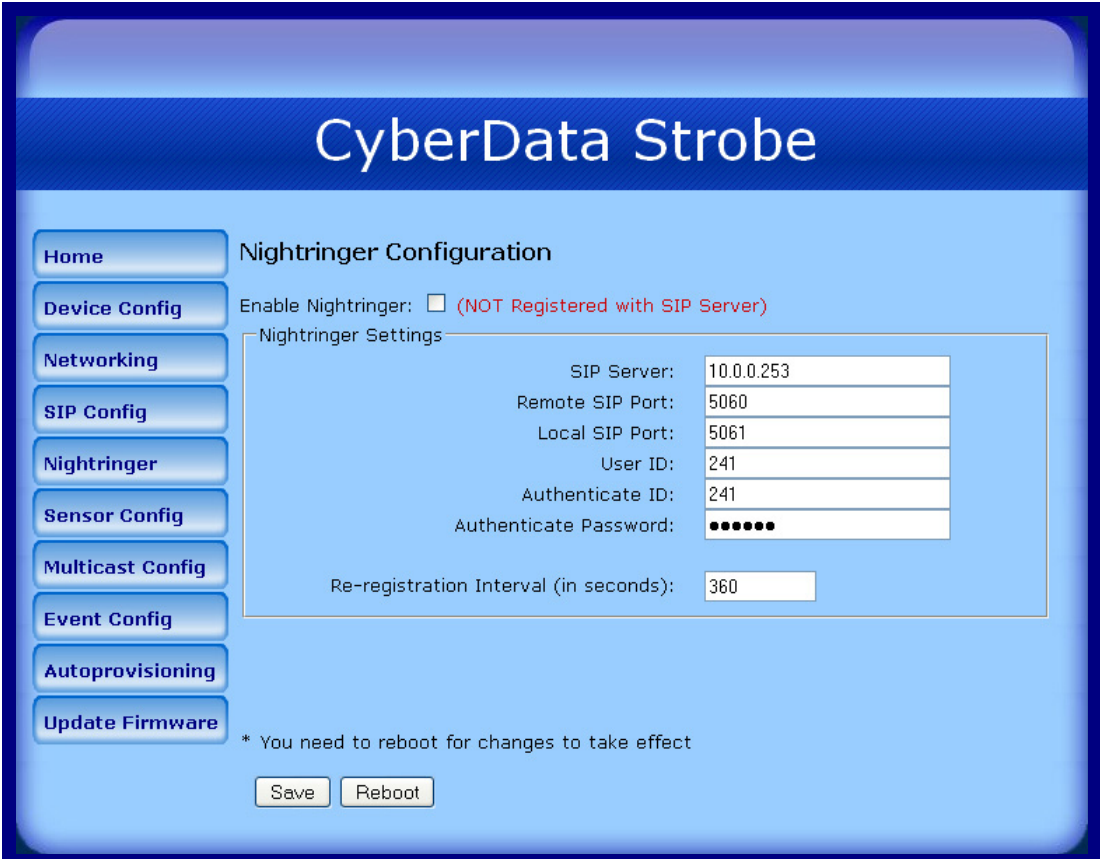
## 2.2.6 Configure the Night Ringer Parameters

When the Nightringer is enabled, the device will register as a second SIP extension. Registration does not have to be to the same server as the primary SIP registration. Any calls made to the Nightringer extension will cause the device to play a ring tone. There is no way to answer this call. The Nightringer is designed to be used in buildings where calls made after hours are directed to a ring group.

**Caution**  
Nightringer requires SIP Registration.

1. Click on the **Nightringer** button to open the **Nightringer Configuration** page. See [Figure 2-15](#).

**Figure 2-15. Nightringer Configuration Setup**



**CyberData Strobe**

**Nightringer Configuration**

Enable Nightringer: ☐ (NOT Registered with SIP Server)

Nightringer Settings

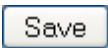

SIP Server:	10.0.0.253
Remote SIP Port:	5060
Local SIP Port:	5061
User ID:	241
Authenticate ID:	241
Authenticate Password:	••••••

Re-registration Interval (in seconds): 360

\* You need to reboot for changes to take effect

2. On the **Nightringer Configuration** page, enter values for the parameters indicated in [Table 2-11](#).

**Table 2-11. Nightringer Configuration Parameters**

Web Page Item	Description
Enable Nightringer	When the nightringer is enabled, the SIP Strobe will attempt to register a second extension with the SIP server. Any calls made to this extension will cause the strobe to flash.
<b>Nightringer Settings</b>	
SIP Server	Type the SIP server represented as either a numeric IP address in dotted decimal notation.
Remote SIP Port	Type the Remote SIP Port number (default 5060) (8 character limit).
Local SIP Port	Type the Local SIP Port number (default 5060) (8 character limit). <b>Note:</b> This value cannot be the same as the <a href="#">Local SIP Port</a> found on the <a href="#">SIP Configuration Page</a> .
User ID	Type the <b>User ID</b> (up to 64 alphanumeric characters).
Authenticate ID	Type the <b>Authenticate ID</b> (up to 64 alphanumeric characters).
Authenticate Password	Type the <b>Authenticate Password</b> (up to 64 alphanumeric characters).
Re-registration Interval (in seconds)	Type the SIP Registration lease time in minutes (default is 60 minutes) (8 character limit). Re-registration Interval (in seconds)
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

3. After changing the parameters, click on the **Save** button.

## 2.2.7 Configure the Sensor Configuration Parameters

The sensor (pins 5 and 6) on the header can be used to monitor the open or closed state of a switch. There is an option on the **Sensor Configuration** page to trigger on an open or short condition on these pins.

The intrusion sensor is an optical sensor installed on the SIP Strobe board and will be activated when the SIP Strobe is removed from the case.

For each sensor there are two actions the SIP Strobe can take:

- Flash the LED until the sensor is deactivated (roughly 10 times/second)
- Activate the relay until the sensor is deactivated

1. Click **Sensor Config** to open the **Sensor Configuration** page (Figure 2-16).

Figure 2-16. Sensor Configuration Page

**CyberData Strobe**

**Sensor Configuration**

**Sensor Settings**

Sensor Normally Closed: ☐ Yes ☒ No

Activate Relay: ☐

Blink Strobe: ☐

Test Sensor

**Intrusion Sensor Settings**

Activate Relay: ☐

Blink Strobe: ☐



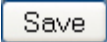

Test Intrusion Sensor

\* You need to reboot for changes to take effect

Save Reboot

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

**Table 2-12. Sensor Configuration Parameters**

Web Page Item	Description
<b>Sensor Settings</b>	
Sensor Normally Closed	Select the inactive state of the sensors.
Activate Relay	Check this box to blink the strobe light until the sensor is deactivated.
Blink Strobe	Check this box to activate the blinking strobe until the sensor is deactivated.
	Use this button to test the sensor.
<b>Intrusion Sensor Settings</b>	
Activate Relay	Check this box to activate the relay until the sensor is deactivated.
Blink Strobe	Check this box to blink the strobe light until the sensor is deactivated.
	Use this button to test the Intrusion sensor.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

## 2.2.8 Configure the Multicast Parameters

Multicast groups use multicasting to create public address paging zones. Multicasting is based on the concept of a group. Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to the group. Group members send IGMP messages to their local multicast routers, allowing the group traffic traversal from the source.

The **Multicast Configuration** page allows the device to join up to 10 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 devices 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 three. The device supports simultaneous SIP and Multicast.

1. Click on the **Multicast Configuration** button to open the **Multicast Configuration** page. See [Figure 2-17](#).

**Figure 2-17. Multicast Configuration Page**

**CyberData Strobe**

**Multicast Configuration**

Enable Multicast operation: ☐

Device Settings

priority	Address	port	Multicast Group Name
9	239.168.3.10	11000	Emergency
8	239.168.3.9	10000	MG8
7	239.168.3.8	9000	MG7
6	239.168.3.7	8000	MG6
5	239.168.3.6	7000	MG5
SIP calls are considered priority 4.5			
4	239.168.3.5	6000	MG4
3	239.168.3.4	5000	MG3
2	239.168.3.3	4000	MG2
1	239.168.3.2	3000	MG1
0	239.168.3.1	2000	Background Music

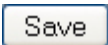
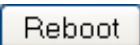
Port range can be from 2000-65535  
 Ports must be even numbers  
 Priority 9 is the highest and 0 is the lowest  
 A higher priority audio stream will always supercede a lower one  
 Priority 9 streams will play at maximum volume

\* You need to reboot for changes to take effect

Save Reboot

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

**Table 2-13. Multicast Configuration Parameters**

Web Page Item	Description
Enable Multicast Operation	Enables or disables multicast operation.
<b>Device Settings</b>	
Priority	Indicates the priority for the multicast group. Priority <b>9</b> is the highest (emergency streams). <b>0</b> is the lowest (background music). SIP calls are considered priority <b>4.5</b> . See <a href="#">Section 2.2.8.1, "Assigning Priority"</a> for more details.
Address	Enter the multicast IP Address for this multicast group (15 character limit).
Port (range can be from 2000 to 65535)	Enter the port number for this multicast group (5 character limit).  <b>Note:</b> The multicast ports have to be even values. The webpage will enforce this restriction.
Multicast Group Name	Assign a descriptive name for this multicast group (25 character limit).
	Click the <b>Save</b> button to save your configuration settings.  <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

3. After changing the parameters, click on the **Save** button.

### 2.2.8.1 Assigning Priority

When playing multicast streams, audio on different streams will preempt each other according to their priority in the list. An audio stream with a higher priority will interrupt a stream with a lower priority.

If both SIP and Multicast is enabled, SIP audio streams are considered priority **4.5**. SIP audio will interrupt multicast streams with priority **0** through **4** and will be interrupted by multicast streams with priority **5** through **9**.

During priority **9** multicast streams the volume level is set to maximum.

**Note** SIP calls, multicast streams, ring tones, ringback tones, and nightring tones are all prioritized.

Ringtones and  
Nightringtones

Ringtones all play at the same priority level. This means that it is possible to have a nightring tone and a normal ringtone playing at the same time.

## 2.2.9 Configure the Event Parameters

Click the **Event Config** button to open the **Event Configuration** page (Figure 2-18). The **Event Configuration** page specifies a remote server that can be used to receive HTTP POST events when actions take place on the board.

Figure 2-18. Event Configuration Page

**CyberData Strobe**

**Event Configuration**

Enable Event Generation: ☐

Remote Event Server

Remote Event Server IP: 10.0.0.250

Remote Event Server Port: 8080

Remote Event Server URL: xmlparse\_engine

Events

Enable Relay Activated Events: ☐

Enable Relay Deactivated Events: ☐

Enable Ring Events: ☐

Enable Night Ring Events: ☐

Enable Multicast Start Events: ☐

Enable Multicast Stop Events: ☐

Enable Power on Events: ☐

Enable Security Events: ☐

Enable 60 second Heartbeat Events: ☐

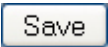
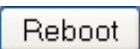
\* You need to reboot for changes to take effect

Save Test Event Reboot



Table 2-14 shows the web page items on the **Event Configuration** page.

**Table 2-14. Event Configuration**

Web Page Item	Description
Enable Event Generation	When selected, Event Generation is enabled.
<b>Remote Event Server</b>	
Remote Event Server IP	Type the Remote Event Server IP address. (64 character limit)
Remote Event Server Port	Type the Remote Event Server port number. (8 character limit)
Remote Event Server URL	Type the Remote Event Server URL. (127 character limit)
<b>Events</b>	
Enable Relay Activated Events	When selected, Relay Activated Events are enabled.
Enable Relay Deactivated Events	When selected, Relay Deactivated Events are enabled.
Enable Ring Events	When selected, Ring Events are enabled.
Enable Night Ring Events	When selected, there is a notification when the device receives a night ring.
Enable Multicast Start Events	When selected, Multicast Start Events are enabled.
Enable Multicast Stop Events	When selected, Multicast Stop Events are enabled.
Enable Power On Events	When selected, Power On Events are enabled.
Enable Security Events	When selected, Security Events are enabled.
Enable 60 Second Heartbeat Events	When selected, 60 Second Heartbeat Events are enabled.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Test Event</b> button to test an event.
	Click on the <b>Reboot</b> button to reboot the system.

### 2.2.9.1 Example Packets for Events

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

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

Here are example packets for every event:

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

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

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

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

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

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

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

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>CALL_ACTIVE</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

```
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 205
Content-Type: application/x-www-form-urlencoded

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

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

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

POST xmlparse_engine HTTP/1.1
Host: 10.0.3.79
User-Agent: CyberData/1.0.0
Content-Length: 234
Content-Type: application/x-www-form-urlencoded

<?xml version="1.0" encoding="ISO-8859-1"?>
<cyberdata NAME='CyberData SIP Device' MAC='0020f70015b6'>
<event>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 SIP 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 SIP Device' MAC='0020f70015b6'>
<event>RELAY_ACTIVATED</event>
</cyberdata>
POST xmlparse_engine HTTP/1.1
```

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

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

## 2.2.10 Configure the Autoprovisioning Parameters

1. Click the **Autoprovisioning** button to open the **Autoprovisioning Configuration** page.  
See [Figure 2-19](#).

**Figure 2-19. Autoprovisioning Configuration Page**

The screenshot shows the 'CyberData Strobe' web interface. On the left is a vertical menu with buttons: Home, Device Config, Networking, SIP Config, Nightringer, Sensor Config, Multicast Config, Event Config, Autoprovisioning (highlighted), and Update Firmware. The main content area is titled 'Autoprovisioning'. Inside this area, there's a sub-section 'Autoprovisioning' containing the following settings:

- Enable Autoprovisioning: ☐
- Get Autoprovisioning from DHCP: ☒
- Autoprovisioning Server (IP Address):
- Autoprovisioning autoupdate (in minutes):


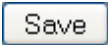

Below these settings is a button labeled 'Get Autoprovisioning Template'. At the bottom of the page, there are two lines of asterisked text:

- \* Autoprovisioning file name: 0020f700e4b7.config
- \* You need to reboot for changes to take effect

At the very bottom are two buttons: 'Save' and 'Reboot'.

2. On the **Autoprovisioning Configuration** page, you may enter values for the parameters indicated in [Table 2-15](#).

**Table 2-15. Autoprovisioning Configuration Parameters**

Web Page Item	Description
<b>Autoprovisioning</b>	
Enable Autoprovisioning	See <a href="#">Section 2.2.10.2, "Autoprovisioning"</a> .
Get Autoprovisioning from DHCP	See <a href="#">Section 2.2.10.2, "Autoprovisioning"</a> .
Autoprovisioning Server (IP Address)	See <a href="#">Section 2.2.10.2, "Autoprovisioning"</a> (15 character limit).
Autoprovisioning Autoupdate (in minutes)	Type the desired time (in minutes) that you want the Autoprovisioning feature to update (6 character limit).
	Press the <b>Get Autoprovisioning Template</b> button to create an autoprovisioning file for this unit. See <a href="#">Section 2.2.10.1, "Get Autoprovisioning Template Button"</a>
Autoprovisioning file name	Displays the current autoprovisioning file name.
	Click the <b>Save</b> button to save your configuration settings. <b>Note:</b> You need to reboot for changes to take effect.
	Click on the <b>Reboot</b> button to reboot the system.

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

### 2.2.10.1 Get Autoprovisioning Template Button

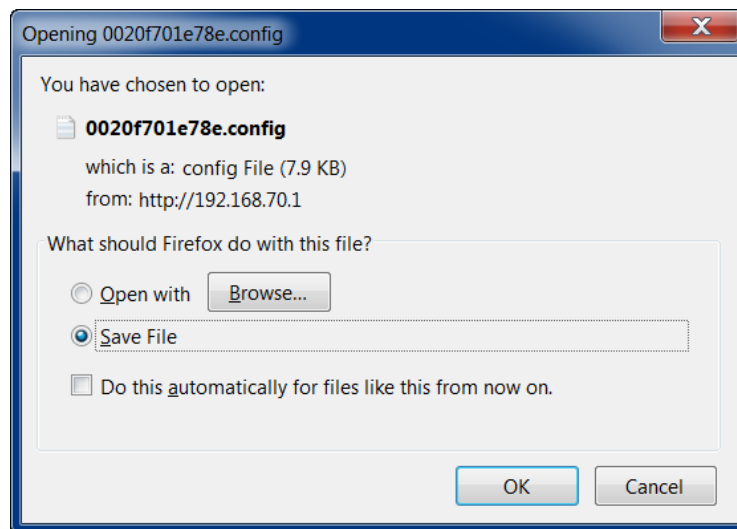
The **Get Autoprovisioning Template** button allows you to create the autoprovisioning template directly from the device by completing the following steps:

1. On the **Autoprovisioning** page, click on the **Get Autoprovisioning Template** button.

**Note** You can also create the autoprovisioning template directly from the device by entering the following web address into your web browser address field:  
**http://<ip address of unit>/cgi-bin/autoprovisioning.cgi**

2. You will see a window prompting you to save a configuration file (**.config**) to a location on your computer ([Figure 2-20](#)). 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 2-20](#).

**Figure 2-20. Configuration File**



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



GENERAL ALERT

#### Caution

Make sure that you do not change the configuration file name. If any part of the configuration file name is changed, the device will not be able to find the file. If you are going to use the configuration file to create multiple configurations, then the configuration files must all be named correctly: **<device mac address>.config**.

5. You can then upload the autoprovisioning file to a TFTP server where the file can be loaded onto other devices.

## 2.2.10.2 Autoprovisioning

### Enable Autoprovisioning Option

With autoprovisioning enabled, the board will get its configuration from a remote TFTP server on startup or periodically on a scheduled delay. Autoprovisioned values will override values stored in on-board memory and will be visible on the web page. The board gets its autoprovisioning information from an XML-formatted file hosted from a TFTP server. CyberData will provide a template for this XML file and the user can modify it for their own use.

To use autoprovisioning, create a copy of the autoprovisioning template with the desired settings and name this file with the mac address of the device to configure (for example: **0020f7350058.config**). Put this file into your TFTP server directory and manually set the TFTP server address on the board.

It is not necessary to set every option found in the autoprovisioning template. As long as the XML is valid, the file can contain any subset. Options not autoprovisioned will default to the values stored in the on board memory. For example if you only wanted to modify the device name, the following would be a valid autoprovisioning file:

```
<?xml version="1.0" encoding="utf-8" ?>
<specific>
  <MiscSettings>
    <DeviceName>auto SIP Strobe</DeviceName>
  </MiscSettings>
</specific>
```

### Networking

The board will only apply networking settings or firmware upgrades after a reboot.

### Get Autoprovisioning from DHCP

When this option is checked, the device will automatically fetch its autoprovisioning server address from the DHCP server. The device will use the address specified in **OPTION 150** (TFTP-server-name) or **OPTION 66**. If both options are set, the device will use **OPTION 150**.

Refer to the documentation of your DHCP server for setting up **OPTION 150**.



To set up a Linux DHCPD server to serve autoprovisioning information (in this case using both option 66 and 150), here's an example dhcpd.conf:

```
# dhcpd.conf
#
# Configuration file for ISC dhcpd (see 'man dhcpd.conf')
#
ddns-update-style ad-hoc;

option option-150 code 150 = ip-address;

subnet 10.0.0.0 netmask 255.0.0.0 {
    max-lease-time 120;
    default-lease-time 120;

    option routers                10.0.0.1;
    option subnet-mask            255.0.0.0;

    option domain-name            "voiplab";
    option domain-name-servers    10.0.0.1;

    option time-offset             -8;      # Pacific Standard Time

    option tftp-server-name        "10.0.0.254";

    option option-150              10.0.0.254;

    range 10.10.0.1 10.10.2.1;}
```

Autoprovisioning Server (IP Address) Instead of using DHCP to provide the autoprovisioning tftp server address, you can specify an address manually.

Autoprovisioning Autoupdate If **Autoprovisioning** is enabled and the **Autoprovisioning Autoupdate** value is something other than **0** minutes, a service is started on startup that will wait the configured number of minutes and then try to re-download its autoprovisioning file. It will compare its previously autoprovisioned file with this new file and if there are differences, it will reboot the board.

Autoprovisioned Firmware Upgrades An Autoprovisioned firmware upgrade only happens after a reboot, will take roughly three minutes, and the web page will be unresponsive during this time.

The '**FirmwareVersion**' value in the xml file *must* match the version stored in the '**FirmwareFile**'.

```
<FirmwareVersion>v5.0.5b01</FirmwareVersion>
<FirmwareFile>505b01-uImage-SIP Strobe</FirmwareFile>
```

If these values are mismatched, the board can get stuck in a loop where it goes through the following sequence of actions:

1. The board downloads and writes a new firmware file.
2. After the next reboot, the board recognizes that the firmware version does not match.
3. The board downloads and writes the firmware file again.

CyberData has timed a firmware upgrade at 140 seconds. Therefore, if you suspect the board is stuck in a loop, either remove or comment out the **FirmwareVersion** line in the XML file and let the board boot as it normally does.

## 2.3 Upgrade the Firmware and Reboot the SIP Strobe

**Note** To guard against failed firmware upgrades, units shipped from CyberData with firmware version 1.0.2 and later feature a built-in "fail safe" mechanism.

**Note** A new firmware signature prevents users from loading firmware intended for one device to a different device.

Use [Table 2-16](#) to determine the purpose of various firmware versions.

**Table 2-16. Firmware Versions**

Firmware Version	Purpose
801-ulmage-strobe	This image must be used to UPGRADE to v8.0.1. Customers wishing to upgrade from v1.0.1 MUST upgrade to v7.1.7 first, then on to later versions.
717-ulmage-strobe	This image must be used to UPGRADE to v7.1.7 from v1.0.1 or older.
717-ulmage-d-strobe	This image must be used to DOWNGRADE from v7.1.8 or LATER to v7.1.7
101-ulmage-d-strobe	This image must be used to DOWNGRADE from v7.1.7 or LATER to v1.0.1.

**Note** It is not possible to do any of the following:

- It is not possible to upgrade v1.0.1 or older with 717-ulmage-d-strobe.
- It is not possible to downgrade from future revisions to v7.1.7 with 717-ulmage-strobe.
- It is not possible to downgrade from v7.1.7 or newer to v1.0.1 with the existing v1.0.1 on our website; 101-ulmage-d-strobe must be used.

**Note** Customers wishing to upgrade from v1.0.1 MUST upgrade to v7.1.7 first, then on to later versions.

To upload the firmware from your computer:

1. Retrieve the latest SIP Strobe firmware file from the SIP Strobe **Downloads** page at:  
<http://www.cyberdata.net/products/voip/digitalanalog/strobe/downloads.html>
2. Unzip the firmware version file. This file may contain the following:
  - Firmware file
  - Release notes
3. Log in to the SIP Strobe home page as instructed in [Section 2.2.2, "Log in to the Configuration Home Page"](#).
4. Click the **Update Firmware** button to open the **Upgrade Firmware** page. See [Figure 2-21](#).


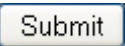
Figure 2-21. Upgrade Firmware Page

5. Select **Browse**, and then navigate to the location of the SIP Strobe firmware file.
6. Click **Submit**.

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

Table 2-17 shows the web page items on the **Upgrade Firmware** page.

Table 2-17. Firmware Upgrade Parameters

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

## 2.3.1 Reboot the SIP Strobe

To reboot a SIP Strobe:

1. Log in to the web page as instructed in [Section 2.2.2, "Log in to the Configuration Home Page"](#).
2. Click the **Reboot** button ([Figure 2-22](#)). A normal restart will occur.

**Figure 2-22. Reboot System Section**

The screenshot displays the 'CyberData Strobe' configuration web interface. On the left is a vertical navigation menu with buttons for Home, Device Config, Networking, SIP Config, Nightringer, Sensor Config, Multicast Config, Event Config, Autoprovisioning, and Update Firmware. The main content area is divided into three sections: 'Device Settings' with fields for Device Name (CyberData VoIP Strobe), Change Username (admin), Change Password, and Re-enter Password; 'Current Settings' listing various parameters like Part Number, Serial Number, Mac Address, Firmware Version, IP Addressing, IP Address, Subnet Mask, Default Gateway, DNS Servers, SIP Mode, Multicast Mode, Event Reporting, Nightringer status, and SIP Servers; and 'Import/Export Settings' with fields for configuration file import/export. At the bottom, a note states '\* You need to reboot for changes to take effect', followed by 'Save' and 'Reboot' buttons. A red arrow points from the 'Reboot' button to the label 'Reboot' located below the screenshot.

Reboot

---

## 2.4 Command Interface

Some functions on the device can be activated using simple POST commands to the web interface. The examples in [Table 2-18](#) use the free unix utility, **wget** commands. However, any program that can send HTTP POST commands to the device should work.

---

### 2.4.1 Command Interface Post Commands

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





**Table 2-18. Command Interface Post Commands**

Device Action	HTTP Post Command <sup>a</sup>
Trigger relay (for configured delay)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "test_relay=yes"
Place call to extension (example: extension 130)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "call=130"
Terminate active call	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "terminate=yes"
Force reboot	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/command.cgi" --post-data "reboot=yes"
Trigger the Door Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "doortest=yes"
Trigger the Intrusion Sensor Test (Sensor Config page)	wget --user admin --password admin --auth-no-challenge --quiet -O /dev/null "http://10.0.3.71/cgi-bin/sensorconfig.cgi" --post-data "intrusiontest=yes"

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

# Appendix A: Mounting the SIP Strobe

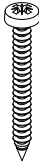
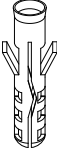
## A.1 Important Safety Instructions

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

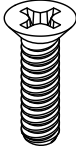
## A.2 Mount the SIP Strobe

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

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

Quantity	Part Name	Illustration
4	#6 x 1.5 inches Sheet Metal Screw	
4	#6 Ribbed Plastic Anchor	

**Table A-2. Gang Box Mounting Components**

Quantity	Part Name	Illustration
4	#6-32 x 0.625-inch Flat-Head Machine Screw.	

After the SIP Strobe is assembled, plug the Ethernet cable into the SIP Strobe Assembly (see [Figure A-1](#)).

[Section 2.1.4, "Network Connectivity, and Data Rate"](#) explains how the **Link** and **Status** LEDs work.

**Figure A-1. Network Connector Prior to Installation**

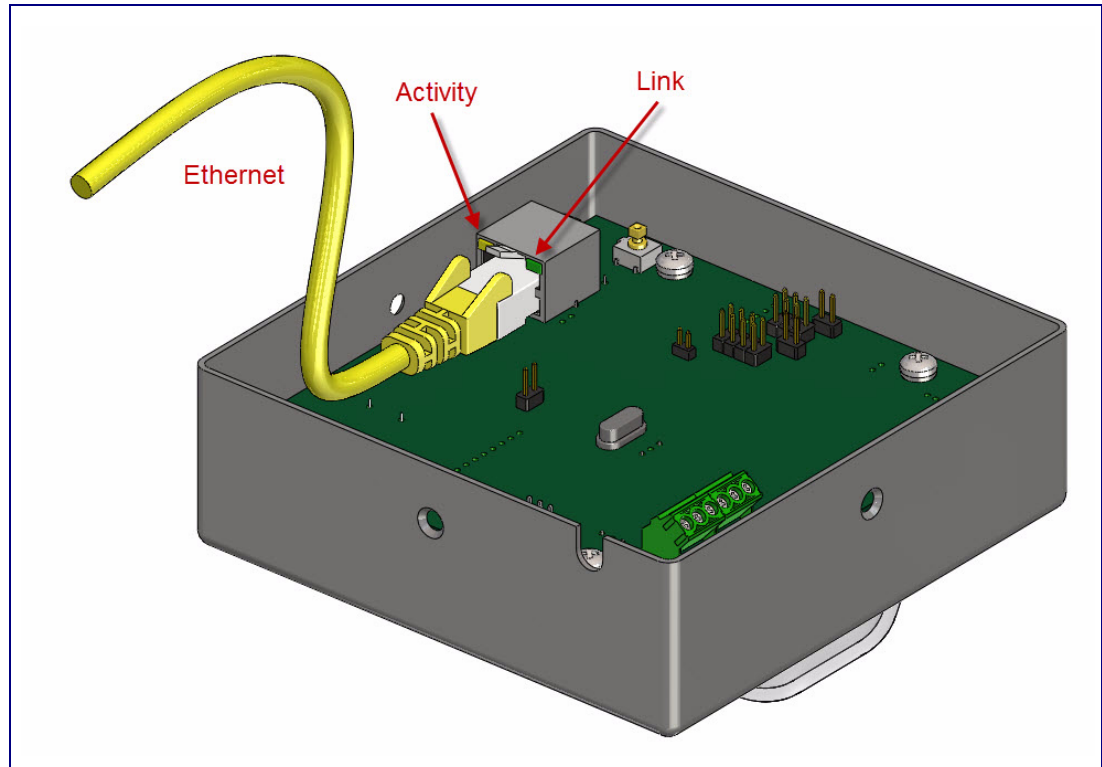




Figure A-2 shows the wall mounting options for the SIP Strobe.

**Note** Be sure to connect the SIP Strobe up to the Earth Ground.

**Figure A-2. Wall Mounting Options**

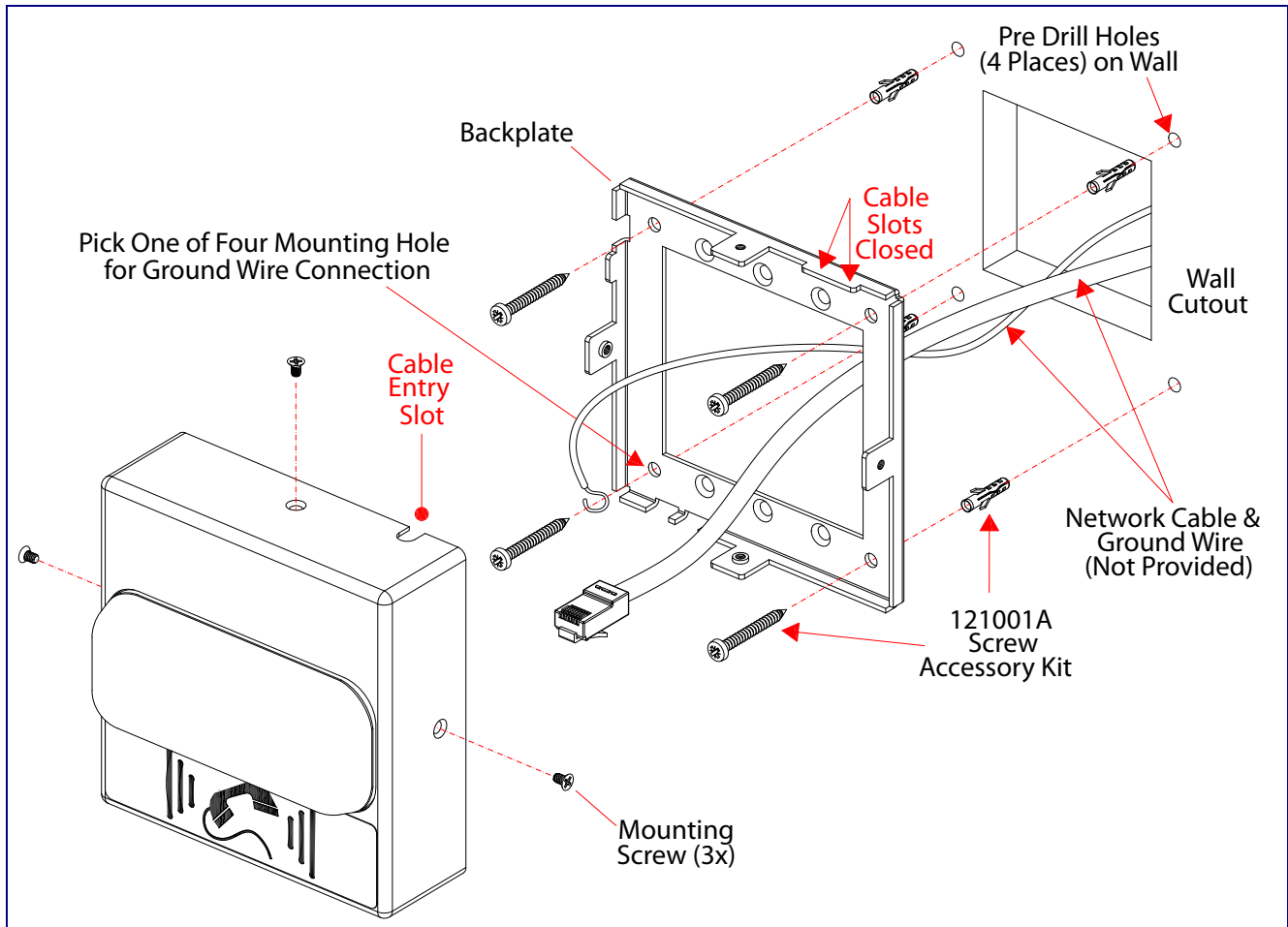


Figure A-2 shows the gang box mounting options for the SIP Strobe.

**Note** Be sure to connect the SIP Strobe up to the Earth Ground.

**Figure A-3. Gang Box Mounting Options**

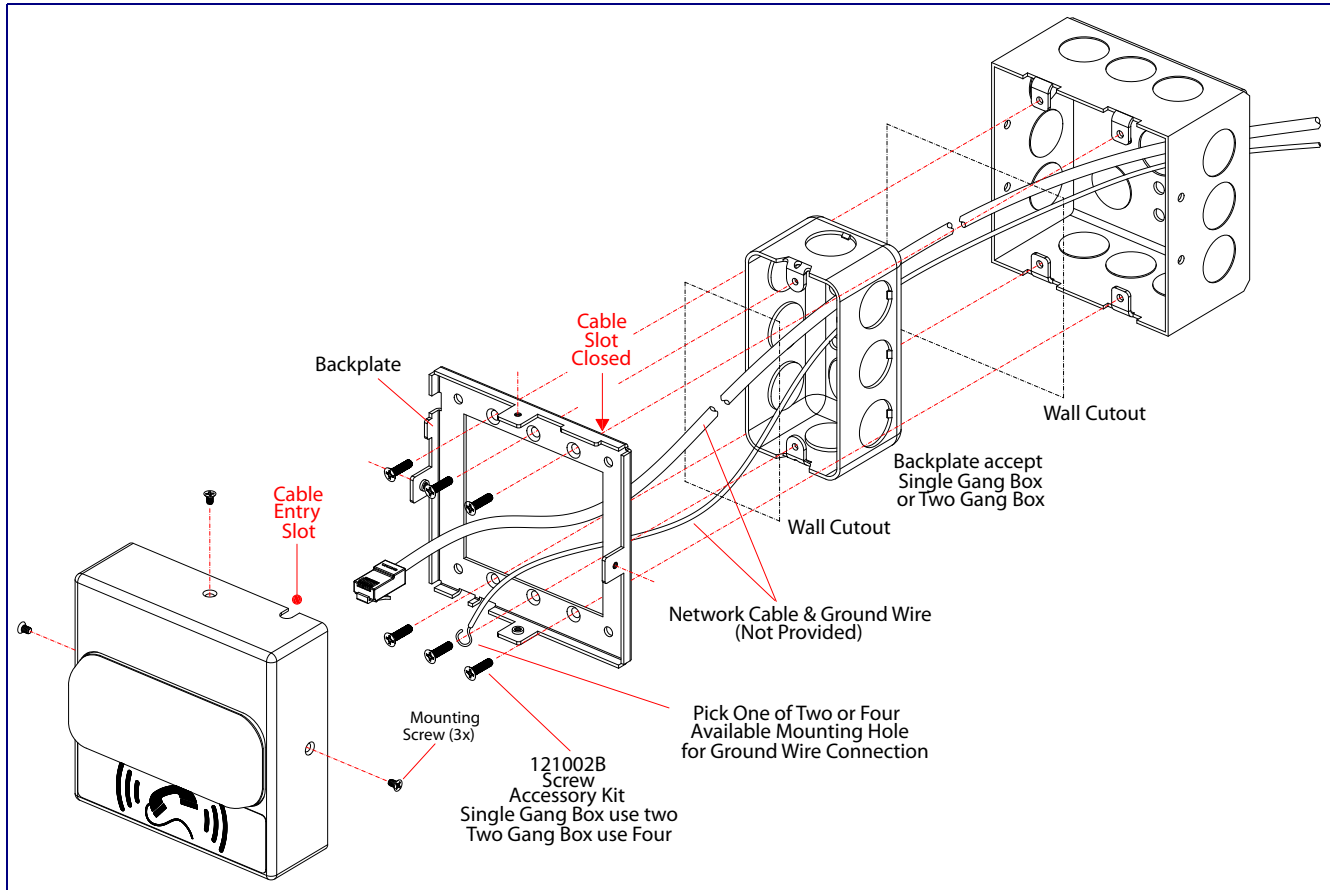
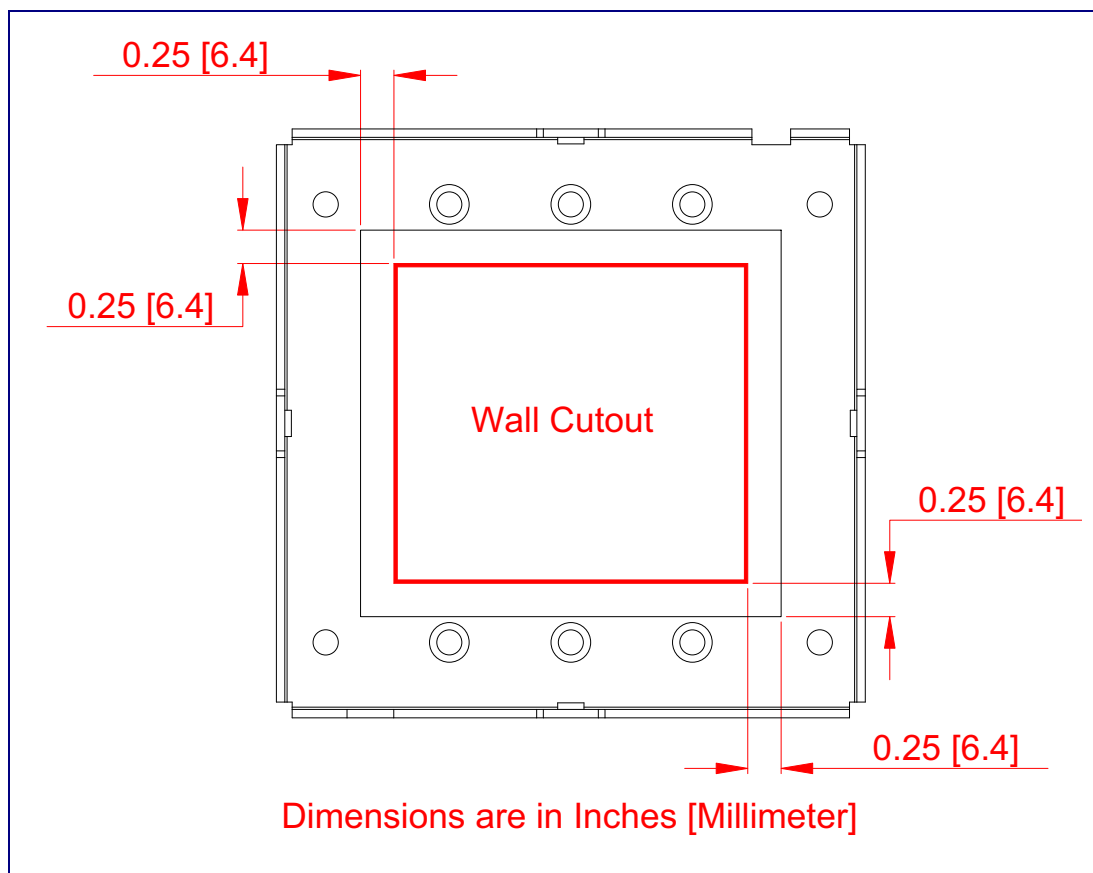


Figure A-4 shows the maximum recommended wall cutout dimensions for mounting the SIP Strobe.

**Figure A-4. Maximum Recommended Wall Cutout Dimensions**



# Appendix B: Troubleshooting/Technical Support

---

## B.1 Frequently Asked Questions (FAQ)

A list of frequently asked questions (FAQs) are available on the SIP Strobe product page at:

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

Select the support page for your product to see a list of frequently asked questions for the CyberData product:

---

## B.2 Documentation

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

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

## B.3 Contact Information

Contact	<p>CyberData Corporation  3 Justin Court  Monterey, CA 93940 USA  <a href="http://www.CyberData.net">www.CyberData.net</a>  Phone: 800-CYBERDATA (800-292-3732)  Fax: 831-373-4193</p>
Sales	<p>Sales 831-373-2601 Extension 334</p>
Technical Support	<p>The fastest way to get technical support for your VoIP product is to submit a VoIP Technical Support form at the following website:</p> <p><a href="http://support.cyberdata.net/">http://support.cyberdata.net/</a></p> <p>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 <b>Comments</b> section of the Support Form.</p> <p>Phone: (831) 373-2601, Ext. 333  Email: support@cyberdata.net</p>
Returned Materials Authorization	<p>To return the product, contact the Returned Materials Authorization (RMA) department:</p> <p>Phone: 831-373-2601, Extension 136  Email: RMA@CyberData.net</p> <p>When returning a product to CyberData, an approved CyberData RMA number must be printed on the outside of the original shipping package. Also, RMA numbers require an active VoIP Technical Support ticket number. A product will not be accepted for return without an approved RMA number. Send the product, in its original package, to the following address:</p> <p>CyberData Corporation  3 Justin Court  Monterey, CA 93940  Attention: RMA "your RMA number"</p>
RMA Status Form	<p>If you need to inquire about the repair status of your product(s), please use the CyberData RMA Status form at the following web address:</p> <p><a href="http://support.cyberdata.net/">http://support.cyberdata.net/</a></p>

## B.4 Warranty and RMA Information

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

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

# Index

---

## Numerics

16 AWG gauge wire 6

## A

AC voltages 2  
 AC voltages, enclosure is not rated 7, 47  
 act light 12  
 activate relay (intrusion sensor) 30  
 activate relay (sensor) 30  
 address, configuration login 17  
 alternative power input 4  
 audio encodings 3  
 autoprovisioning 41  
     autoprovisioned firmware upgrades 42  
     autoprovisioning autoupdate 42  
     autoprovisioning enabled option 41  
     autoprovisioning from DHCP 41  
     autoprovisioning server (IP address) 42  
     get autoprovisioning template button 39  
     networking 41  
 autoprovisioning configuration 38, 39  
 auxiliary relay 7  
 auxiliary relay wiring diagram 8

## B

backup SIP server 1 25  
 backup SIP server 2 25  
 backup SIP servers, SIP server  
     backups 25  
 baud rate  
     verifying 11  
 blink strobe (intrusion sensor) 30  
 blink strobe (sensor) 30

## C

changing  
     the web access password 20  
 Cisco SRST 25  
 command interface 46  
 commands 46  
 configurable parameters 19, 21, 23, 25, 44  
 configuration

    default IP settings 15  
     door sensor 29  
     intrusion sensor 29  
     network 22  
     SIP 24  
     using Web interface 15  
 configuration home page 18  
 configuration page  
     configurable parameters 19, 21, 23, 25, 44  
 contact information 54  
 contact information for CyberData 54  
 Current Network Settings 23  
 current network settings 23  
 CyberData contact information 54

## D

default  
     device settings 55  
     gateway 15  
     IP address 15  
     subnet mask 15  
     username and password 15  
     web login username and password 18  
 default device settings 14  
 default gateway 15, 23  
 default IP settings 15  
 default login address 17  
 device configuration 20  
     device configuration parameters 39  
     the device configuration page 38  
 device configuration page 20  
 device configuration parameters 21  
 device configuration password  
     changing for web configuration access 20  
 DHCP Client 3  
 DHCP IP addressing 23  
 dimensions 4  
 discovery utility program 17  
 DNS server 23  
 door sensor 30

## E

earth ground 50, 51  
 enable night ring events 34  
 ethernet cable 49  
 ethernet I/F 4

- event configuration
  - enable night ring events 34
- expiration time for SIP server lease 25, 26, 28
- export configuration button 19
- export settings 19

## F

- factory default settings 14
  - how to set 14
- firmware
  - where to get the latest firmware 43

## G

- gang box mounting 50, 51
- get autoprovisioning template button 39
- green link light 11

## H

- home page 18
- http POST command 46
- http web-based configuration 3

## I

- identifying your product 1
- illustration of device mounting process 48
- import configuration button 19
- import settings 19
- import/export settings 19
- installation, typical device system 2
- intrusion sensor 29, 30
  - activate relay 30
- IP address 15, 23
- IP addressing 23
  - default
    - IP addressing setting 15

## J

- J3 terminal block, 16 AWG gauge wire 6

## L

- lease, SIP server expiration time 25, 26, 28
- lengthy pages 32
- link LED 49
- link light 11
- local SIP port 25
- log in address 17

## M

- MGROUP
  - MGROUP Name 32
- mounting the device 48
- multicast configuration 31
- Multicast IP Address 32

## N

- navigation (web page) 16
- navigation table 16
- network activity, verifying 12
- network configuration 22
- Network Setup 22
- nightring tones 32
- Nightringer 6, 27, 40
- Nightringer in peer to peer mode (cannot be used) 27
- nightringer settings 28
- Nightringer, SIP registration required 27

## O

- on-board relay 4
- operating temperature 4

## P

- packet time 3
- pages (lengthy) 32
- part number 4
- parts list 5
- password
  - for SIP server login 25
  - login 18
  - restoring the default 15
- payload types 4
- port
  - local SIP 25

- remote SIP 25
- POST command 46
- power input 4
  - alternative 4
- priority
  - assigning 32
- product
  - configuring 15
  - mounting 48
  - parts list 5
- product features 3
- product overview
  - product features 3
  - product specifications 4
  - supported protocols 3
  - supported SIP servers 3
  - typical system installation 2
- product specifications 4
- protocol 4
- protocols supported 3

## R

- reboot 44, 45
- regulatory compliance 4
- remote SIP port 25
- Reset Test Function Management (RTFM) switch 14
- reset test function management switch 13
- resetting the IP address to the default 47, 53
- restoring factory default settings 14, 55
- restoring the factory default settings 14
- ringtones 32
  - lengthy pages 32
- RMA returned materials authorization 54
- RMA status 54
- RTFM jumper 13
- RTFM switch 13, 14
- RTP/AVP 3

## S

- sales 54
- sensor 30
  - activate relay 30
  - blink strobe 30
  - sensor normally closed 30
- sensor setup page 29
- sensor setup parameters 29
- sensors 30
- server address, SIP 25
- service 54
- setting up the device 6

- settings, default 14
- SIP
  - enable SIP operation 25
  - local SIP port 25
  - user ID 25
- SIP (session initiation protocol) 3
- SIP configuration 24
  - SIP Server 25
- SIP configuration parameters
  - outbound proxy 25
  - registration and expiration, SIP server lease 25, 26, 28
  - user ID, SIP 25
- SIP registration 25
- SIP remote SIP port 25
- SIP server 25
  - password for login 25
  - SIP servers supported 3
  - user ID for login 25
- SRST 25
- static IP addressing 23
- status LED 49
- subnet mask 15, 23
- supported protocols 3

## T

- tech support 54
- technical support, contact information 54
- terminal block, 16 AWG gauge wire 6

## U

- user ID
  - for SIP server login 25
- username
  - changing for web configuration access 20
  - default for web configuration access 18
  - restoring the default 15

## V

- verifying
  - baud rate 11
  - network activity 12
  - network connectivity 11



## W

- warranty policy at CyberData 54
- web access password 15
- web access username 15
- web configuration log in address 17
- web page
  - navigation 16
- web page navigation 16
- web-based configuration 15
- weight 4
- wget, free unix utility 46

## Y

- yellow act light 12