



USERS MANUAL

February 2009

Version 1.5a

Customer Service

We support you...

By phone/fax in the USA:

Customer service is available from 9:30 AM to 6:00 PM USA Eastern Time, Monday through Friday at +1 (216) 241-3343. Fax: +1 (216) 241-4103.

By phone/Fax in Europe:

Service is available from Telos Europe in Germany at +49 81 61 42 467.

Fax: +49 81 61 42 402.

By E-Mail:

The address is: support@telos-systems.com

Via World Wide Web:

The Telos Web site has a variety of information that may be useful for product selection, software and manual updates and general information. The URL is:
<http://www.telos-systems.com>.

Feedback

We welcome feedback on any aspect of the Zephyr/IP™ or this manual. In the past, many good ideas from users have made their way into software revisions or new products. Please contact us with your comments.

Telos Systems
2101 Superior Avenue
Cleveland, OH 44114
USA
+1 (216) 241-3343
Fax: +1 (216) 241-4103

Updates

The operation of the Zephyr/IP™ is partially controlled by software. A continuous program of improvement is underway. Contact us to determine if a newer release is available.

Trademarks

Telos Systems, the Telos Systems logo, and Zephyr/IP are trademarks of TLS Corporation. All other trademarks are the property of their respective holders.

Copyright

Copyright © 1994-2007 by TLS Corporation. Published by Telos Systems, who reserves the right to make improvements or changes in the products described in this manual, which may affect the product specifications, or to revise the manual without notice. All rights reserved.

Notice

All versions, claims of compatibility, trademarks, etc. of hardware and software products not made by Telos Systems mentioned in this manual or accompanying material are informational only. Telos Systems makes no endorsement of any particular product for any purpose, nor claims any responsibility for operation or accuracy.

Warranty

This product is covered by a one year limited warranty, the full text of which is included in the Appendix of this manual.

Updates

The operation of the Zephyr/IP is determined largely by software. Please check the Telos website for the latest available version.

Service

You must contact Telos Systems before returning any equipment for factory service. Telos Systems will issue a Return Authorization number **which must be written on the exterior of your shipping container**. Please do not return cables or accessories unless specifically requested by Telos Systems technical support. Be sure to adequately insure your shipment for its replacement value. Packages without proper authorization may be refused. USA customers: please contact Telos Systems technical support at +1 (216) 241-7225. All other customers should contact their local dealer to make arrangements for service.

Hardware Notices and Cautions



CAUTION:

THE INSTALLATION AND SERVICING INSTRUCTIONS IN THIS MANUAL ARE FOR USE BY QUALIFIED PERSONNEL ONLY. TO AVOID ELECTRIC SHOCK, DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE OPERATING INSTRUCTIONS UNLESS YOU ARE QUALIFIED TO DO SO. REFER ALL SERVICING TO QUALIFIED PERSONNEL.



WARNING:

TO REDUCE THE RISK OF ELECTRICAL SHOCK, DO NOT EXPOSE THIS PRODUCT TO RAIN OR MOISTURE. DO NOT SHOWER WITH THE UNIT.



THIS SYMBOL, WHEREVER IT APPEARS, ALERTS YOU TO THE PRESENCE OF UNINSULATED, DANGEROUS VOLTAGE INSIDE THE CLOSURE - VOLTAGE WHICH MAY BE SUFFICIENT TO CONSTITUTE A RISK OF SHOCK.



THIS SYMBOL, WHEREVER IT APPEARS, ALERTS YOU TO IMPORTANT OPERATING INSTRUCTIONS.



CAUTION
TO PREVENT RISKS OF
ELECTRIC SHOCK
DISCONNECT POWER
CORD BEFORE SERVICING



USA CLASS A COMPUTING DEVICE INFORMATION TO USER.

WARNING: This equipment generates, uses, and can radiate radio-frequency energy. If it is not installed and used as directed by this manual, it may cause interference to radio communication. This equipment complies with the limits for a Class A computing device, as specified by FCC Rules, Part 15, Subpart J, which are designed to provide reasonable protection against such interference when this type of equipment is operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference. If it does, the user will be required to eliminate the interference at the user's expense. **NOTE:** Objectionable interference to TV or radio reception can occur if other devices are connected to this device without the use of shielded interconnect cables. FCC rules require the use of only shielded cables.



CANADA WARNING: "This digital apparatus does not exceed the Class A limits for radio noise emissions set out in the Radio Interference Regulations of the Canadian Department of Communications." "Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques (de les Class A) prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada."

Table of Contents

1	INTRODUCTION.....	10
2	QUICK START GUIDE.....	13
3	INSTALLATION.....	22
3.1	RACK MOUNTING THE STUDIO UNIT.....	22
3.2	POWER.....	22
3.3	ANALOG AUDIO INPUTS.....	22
	<i>STUDIO VERSION.....</i>	<i>22</i>
	<i>MXP VERSION.....</i>	<i>23</i>
3.4	AES/EBU DIGITAL AUDIO INPUT (STUDIO UNIT ONLY).....	23
3.5	AES/EBU DIGITAL AUDIO OUTPUT (STUDIO UNIT ONLY).....	23
3.6	AES/EBU DIGITAL AUDIO SYNC (OPTIONAL, STUDIO UNIT ONLY).....	23
3.7	NETWORK ADAPTORS.....	24
3.8	USB PORTS.....	24
3.9	PARALLEL CONTROL.....	24
4	THE USER INTERFACE AND SETUP.....	26
4.1	THE FRONT PANEL BUTTON CONTROLS.....	26
4.2	THE GRAPHICAL INTERFACE AND MENU SYSTEM.....	29
	<i>THE STUDIO VERSION AUDIO MENU.....</i>	<i>30</i>
	<i>THE MXP VERSION AUDIO MENU.....</i>	<i>31</i>
	<i>THE CODEC MENU.....</i>	<i>34</i>
	<i>THE NETWORK MENU.....</i>	<i>35</i>

<i>THE STATUS MENU</i>	38
<i>THE SETTINGS MENU</i>	41

5 THE WEB INTERFACE..... 43

5.1 HOW TO ACCESS THE WEB INTERFACE 43

5.2 WHAT CAN I DO ON THE WEB INTERFACE?..... 43

<i>MAIN MENU</i>	43
<i>QUICKSTART MENU</i>	43
<i>NETWORK MENU</i>	45
<i>SETTINGS MENU</i>	45
<i>SOFTWARE UPDATE</i>	46
<i>AUTO DIAL MENU (JAVA INTERFACE)</i>	47

6 MAKING CONNECTIONS WITH OTHER UNITS 49

6.1 CREATING A Z/IP IDENTITY ON THE Z/IP SERVER 49

6.2 THE BUDDY LIST 50

<i>ADD A BUDDY TO YOUR LIST</i>	51
---------------------------------------	----

6.3 THE STATUS BAR..... 54

6.4 CALLING A UNIT DIRECTLY 55

<i>CALL HISTORY</i>	56
---------------------------	----

6.5 RELAY CONNECTION OVER THE SERVER 56

6.6 SIP CALLS 57

<i>SIP CONFIGURATION</i>	57
<i>MAKING SIP CALLS</i>	58
<i>ADDING SIP DEVICES TO THE SPEED DIAL LIST</i>	58

7 THE ZEPHYR/IP SERVER 59

7.1 DIRECTORY SERVICE 59

7.2 PRESENCE SERVICE 60

7.3 NAT TRAVERSAL SERVICE 60

7.4 MEDIA RELAY SERVICE 60

7.5 GEO-LOCATION SERVICE	60
---------------------------------------	-----------

8 GROUPS AND DIRECTORY SERVICES.....	62
---	-----------

<i>WHY GROUPS?</i>	<i>62</i>
<i>THE PUBLIC GROUP</i>	<i>62</i>
<i>CREATING GROUPS.....</i>	<i>62</i>
<i>DIRECTORY LISTING VISIBILITY.....</i>	<i>63</i>
<i>GROUP AND DEVICE NAME LONGEVITY</i>	<i>63</i>
<i>REUSING A ZEPHYR/IP NAME</i>	<i>64</i>

9 WHEN AN IT DEPARTMENT IS NOT AVAILABLE	65
---	-----------

9.1 IP ADDRESSES, SUBNET MASKS AND GATEWAYS	65
--	-----------

<i>IP ADDRESSES</i>	<i>65</i>
<i>SUBNET MASKS</i>	<i>65</i>
<i>GATEWAYS</i>	<i>68</i>
<i>DNS.....</i>	<i>68</i>
<i>DHCP</i>	<i>68</i>

9.2 DISCOVER THE LOCAL NETWORK SETTINGS	69
--	-----------

9.3 FIND AN AVAILABLE IP ADDRESS WITHOUT A DHCP SERVER	70
---	-----------

9.4 DUPLICATE IP ADDRESSES.....	72
--	-----------

9.5 USE TRACEROUTE TO FIND THE COMMUNICATION BOTTLENECKS.....	72
--	-----------

9.6 NETWORK ADDRESS TRANSLATION	73
--	-----------

<i>WHAT IS IT?.....</i>	<i>73</i>
<i>ARE ALL NAT DEVICES THE SAME?</i>	<i>74</i>
<i>HOW DO NAT DEVICES AFFECT COMMUNICATION DEVICES?</i>	<i>74</i>
<i>HOW DOES THE Z/IP SERVER HELP?</i>	<i>74</i>
<i>HOW DO I USE PORT FORWARDING WITH THE Z/IP?</i>	<i>74</i>

10 OPTION CARDS.....	76
-----------------------------	-----------

10.1 INSTALLATION OF OPTION CARDS.....	76
---	-----------

11 THE PARALLEL PORT AND CONTACT CLOSURES 77

11.1 PARALLEL PORT OUTPUT MODES 79

11.2 PARALLEL PORT INPUT MODES 80

12 AUDIO CODING REFERENCE 81

12.1 INTRODUCTION TO AUDIO CODING TECHNOLOGY 81

<i>INTRODUCTION</i>	81
<i>BASIC PRINCIPLES OF PERCEPTUAL CODING</i>	82
<i>MPEG</i>	85
<i>MPEG4 AAC (ADVANCED AUDIO CODING)</i>	86
<i>AAC-LD (AAC LOW DELAY)</i>	88
<i>MPEG-4 HIGH EFFICIENCY AAC (HE-AAC)</i>	90
<i>MPEG-4 ENHANCED LOW DELAY AAC</i>	90
<i>ISO/MPEG LAYER-2</i>	91
<i>G.722</i>	91

13 MOBILE NETWORK DEVICES 93

13.1 HOW TO USE MOBILE DATA DEVICES ON THE ZEPHYR/IP 93

13.2 WI-FI DEVICES..... 94

13.3 EVDO OR MOBILE BROADBAND MODEMS..... 94

14 USING THE FIELD UPGRADE OPTION 96

14.1 UPDATING THE SOFTWARE THROUGH THE WEB INTERFACE 96

<i>FIRMWARE UPDATE:</i>	97
<i>UPDATE SYSTEM SOFTWARE</i>	97

14.2 INSTALLING A NEW FLASH CARD 98

15 SPECIFICATIONS 101

AUDIO SPECIFICATIONS 101

POWER 101

16 WARRANTY AND APPLICATION CAUTION 103

ZEPHYR/IP LIMITED WARRANTY 103

17 CE DECLARATION OF CONFORMITY 105

SUPPLEMENTARY INFORMATION FOR OUR EUROPEAN USERS 105

DECLARATION OF CONFORMITY 105

USE OF SHIELDED CABLES 107

18 SAFETY NOTIFICATION 108

1 Introduction

The Zephyr/IP is available in two versions:

- A rackmount “Studio Version” intended to be used inside broadcast facilities:



- A rugged “MXP (mixer) Version” intended to be used for remote broadcasts:



Both versions combine RTP/UDP and TCP/IP streaming capabilities with MPEG coding to deliver broadcast-quality audio over IP connections. Zephyr/IP employs sophisticated new technology to achieve superb audio quality over IP links such as the Internet and mobile IP services. Zephyr/IP utilizes ACT™ - Agile Connection Technology – to continuously adapt to network conditions, minimizing the effects of packet loss, varying bandwidth, and jitter that can occur on these networks by means of sophisticated error detection and concealment, dynamic buffering and other techniques that work together to provide reliable IP audio connections.

The Zephyr/IP has an impressive list of features including:

- Analog and Digital audio inputs (Studio unit)

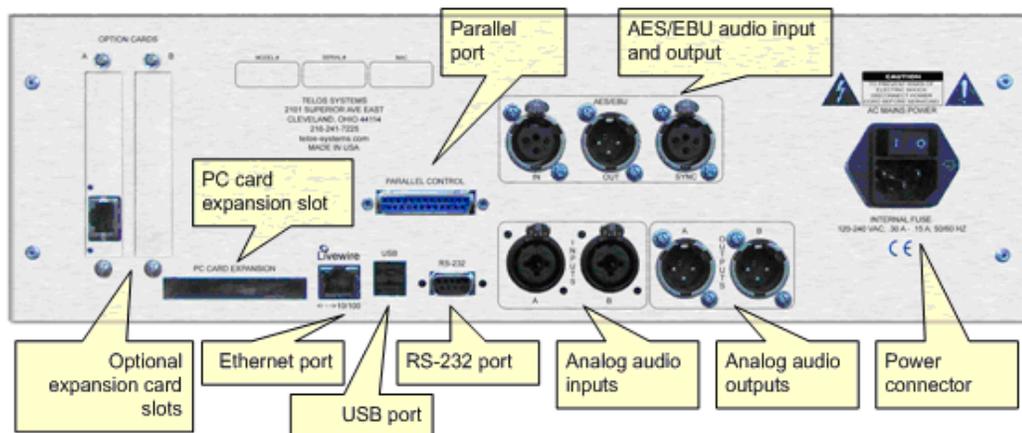
- Analog microphone inputs and analog outputs (MXP version)
- Selectable microphone input level and audio processing (MXP version)
- Supports transmission bit rates from 16 kbps to 256 kbps
- User-friendly, information-rich graphical interface with large full VGA display screen
- A full-color, real-time graphical connection status display
- Context-sensitive on-screen help available at a touch. Telos-hosted Z/IP Server service enables speedy lookup of and connection to other Zephyr/IP users worldwide, even through firewalls and Network Address Translation (NAT) devices
- Backward compatible with Telos Zephyr Xstream and other third party codecs
- Built-In web server for configuration and remote control
- Wireless connection through Wi-Fi and EVDO modems (USB modem required)
- Livewire input and output.

2 Quick Start Guide

After unpacking your Zephyr/IP you can quickly get up and running using this simple guide. The steps involved are: attach cables, configure the network interface, configure the Z/IP server settings, connect to the network, adjust the audio settings and make a test call. Details follow below.

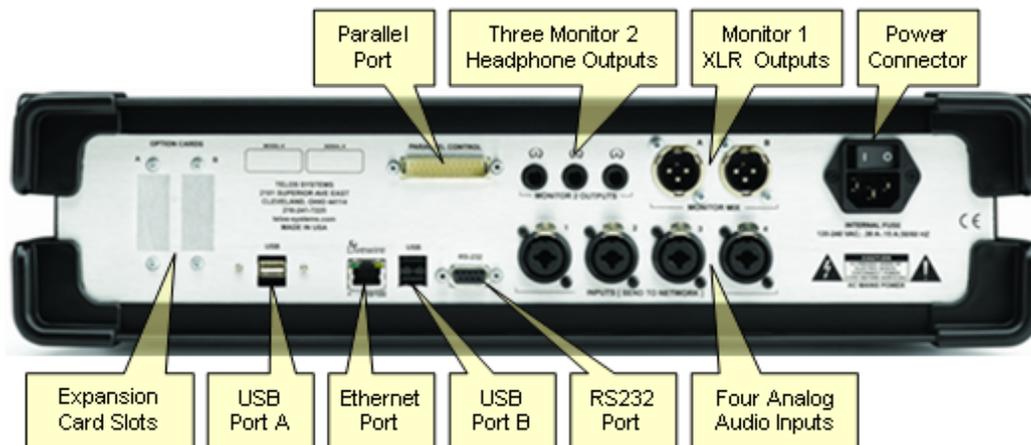
Step 1a: Attach Cables to Studio Unit

Attach the power cable, and your audio cables (two pairs of XLR cables for stereo analog, or one pair of cables for AES/EBU in and out). Do not connect the unit on your network at this time.



Step 1b: Attach Cables to MXP Unit

Attach the power cable, and your audio cables. One pair of analog XLR cables for stereo output; up to four XLR cables for microphone input. Note that the microphone input levels can be adjusted in the “Audio” menu to four different levels from professional level to +40dB. Also, phantom power can be turned on from the Audio menu. Do not connect the unit on your network at this time.



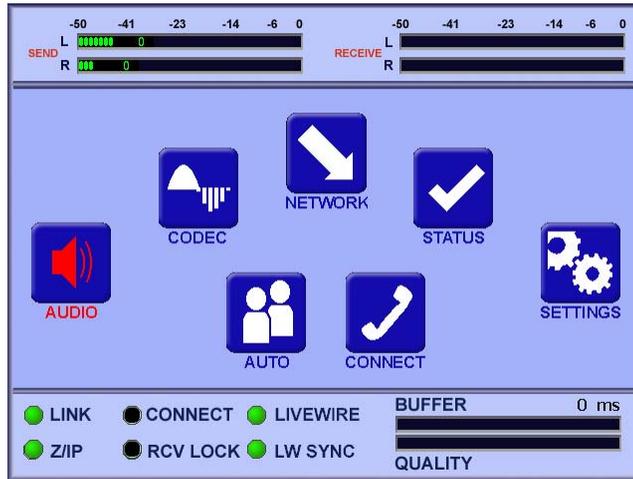
If you are using the MXP inputs as line input make sure that you have phantom power disabled in the Audio menu! Phantom power can easily damage the output stages of your audio device feeding the MXP inputs.



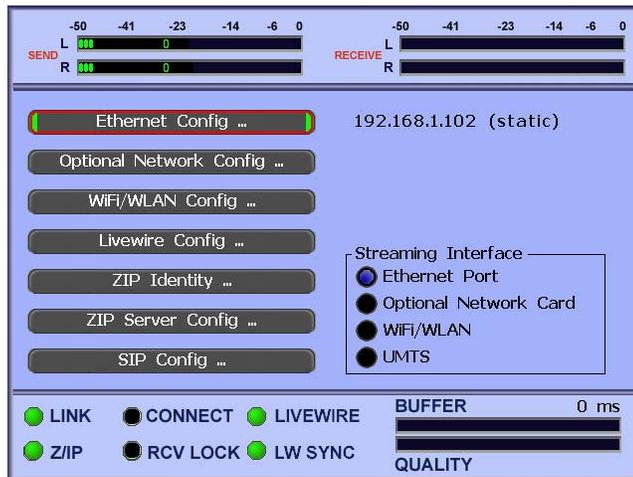
We recommended that you do not connect the unit to your network until you configure the network interface through the front panel. This avoids the possibility of using the same IP address as another device on your network. Duplicate IP addresses are a sure source of weird problems, not to mention unpleasant calls from the IT department.

Step 2: Configure the Network Interface

Turn on the power switch on the rear of the unit. The splash screen (logo and background) will appear for a short time followed by the main menu. When the menu appears, navigate to the “Network” option using the arrow keys. Press the “OK” button to select.



In the Network sub-menu select “Ethernet Config” then press the OK button to enter the information about your network and the unit’s IP address.



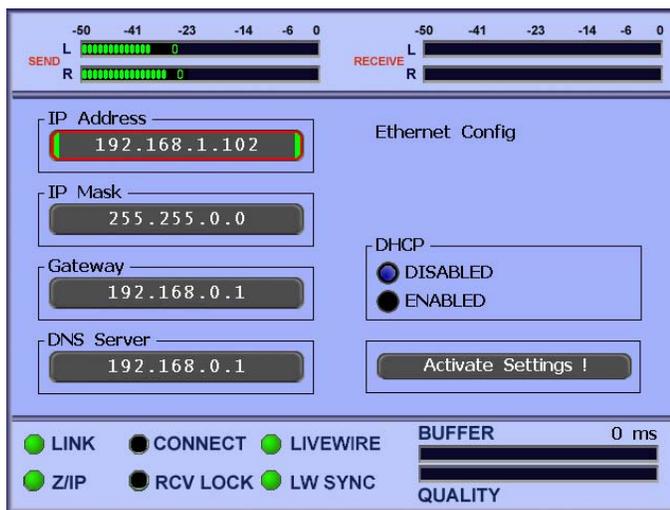
There are two ways to assign an IP address to the Zephyr/IP: either a static address supplied by your IT department or by DHCP if you have a DHCP server on your network. If you wish to use a static IP address, enter it in the IP Address field and make sure the DHCP option is DISABLED. If you use DHCP then leave the IP Address as is.

Next, enter the subnet mask and the gateway IP address (contact your IT department for these as well). If you do not have an IT department, on the majority of installations the subnet mask will be 255.255.255.0 and the gateway is the IP address of your router. One simple way to double check this information is to view the network settings on a PC on the same network.



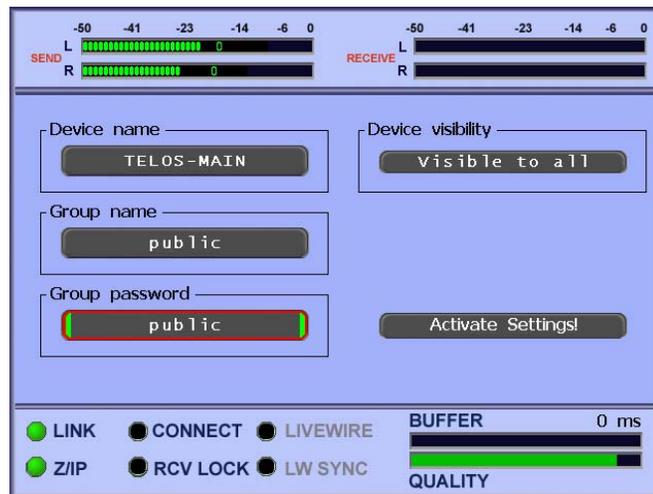
Use the cursor keys to navigate to the field you want to change then press the OK button to edit the field. While you are editing a field, use the keypad to enter the data. Use the UP arrow to erase any mistakes. Press the OK button to save your changes or ESC to discard them.

Make sure you “Commit” changes after entering all of the information on this menu then press ESC to return to the Network sub-menu.



Step 3: Configure the Z/IP Server Settings

On the Network sub-menu, select the Z/IP Identity option. The following dialog is displayed:



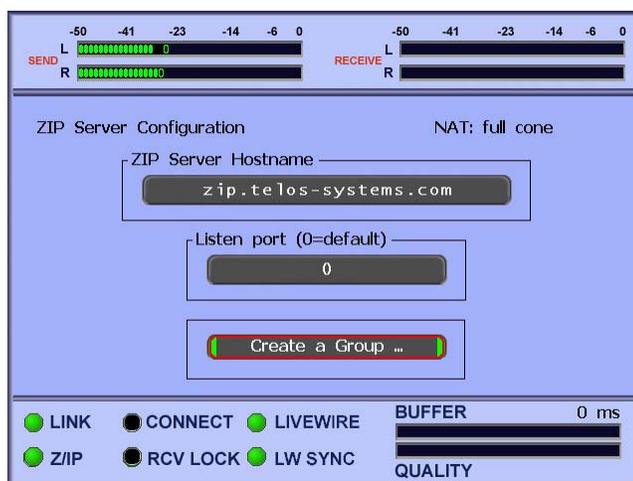
In this dialog you enter a name for your unit and the group to which this unit belongs. The "public" group is a default group that anyone can use (the password is also "public"). You may create a new group at any time. Generally a group represents your organization but you can use any group name you like¹.

The unit name together with the group name forms the "phone number" for the unit. This is the "number" you give out and how others can call your Z/IP regardless of what IP address you have at the moment.

The unit name must be unique within your group. If the name you happen to select is already in use the server will return a unique name by appending a number to the name. If the unique name is acceptable you may use it; otherwise try another name.

The visibility option determines if your unit will be visible to others in the directory listing. There are three choices here. The first, "visible to all" is just what the name indicates; anyone will be able to see the name and the group of your Z/IP. The second, "group visible" allows only members of your group (those that know the group password) to see your Z/IP. The last option, "hidden" is just that; your Z/IP does not appear in any directory listings. Please note that this option only affects the directory listing. Anyone is still able to call you regardless of the choice you make here (just like you continue to get phone calls during dinner time even if you have an unlisted number).

¹ Names are not case sensitive. They may contain alphanumeric characters along with the hyphen (-) and underscore (_) characters.

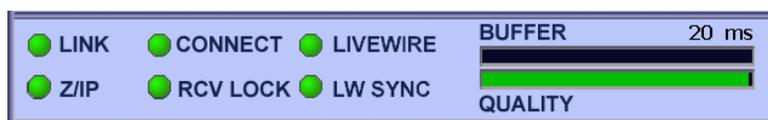


Now, press ESC to back up to the Network menu and then enter the Z/IP Server Config sub-menu. Here, you can set a TCP/IP port for your device to listen on if you are using “port forwarding” on your NAT. The Listen port determines what port the Z/IP will use to accept messages from others. The default value of 0 tells the Z/IP to assign a port itself. This setting works best for most cases. You may need to change this value if you are behind a very restrictive NAT and others have difficulties reaching your device. The "How do I use port forwarding with the Z/IP?" section on page 74 describes how to configure port forwarding.

Press ESC to exit the Z/IP Server configuration dialog.

Step 4: Connect to the Network

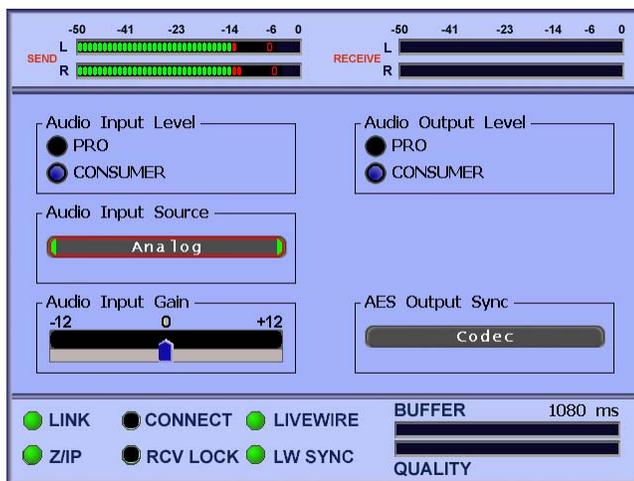
With the network configuration completed, you are now ready to connect to the network. Plug your network cable into the Ethernet jack on the back of the unit (labeled “Livewire 10/100”). Make sure to use a CAT5e or CAT6 cable. After connecting to you LAN, check the “Link” light on the front panel status bar (bottom of the user interface).



This light will be green if you are connected to an active network. The Z/IP indicator on the status bar turns green to indicate that you have a connection to the Internet, and that the unit is in contact with the Z/IP server. If either of these lights is not green, verify your Ethernet settings on the network menu. Check with your IT department or have a look at the "When you don't have an IT department" section.

Step 5a: Configure Studio Unit Audio Settings

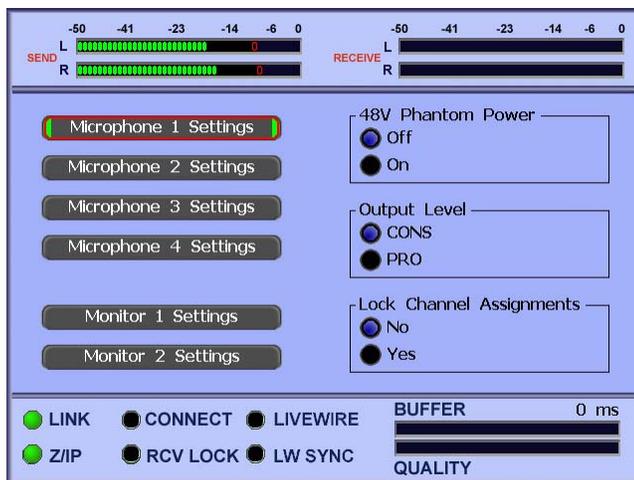
Select the Audio option on the Main Menu screen (press ESC a few times, if you're not on the Main Menu screen). Press OK to select. The following dialog will be displayed:



Select the appropriate options depending on your audio connections (Analog or AES/EBU inputs, AES/EBU sync, analog nominal audio levels you are using on the inputs and outputs). Press ESC to exit the dialog when done.

Step 5b: Configure MXP Unit Audio Settings

Select the Audio option on the Main Menu screen (press ESC a few times, if you're not on the Main Menu screen). Press OK to select. The following dialog will be displayed:



Use the arrow and OK buttons to choose the appropriate settings the analog XLR output level. For now do not lock channel assignments. Also, turn on phantom power only if absolutely necessary for your microphones! Navigate to the audio input or monitor output you want to configure. Please note:

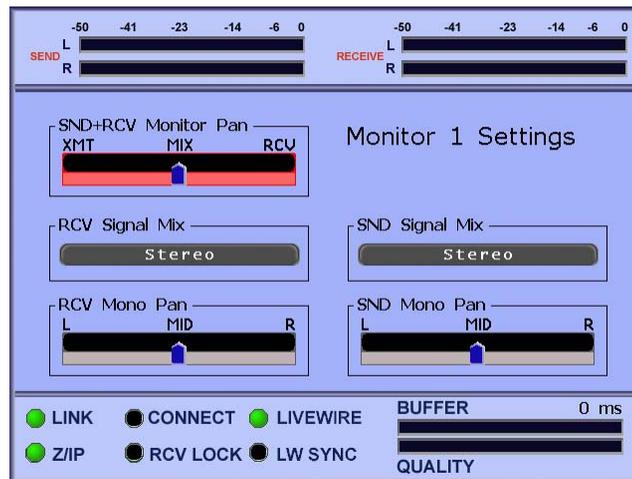
- “Monitor 1” corresponds to the audio sent to the headphone jack on the frontpanel of the MXP unit.
- “Monitor 2” corresponds to the audio sent to the analog XLR and headphone outputs on the backpanel of the MXP unit.

The for microphone settings pages all look identical:



Adjust the input gain level as necessary, keep the “A+B Channel Panning” at center, choose an appropriate audio processing scheme and turn on the low-cut filter if you are using microphones rather than line input.

The two monitor settings pages all look like this:



For now keep all panning sliders in their center position and select “Stereo” for the RCV and SND Signal Mix.

Step 6: Make a Test Call

You are now ready to make a test call to the Zephyr IP test line at Telos. Press the AUTO button on the front panel. The call dialog is displayed:



Navigate to the "buddy list" on the left side of the screen and select TelosHome. You should see a green checkmark next to the name, indicating that it is online. Navigate to the CALL button on the menu. When you press OK the screen will change to the status screen. On the status bar at the bottom of the screen you should see the CONNECT and RECEIVE LOCK lights go green, and possibly some level meters on the receive side. If the connect light stays yellow or blue it indicates that the call failed.

3 Installation

3.1 Rack Mounting the Studio Unit

The Zephyr/IP mounts in a 3RU space in a standard 19" rack. Please note that early versions of the Zephyr/IP were designed to work with "Universal Mounting Rails" per EIA Standard RS-310-C and utilized the "center" holes on most equipment racks: therefore they may not be compatible with all racks (as many rack manufacturers choose to conform to the subset of hole spacing patterns per IEC Recommendation 297). If you find this to be the case with *your* installation, please contact Telos Customer Support for a free set of rack ears and plastic front panel bezels that are compatible with ALL equipment racks. We apologize for the inconvenience.

The Z/IP does not have an internal fan, and does not have any special requirements for space above and below the unit. As long as you keep the stirred air in the rack between 0 and 40 degrees Celsius (32 to 104 degrees Fahrenheit) with a relative humidity of 0 to 98% (non-condensing) the unit will operate as described.

3.2 Power

Install the power cord included with the Zephyr/IP in the marked AC power connector located in the rear of the unit. The internal universal switching supply will accept 115 – 240 VAC input. You should see the graphical display illuminate and display the "boot-up text", rotated 90 degrees. Subsequently the "splash" screen logo will appear, and then the main menu. This process can take about 90 seconds.

3.3 Analog Audio Inputs

Analog Audio XLR Pinout

PIN	DESCRIPTION
1	Ground
2	Signal +
3	Signal -

Studio Version

Install the left and right analog audio cables in the female XLR connectors marked LEFT and RIGHT on the rear panel. The analog audio section accepts audio input with a peak level of

+22dBu. In the Audio/Microphone menus the input can be configured for the following gain settings:

- Line Professional (+4 dBu nominal)
- Line Consumer (-10 dBu nominal)

MXP Version

Install the XLR cables in the female XLR connectors marked INPUT 1...4 on the rear panel. In the Audio/Microphone menus the inputs can be configured for the following four gain settings:

- Line Professional (+4 dBu nominal)
- Line Consumer (-10 dBu nominal)
- Microphone +30 (-40 dBu nominal)
- Microphone +55 (-44 dBu nominal)

3.4 AES/EBU Digital Audio Input (Studio Unit only)

Insert the AES/EBU cable (110 Ohm XLR) in the female XLR connector labeled AES/EBU Input on the back panel of the Zephyr/IP. The Zephyr/IP expects a peak input level of -3dBFS on the digital audio input.

AES/EBU XLR Pinout

PIN	DESCRIPTION
1	Ground
2	Signal +
3	Signal -

3.5 AES/EBU Digital Audio Output (Studio Unit only)

Insert the AES/EBU cable (110 Ohm XLR) in the male XLR connector labeled AES/EBU Output on the back panel of the Zephyr/IP. The Zephyr/IP provides a peak output level of -3dBFS on the digital audio output.

3.6 AES/EBU Digital Audio Sync (optional, Studio Unit only)

Insert the AES/EBU cable (110 Ohm XLR) in the female XLR connector labeled AES/EBU Sync Input on the back panel of the Zephyr/IP. The Z/IP will extract the clock from this input and (if selected in the AUDIO menu) can synchronize the AES/EBU Output audio stream to this recovered clock.

3.7 Network Adaptors

Attach a CAT5e or CAT6 network cable to the connector labeled 10/100BT/Livewire. The network interface is an Ethernet twisted pair 100BASE-T connector.

The standard pinout for an RJ45 10/100BT Ethernet Jack is:

<i>PIN</i>	<i>FUNCTION</i>
1	Transmit +
2	Transmit -
3	Receive +
4	Unused
5	Unused
6	Receive -
7	Unused
8	Unused

3.8 USB Ports

Attach any of the supported USB-network extension devices to one of the ports.

The pinout of the standard USB connector on the Z/IP is:

<i>PIN</i>	<i>FUNCTION</i>
1	+5 Volts
2	Data -
3	Data +
4	Ground

3.9 Parallel Control

The DB25 connector on the back panel provides contact closure (close-to-ground) inputs and outputs. There are 8 open-collector outputs, and 8 open collector inputs, each configurable from the Settings menu in the user interface. The DB25 connector is pinned out as follows:

<i>PIN</i>	<i>FUNCTION</i>
1	+5 Volts DC 400 mA max
2	Output 0
3	Output 1
4	Output 2
5	Output 3
6	Output 4
7	Output 5
8	Output 6
9	Output 7
10	No Connection

11	No Connection
12	No Connection
13	No Connection
14	Input 0
15	Input 1
16	Input 2
17	Input 3
18	Input 4
19	Input 5
20	Input 6
21	Input 7
22	Not Connected
23	Not Connected
24	Not Connected
25	Ground

See chapter 11 below for more detailed information on the Contact Closure operations

4 The User Interface and Setup



4.1 The Front Panel Button Controls

OK Button

The OK button performs different functions depending on context. When an on-screen button is selected, pressing the physical OK button performs the action of the on-screen button.

When an input box is selected, pressing the OK button enters edit mode. Pressing the OK button while in edit mode keeps the changes you have made.

The OK button is also used to activate and select drop down fields.

Arrow Buttons

The arrow buttons are used to navigate the user interface. When pressed, the arrow button change the input focus from one on-screen element to the next.

While editing a field, the UP arrow button works as a Delete/Backspace key to erase data and the LEFT/RIGHT keys change the cursor position within the field.

When the status screen is displayed the UP/DOWN arrows select between the map and other statistics screens.

ESC Button

This button escapes from currently selected menu or dialog screen. While in edit mode, pressing ESC cancels any edits and leaves the field unchanged.

The Number Pad

The number pad is used to enter data in edit fields. If the field accepts only numeric data (or IP addresses) then pressing the buttons will enter the number pressed. For IP addresses, use the # key to enter the dot.

Other fields accept alphanumeric strings. In these fields the buttons cycle though the alphabetic characters in uppercase then lowercase then the numeric value. The 1, * and # buttons allow you to enter special characters.

Key	Characters entered
1	<space> : / @ 1
2	A B C a b c 2
3	D E F d e f 3
4	G H I g h i 4
5	J K L j k l 5
6	M N O m n o 6
7	P Q R S p q r s 7
8	T U V t u v 8
9	W X Y Z w x y z 9
*	* () = %
#	# . , - _

The Connection Buttons

The Zephyr/IP has 3 buttons on the very right side for setting up and dismissing connections, labeled "AUTO", "CONN" and "DISC".

- **AUTO Button:** Press the AUTO button to bring up your "Buddy List". This screen displays the current status of the other Z/IPs so you can see if they are available before you call. You can select one of the entries and dial it directly.

- **CONN Button:** Press the CONN button to bring up the dial screen. Here you can enter an address to call. The same screen also shows a list of previous connections. You may select one from the list and dial it.
- **DISC Button:** Press the DISC button to disconnect any established connections. You will be prompted to confirm the disconnect.

MXP Buttons & Knobs

The top row of the MXP unit's turn-knobs are used to adjust the audio input level.

The buttons between the knobs toggle the channel assignment of the respective mono input:

- **No LED lit:** Input is disabled.
- **"A" LED lit:** Mono input is assigned to the left transmit channel.
- **"B" LED lit:** Mono input is assigned to the right transmit channel.
- **"A" and "B" LED lit:** Mono input is assigned to both transmit channels. The panning is determined by the "Channel Panning" setting in the Audio/Microphone setting menu page.

The bottom row of knobs adjust the volume of the four headphones that can be connected to the unit. Note that "Monitor 1" corresponds to the headphone jack on the frontpanel whereas "Monitor 2" outputs can be found on the back of the unit.

The two buttons in the "Monitor 1" and "Monitor 2" sections toggle the audio selection for the respective monitor output:

- **No LED lit:** Monitor output is disabled.
- **"SND" LED lit:** The monitor outputs the audio received from the far-end.
- **"RCV" LED lit:** The monitor outputs the audio sent to the far-end.
- **"SND" and "RCV" LED lit:** The monitor outputs a mix of transmit and receive audio.

Various monitor panning options for the send and receive audio are available thru the Audio/Monitor menus.



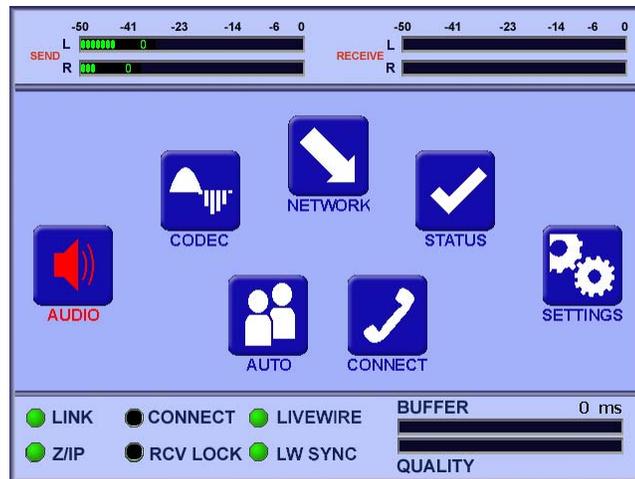
The analog XLR outputs on the back of the MXP unit labeled "MONITOR 2" output the audio that has been selected with the MONITOR 2 switch on the frontpanel. Most notably, it is possible to disable MONITOR 2 XLR outputs by neither selecting SND nor RCV monitoring.

The XLR output level is not affected by the MONITOR 2 volume adjustment knob.

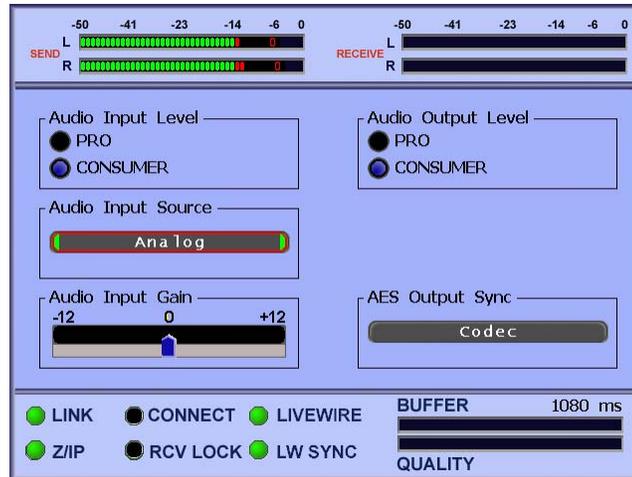
4.2 The Graphical Interface and Menu System

The Zephyr/IP has a full VGA color display to show status information as well as help the user to navigate through the different setup menus. Use the Navigation cluster (arrows, OK, and ESC) to maneuver around the screen. Press “OK” to enter a highlighted sub-menu or to edit a particular user field. Use the arrow keys to select different options from the various radio-buttons, sliders, drop-down menus, and scrolling lists. Use “OK” to confirm your choice and activate the new setting. Some controls will provide a pop-up screen asking you to confirm your choice.

From the Main Menu (below) you can access the Audio, Codec, Network, Status, Settings, Auto, and Connect submenus by selecting the appropriate menu icon and pressing “OK”.



The Studio Version Audio Menu



The Audio menu gives access to the various settings related to audio into and out of the device.

- Audio Input Level: Choose PRO for a nominal *analog* input level of +4dBu. Choose CONSUMER for a nominal *analog* input level of –10dBV.
- Audio Output Level: Choose PRO for a nominal *analog* output level of +4dBu. Choose CONSUMER for a nominal *analog* output level of –10dBV.
- Audio Input Gain: The audio input gain has can provide a digital level adjustment (post ADC or post AES/EBU Receiver) of the input audio from –12dB to +12dB.
- Send Mix: Choose DISCRETE for a stereo send mix. Choose MONO A+B to have the unit sum the two input channels to mono before sending.
- Audio Input Source: Choose Analog or Digital to select the Analog XLR or AES/EBU as the audio input source. Choose Livewire to use the Axia Networked Audio interface as the audio source. Both the Analog and AES/EBU outputs are always active.



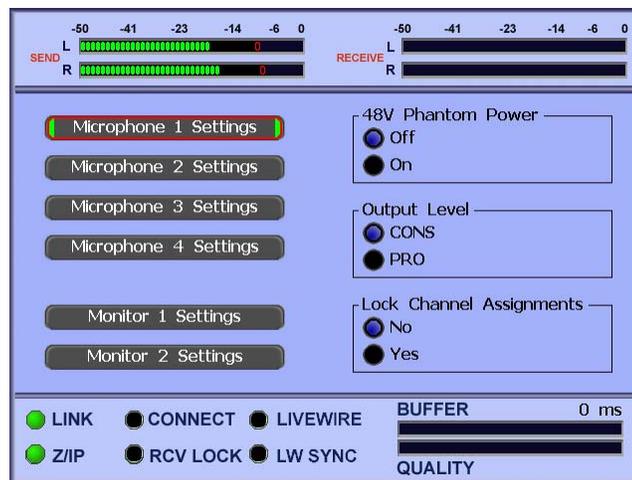
About Livewire: If you decide to use Livewire input you also need to choose a Livewire input stream (“destination”) in the Network/Livewire page.

Livewire output is always enabled provided a Livewire output stream number (“source”) has been selected in the Network/Livewire page.

- AES Output Sync:

- Choose CODEC to have the AES/EBU output samplerate synchronized to the internal samplerate of the unit.
- Choose 48KHz to have the AES/EBU output samplerate set to 48KHz, regardless of the internal samplerate.
- Choose 44KHz to have the AES/EBU output samplerate set to 44KHz, regardless of the internal samplerate.
- Choose 32KHz to have the AES/EBU output samplerate set to 32KHz, regardless of the internal samplerate.
- Choose SYNC IN to synchronize the AES/EBU output to the AES/EBU input.
- Choose SYNC EXT to synchronize the AES/EBU output to the AES/EBU Sync Input.

The MXP Version Audio Menu



- 48V Phantom Power: Turns on or off the phantom power for audio XLR inputs 1 and 2. Phantom power is only intended to be used for microphones which require external power.



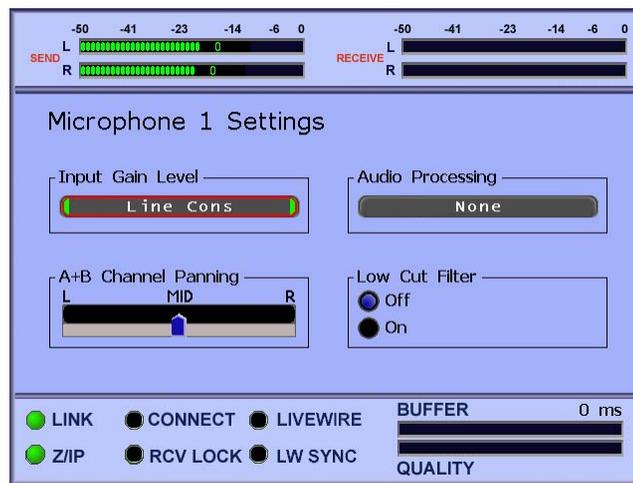
Phantom power is not available on inputs 3 and 4 !

It is a good idea to always turn off phantom power unless absolutely necessary. If you switch the MXP's audio inputs to line level and connect an audio device like a CD-player or Axia Analog Node then phantom power can easily destroy the analog output drivers of these units!

- Output Level: Choose PRO for a nominal *analog* output level of +4dBu. Choose CONSUMER for a nominal *analog* output level of -10dBV.
- Lock Channel Assignments: When turned on the frontpanel buttons for the microphone A/B channel assignments and the monitor SND/RCV assignments are locked at their current setting. This feature helps to prevent that accidentally touching one of these assignment buttons kills the audio being transmitted to the studio.

Microphone Settings

All four “Microphone Settings” menus look alike:



- Input Gain Level: Switches analog input levels to professional (“Line Pro”) or consumer (“Line Cons”) line level or +30 dB (“Mic +30dB”) or +40 dB (“Mic +40dB”) microphone level.
- A+B Channel Panning: If the channel assignment for this input is set to A+B (both “A” and “B” LEDs lit for this channel on the frontpanel) then this menu slider allows to continuously pan the mono input to the left or right transmit channel.
- Audio Processing: This menu selection allows you to enable the built in AGC/Limiter (processor) for the selected input. The built in Omnia processor is quite sophisticated and offers the following options:
 - None: This disables the input processor for this channel.
 - Voice Low: This is the least aggressive setting, intended to protect against minor level problems when running a live show. Provides AGC with no limiting. Ideal where you want the most natural sound in live situations where mixing could be difficult.
 - Voice Medium: This is a moderate setting. It combines AGC with a small amount of limiting. This provides good dynamics control, and serves to

"beef up" the voice. This setting is the most frequently used general purpose setting for voice.

- Voice High: This is an aggressive setting employing both AGC and limiting. This setting is perfect for easily excited talent such as sportscasters.
- Music: This setting offers a slow AGC only.

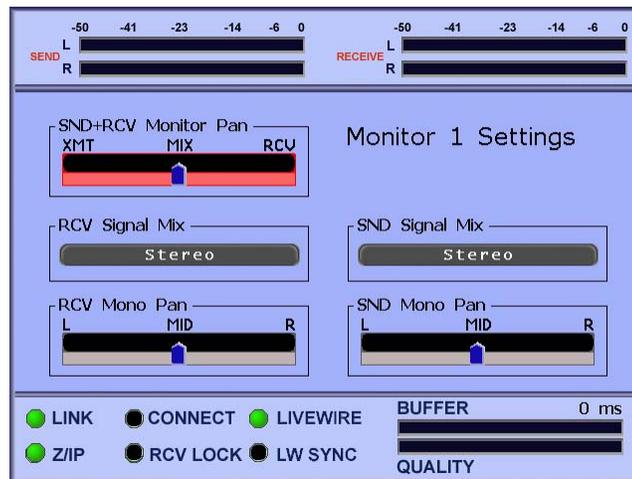


Please don't use the "voice" processor settings if your source includes musical material. The fast time constants used in the Voice Medium and Voice High settings will cause noticeable artifacts if used on most music.

- Low Cut Filter: This is a low cut (pop) filter designed to reduce wind and breath noise. Its characteristics are as follows: Cut off frequency: 80 Hz, Slope: 3 dB per octave.

Monitor Settings

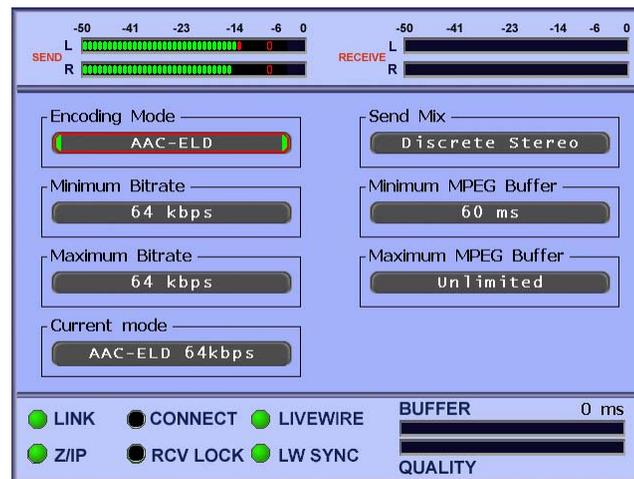
Both "Monitor Settings" menus look alike:



- SND+RCV Monitor Pan: If the monitor selection on the frontpanel is set to both receive and transmit (Both "SND" and "RCV" LEDs lit for this monitor on the frontpanel) then this slider can be used to adjust the volume balance between the transmit and receive audio.

- **RCV Signal Mix:** Affects how the receive audio is sent to the monitor output: “Stereo” preserves the original stereo image, “Mono L+R”, “Mono L” and “Mono R” create a mono mix from the corresponding receive audio channels.
- **RCV Mono Pan:** If the “Receive Signal Mix” is set to one of the mono modes then this menu slider allows to continuously pan the mono receive mix to the left or right monitor output.
- **SND Signal Mix:** Affects how the transmit audio is sent to the monitor output: “Stereo” preserves the original stereo image, “Mono L+R”, “Mono L” and “Mono R” create a mono mix from the corresponding transmit audio channels.
- **SND Mono Pan:** If the “Transmit Signal Mix” is set to one of the mono modes then this menu slider allows to continuously pan the mono transmit mix to the left or right monitor output.

The Codec Menu

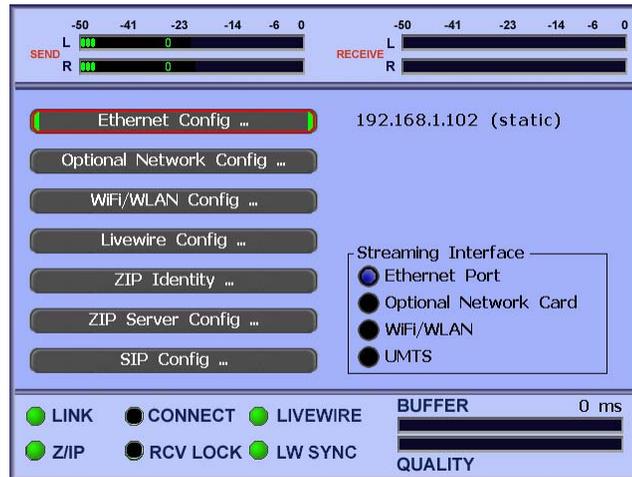


The Codec menu allows the user to change various settings related to the audio and transmission quality as well as select the appropriate compression scheme.

- **Encoding Mode:** The Zephyr/IP supports AAC, HE-AAC, HE-AAC-V2, HELD-AAC, AAC-LD, G711 and G722.
- **Minimum and Maximum Bitrate:** You can set limits on the range of bitrates available to the encoder when it needs to adjust for various network defects. The wider the range, the greater the flexibility of the encoder to “fine-tune” your connection and audio fidelity.
- **Send Mix:** The user can force STEREO or MONO or use AUTO to let the unit choose the best mode for a given bitrate and encoding mode setting.
- **Minimum and Maximum MPEG Buffer:** These two numbers specify the minimum and maximum decoder buffering in milliseconds. For optimum performance you should set these values to 0 ms and Unlimited. Note that if you change the buffering

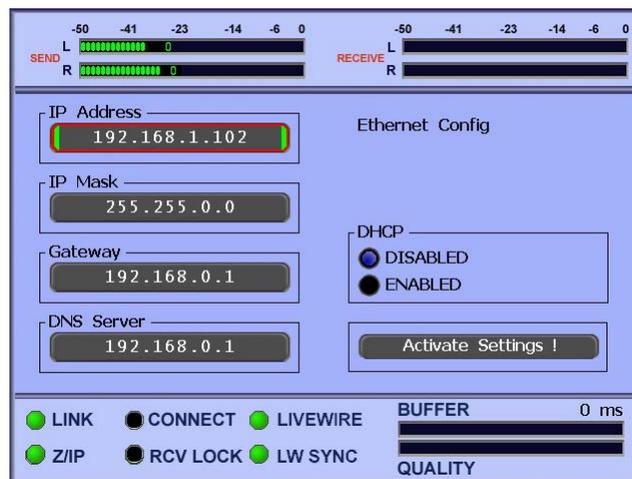
while a call is in progress you will be notified that the changes will only take effect after the call is reconnected. Furthermore, the buffering only applies to MPEG codec modes but not to G.711, G.722 and PCM.

The Network Menu



The Network Menu gives a list of various network related sub-menus:

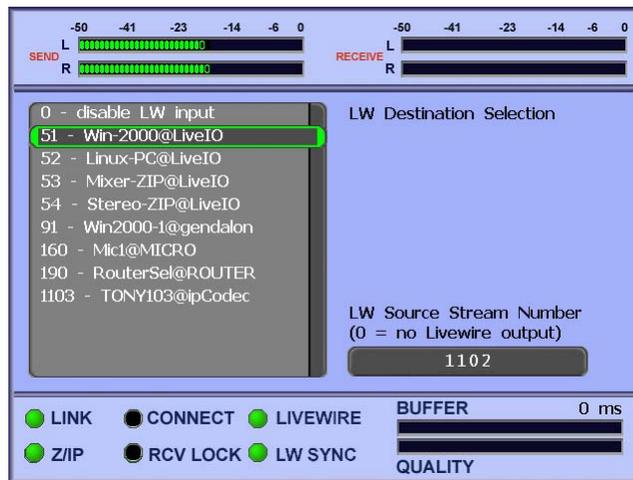
- **Ethernet Config:** Use this menu to set your *wired* network connection for the port on the back of the unit. This port supports either static or DHCP controlled network settings.



- **Static Setup:** Supply an IP-address in the first box, a valid netmask of your local network, the gateway and a domain name server. Navigate to the “Commit Changes” button on the right side of the screen and press OK.
- **DHCP Setup:** Enable the DHCP radio button on the right side of the screen. Navigate to the “Commit Changes” button on the right side of the

screen and press OK. If you later disable the DHCP, the unit will revert to the last static IP settings entered.

- **Optional Network Config:** This page is used to set your network configuration for the optional secondary network interface that you may have installed in one of the PCI slots in the Zephyr/IP. The configuration method is identical to the Ethernet Port; just make sure you give a unique IP address to this port.
- **Wi-Fi/WLAN Configuration:** This sub-menu is used to configure your USB wireless device.
 - DHCP Hostname: Enter the IP Address of the Dynamic Host Configuration Protocol server name.
 - ESSID Network Name: Enter the name of the Wi-Fi network you are joining.
 - Encryption Key: If the Wi-Fi network has encryption enabled, enter the key here.
 - Commit Changes: After setting up your Wi-Fi options, press the Commit Changes button to submit your settings.
- **Livewire Config:** This sub-menu is used to configure your Livewire input (“destination”) and output (“source”) streams.



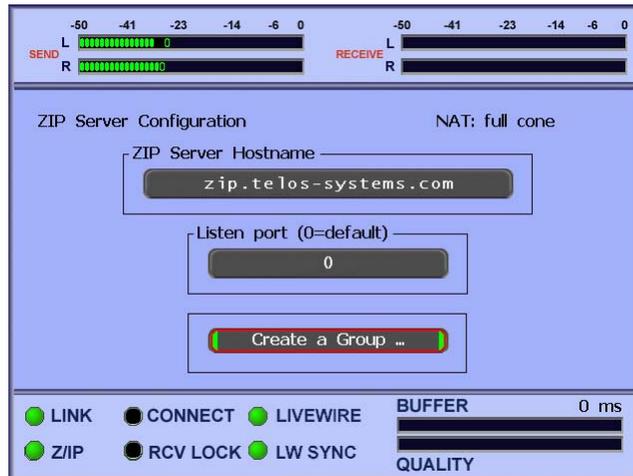
- LW Destination Selection: This list box shows the available Livewire streams in your network. After bootup it may take a few seconds until all available streams have been detected. Browse to the desired stream to select it as your Livewire input.
- LW Source Stream number: Enter 0 to disable Livewire output. Enter a stream number in the range 1 – 32000 to generate a Livewire stream. This stream will always be active.



To actually use the selected Livewire input stream as your audio input you must also change your audio input device in the Audio menu to “Livewire”.

VERY IMPORTANT: If you select a Livewire input stream other than 0 on your MXP unit then this stream will replace the stereo send mix of all four analog inputs! In addition, the frontpanel INPUT LEDs will be disabled to indicate that these inputs are no more active. The MONITOR LEDs will be locked in the RCV position.

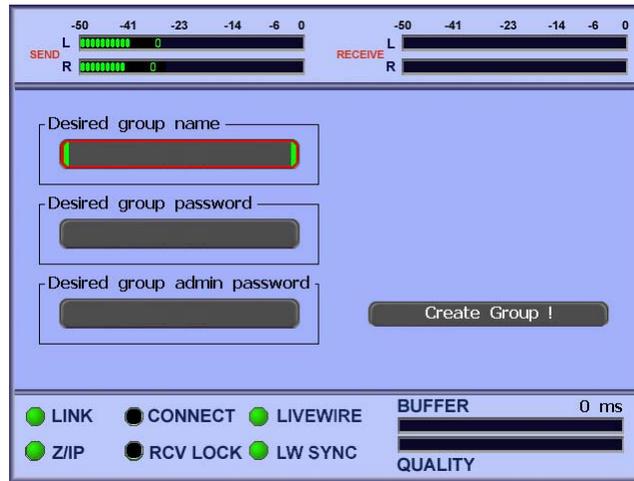
- **Z/IP Identity:** This sub-menu is used to register your Zephyr/IP on the Z/IP Server.
 - **Z/IP Device:** Use the keypad to enter a unique name for your Zephyr/IP. You will share this name with your peers so they can see your online status and call you. Don’t worry if you pick a name that another user has already chosen: The Z/IP server will append a number to your name and display it accordingly.
 - **Group Name:** Use this field to register with a particular group that has been created on the Z/IP server. The default is “public” which allows your Z/IP to be contacted by anyone in the network. If you have created a private group on the server, enter the name here.
 - **Group Password:** The default is “public” for the public group. If you are registering with a private group, enter the password here.
- **Z/IP Server Config:** This sub-menu allows you to select the appropriate Z/IP server with which to register. Additionally, you can change the TCP/IP port to use if your unit is behind a particularly stubborn NAT. Finally, this sub-menu allows you to “Create a Group” on the Z/IP server to make it easier to organize your device and those of your regularly contacted peers.



- **Z/IP Server Hostname:** Use this field to enter the name of the Z/IP Server you will be connecting to. The unit defaults to one of the Telos-maintained servers, (you can use zip.telos-systems.com if you another default value is not present), but you can change to a private server if you have one. You may also specify a port number by appending the port number to the name

separated by a colon. This is useful if the server is not operating on the default port of 24,308.

- Listen Port: Use this field to select a particular port on your Ethernet router to listen to for Z/IP communications. The default is “0”. Contact your IT Administrator for more information on this setting if you have special conditions under which you need to operate your Internet traffic.
- Create a Group: Select this option to go to the Group Creation screen. Here you will enter the desired name for your group, the group password that users will enter to join (and search) the group, and the Admin password for the group.



- **SIP Config:** Use this page to enter the SIP Server Hostname if you will be calling SIP devices on the network.

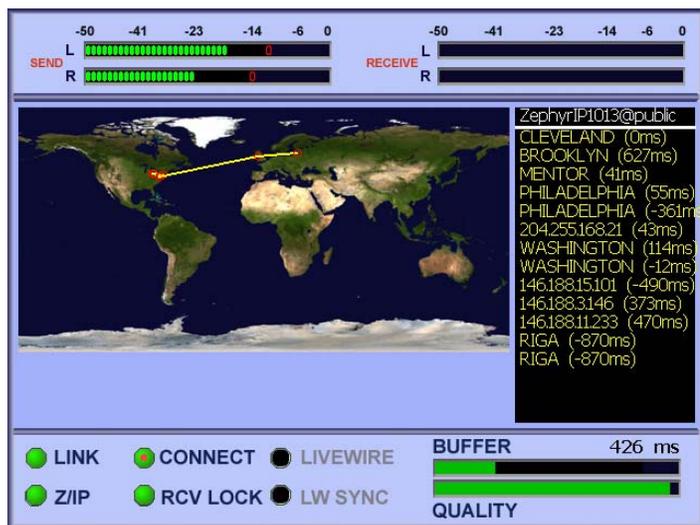
To ensure the best performance of your Zephyr/IP it is recommended to setup a port forward for any unit in the studio to a free port and set this port in the Zephyr/IP Server Configuration page correspondingly. You do not need a port forward for any unit outside your network that connects to units in that network.

The Status Menu

The status menu consists of three different screens. The Map screen gives an approximate overview of the routing of your Zephyr/IP call. The Graph screen gives a graphical representation (in various timescales) of various statistics indicating the network quality during a “call”. The Text screen gives real-time information about network statistics, current codec settings, and system data.

- **The Map Screen:** This screen shows the path taken among the interconnected gateways between the two connected Zephyr/IPs and the “PING” times between each successive network hop. The screen uses a program called “traceroute” (see section 9.5 below) to get a list of the IP Addresses of each “hop” taken when the connection is established. These IP Address are then correlated with a database of

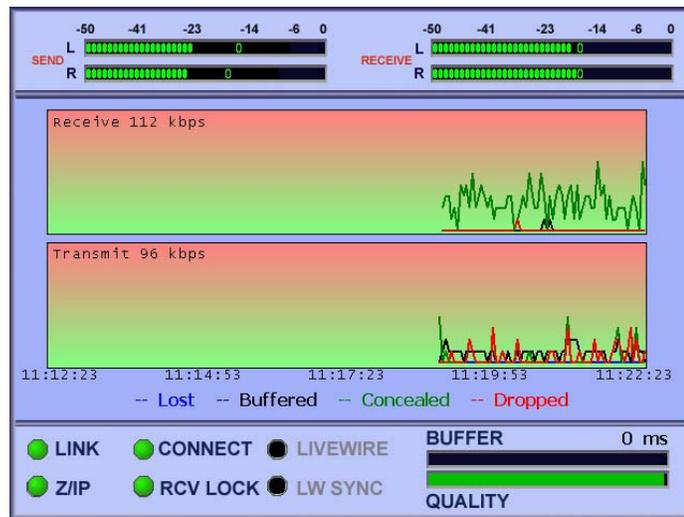
the geographic location of each router, and then the entire route is plotted on the map. NOTE: each packet transmitted and received can take a completely unique route through the net, but this screen gives a general indication of the route, including the network speed of each hop (represented by the Ping time: higher numbers indicate slower hops).



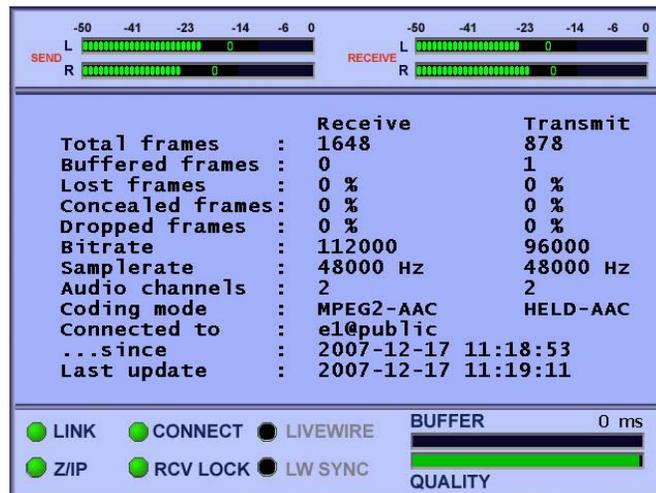
- **The Graph Screen:** The 2 graphs on the graph screen display 4 statistics about the network connection over time. The top graph shows information about the Received data stream, and the bottom graph shows information about the Transmitted stream. The four items displayed are:
 - Lost Packets: The percentage of frames in a particular time interval that were either lost or arrived too late in transmission for the decoder to utilize.
 - Concealed Packets: The percentage of frames that were concealed by the decoder due for any reason (lost, dropped, inserted due to clock skew).
 - Dropped Frames: The percentage of frames dropped by the decoder because of buffer overflows (clock skew from transmitter to receiver).
 - Buffered: The number of packets in the buffer at a particular time.

Generally speaking, as the graph lines approach the top of the graph, this indicates poor performance over the network (more packets lost, dropped, or concealed, and more buffering inserted to correct for these errors).

To view the data in different timescales use the Left and Right arrow keys to zoom in and out. The scales available are 10 Hours, 1 Hour, and 10 minutes.



- The Text Statistics Screen: This screen gives detailed real-time information about the network quality by explicitly reporting lost and dropped MPEG frames, concealed frames, and the size of the audio data buffer. These four values constitute the major part of the decision process of ACT™ - Agile Connection Technology.



- Total Frames: The number of frames transmitted and received during a particular call.
- Buffered Frames: The number of frames in the buffer at both ends of the connection.
- Lost Frames: The percentage of frames lost or late.
- Concealed Frames: The percentage of concealed frames (lost, dropped, and inserted).

- Dropped Frames: The percentage of dropped or late frames due to network congestion.
- Bitrate: The data rates currently being used by the encoders at either end of the connection.
- Samplerate: The audio sampling rate being used by the encoders.
- Audio Channels: The number of discrete audio channels being sent in the data streams.
- Coding Mode: The currently used coding mode for transmission (in either direction).on
- Connected To: The name or IP address of the unit at the other end of your connection.
- ...Since: The time of the call origination.
- Last Update: Indicates the data and time of the last update of the information on the screen.

The Settings Menu



The settings menu contains all menus to configuring the Zephyr/IP for the user's convenience.

- **Frontpanel Config:** Takes you to the frontpanel configuration screen. It allows you to choose a frontpanel backlight timeout and to disable the button keyclick as well as connect/disconnect sounds.
- **Security Config:** Takes to the security screen where you can specify the HTML access password. Note that the username which needs to be given in you browser's login-box is always "user".
- **Time Config:** Takes you to the date/time configuration screen. You can specify an explicit date/time or a NTP server IP address or hostname. Timezone numbers must be given in minutes east of Greenwich. I.e. Cleveland is at -5 hrs = -300.

- **Parallel Port Config:** Takes you to the Parallel Port configuration page. For more details see section 11.1.
- **Reboot:** Takes you to the reboot page where you can shutdown any connections and reboot the unit.
- **About:** Displays information about the unit, CPU temperature, software versions, etc.
- **Auto Answer:** Set to ON to have the unit automatically accept any incoming “calls”.
- **Redial lost connections:** When enabled a broken audio connection will automatically be redialed the specified amount of times. These dial attempts will be repeated every 45 seconds.
- **Audio Loop:**
 - **Hardware-loop:** loop the audio input source (Analog or AES/EBU) back to the analog and AES/EBU audio outputs. Note that Livewire input will not be looped back out to the outputs. Furthermore, the frontpanel RECEIVE level meters will not be activate in Hardware loop mode. Finally, the input level adjustment knobs of a Mixer Unit will not affect the looped-back audio.
 - **Codec-loop:** loop the encoded audio directly back to the decoder. This will also work for Livewire input audio.
- **Send logs per email:** If you enter an email address in the text box an email will be sent to this recipient. The unit uses a GMX email account to send the email. Your firewall must be configured to allow outgoing SMTP connections. Typically, you will enter the Telos support email in case of problems.

5 The Web Interface

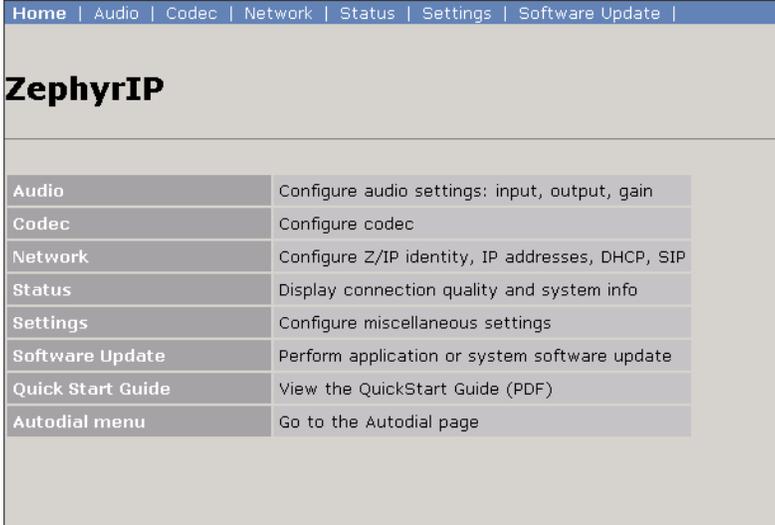
5.1 How to Access the Web Interface

From any internet browser on your network you should be able to access the internal web pages of the Zephyr/IP. Simply open the browser window, and type the IP address of the Z/IP you are trying to contact. You will be prompted to enter a user name and password. The user name is "user" and the default password is "Telos" (case sensitive, without quotes). You can always check or change the web password from the Settings dialog on the Z/IP's front panel.

5.2 What Can I Do on the Web Interface?

From the Z/IP web interface, you can configure most of the options that are available on the Graphical User Interface, plus some that are not. The following pages are available from the web interface:

Main Menu

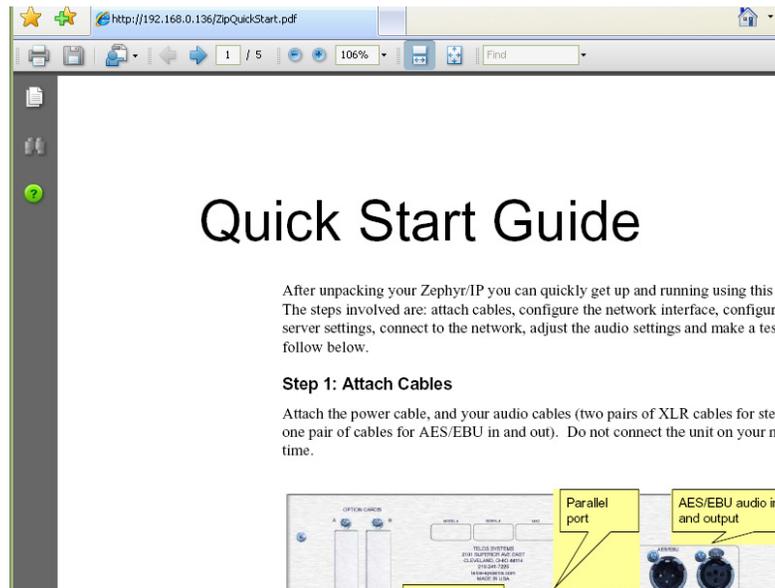


Home Audio Codec Network Status Settings Software Update	
ZephyrIP	
Audio	Configure audio settings: input, output, gain
Codec	Configure codec
Network	Configure Z/IP identity, IP addresses, DHCP, SIP
Status	Display connection quality and system info
Settings	Configure miscellaneous settings
Software Update	Perform application or system software update
Quick Start Guide	View the QuickStart Guide (PDF)
Autodial menu	Go to the Autodial page

From this menu you can view the available sub-menus. Click on one of the links to go to that menu.

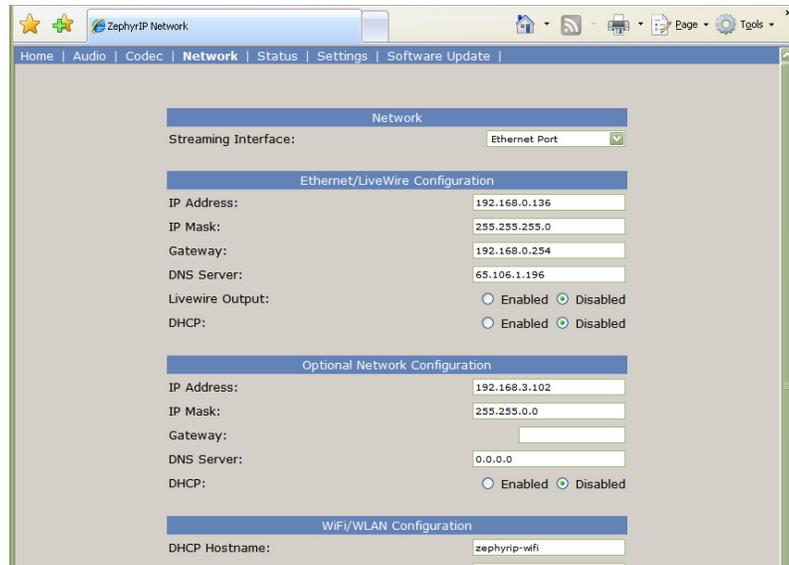
QuickStart Menu

This link opens a PDF copy of the QuickStart Guide in your browser window.



Network Menu

This menu allows you to enter all of the Network Settings and Z/IP Server parameters for your device. This can be quite useful (once you have entered the IP Address in the front panel user interface of the unit) as many of the parameters used by the Z/IP (device identity, DHCP hostnames, etc.) are easier to enter using a keyboard than through the numeric keypad on the front of the unit.

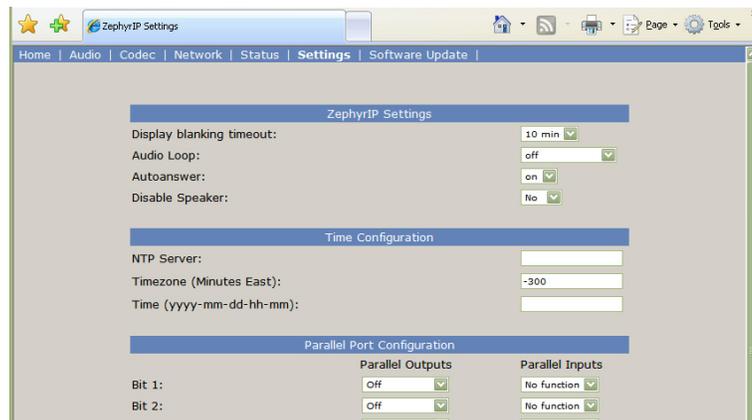


Keep in mind that if you change the IP Address of your unit through the web page, you will need to reconnect to the device using the new IP Address.

After you enter any information in this page you must press the “APPLY” button at the bottom of the page to activate the changes.

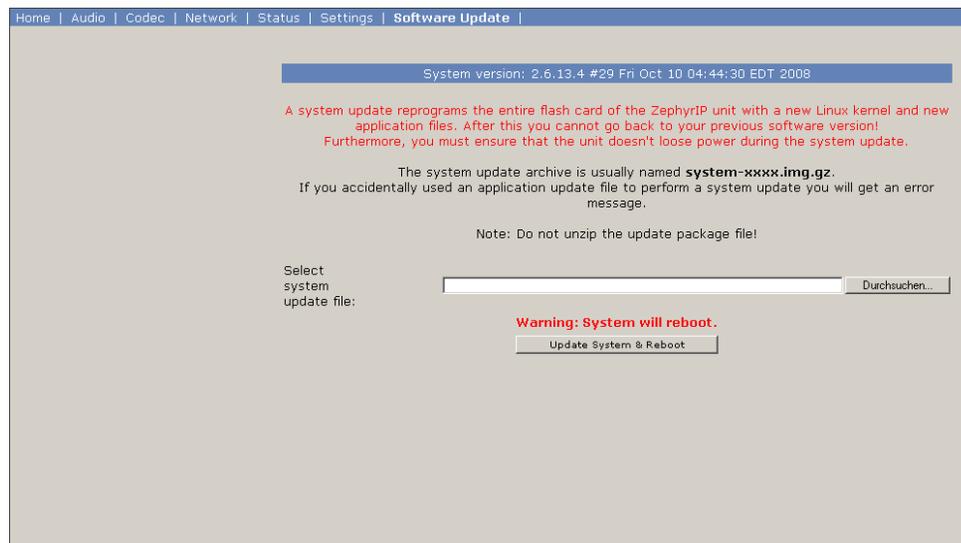
Settings Menu

This menu allows you to change the various utility functions of the Z/IP (speaker, display timeout, auto answer, and diagnostic loop modes). Additionally, you can set the NTP server information from this page. The parallel port configuration is also accessible from this menu. Finally, you can select which firmware bank you would like to run from after you have uploaded new application firmware to the box. This allows you to “try out” different versions of software before committing to a new update.



Software Update

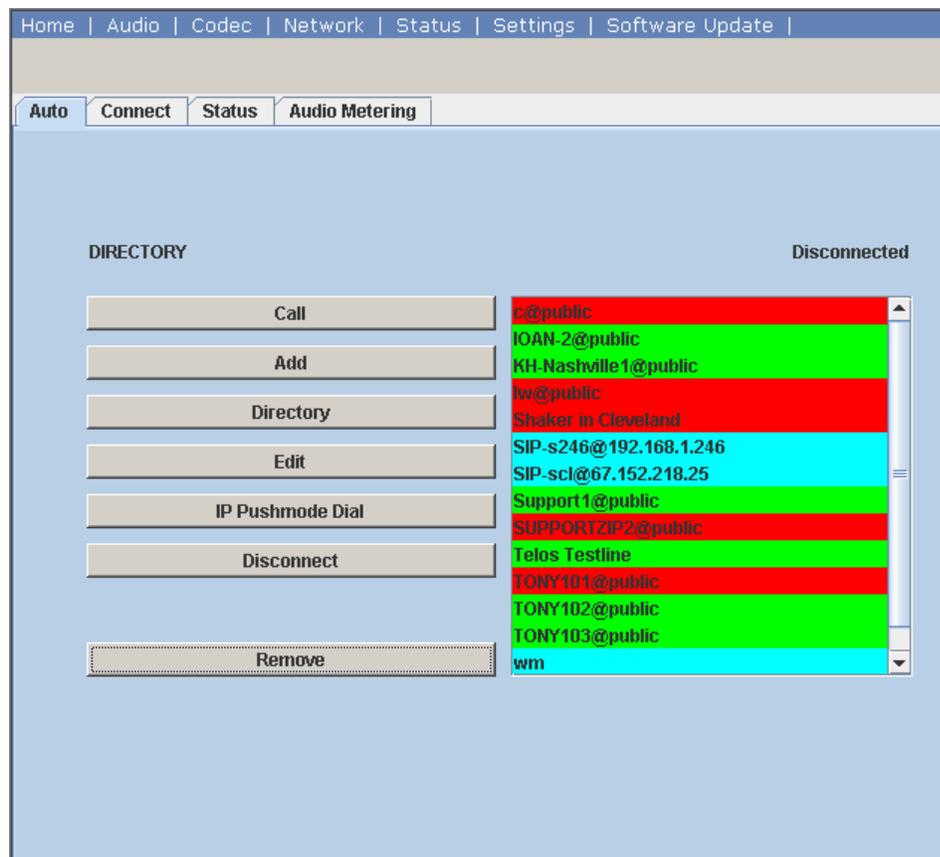
This menu allows you to update the software contained in the Zephyr/IP.



The method will upgrade the entire system. Download the system upgrade file from the Telos website and save it to your local computer. Use the “Browse” button to locate the file and select it. Click the “Update System and Reboot” button to upgrade the unit. The Z/IP will retain all of its settings (IP Address, Z/IP Identity, etc.) after rebooting, but any firmware versions you may have downloaded to bank 0 or 1 will be gone. Only the firmware version included in the system upgrade will be present in bank 0.

Auto Dial Menu (Java Interface)

This menu allows you to use the Zephyr/IP in the same manner as from the front panel. For details read chapter 6 and 8.

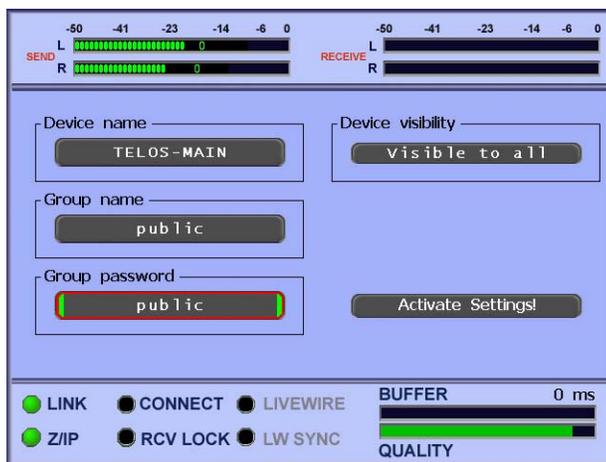


6 Making Connections with Other Units

Obviously, the main job of the Zephyr/IP is to make high quality audio connections with other units in remote locations, usually over the internet. This section will help you to set up your Zephyr/IP, create useful lists of other units, and make reliable connections to them.

6.1 Creating a Z/IP Identity on the Z/IP Server

The first step in connecting with other units is to create a Zephyr/IP Name for your unit on the Z/IP server:



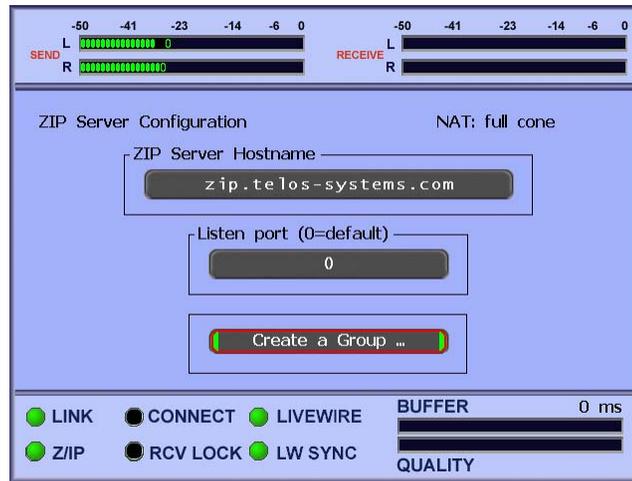
1. From the front panel user interface, navigate to the Network menu, and then to the Z/IP Identity submenu.
2. In the “Device Name” field, enter a name for your unit that will help identify it to other users.



Don't worry if you enter a name that has been chosen by another user: the Z/IP server will generate a unique name by appending a number to the end of the name. If you don't like this new auto-created name, simply enter another choice.

3. Enter the GROUP NAME and GROUP PASSWORD if you are not going to be part of the *Public* group on the Z/IP server.
4. Select the desired level of “visibility” for your device. The visibility option determines if your unit will be visible to others in the directory listing. There are

three choices here. The first, "visible to all" is just what the name indicates; anyone will be able to see the name and the group of your Z/IP. The second, "group visible" allows only members of your group (those that know the group password) to see your Z/IP. The last option, "hidden" is just that; your Z/IP does not appear in any directory listings. Please note that this option only affects the directory listing. Anyone is still able to call you regardless of the choice you make here (just like you continue to get phone calls during dinner time even if you have an unlisted number).



5. ESC back one menu and then enter the Z/IP Server Config Sub-menu. Check to make sure that a valid Z/IP Server Name has been enter in the Z/IP Server Hostname field. "**zip.telos-systems.com**" is the default server name, but you may have your own Z/IP Server configured elsewhere.
6. You have now configured your unit properly to identify itself to the Z/IP server, and to other users.

6.2 The Buddy List

The Zephyr/IP has a nifty way of managing your list of commonly used contacts: The Buddy List in the Auto Menu screen. Press the Auto key on the front panel, or navigate to the Auto Menu on the main screen. On the left side of the screen you will see a list of other units and (possibly) the online status of each unit.



There are 3 symbols used to indicate the status of the units in your list: the checkmark (✓) indicates the unit is online; an “X” indicates that the unit is *not* currently online; the “?” indicates that the Z/IP server is currently unreachable or it does not know about the device (perhaps the other Zephyr/IP changed names or groups).

Press the OK button when you have navigated to the Buddy List, and use the up and down arrows to find the unit in the list that you would like to call. Press OK to select the unit, and then navigate to the “CALL” field on the right side of the screen. Click OK to call the unit.

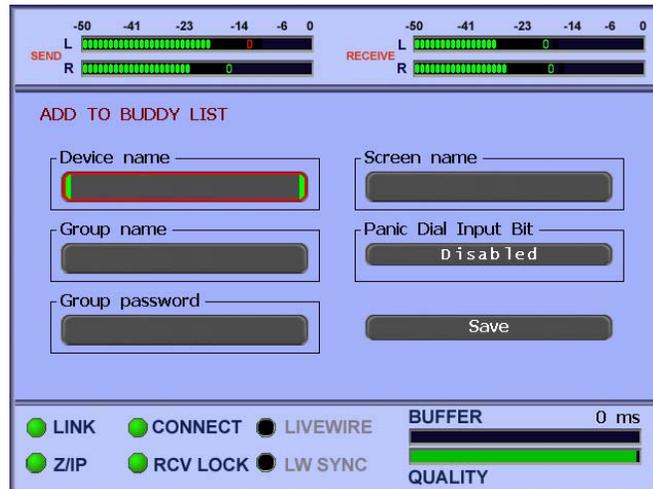
You can also delete old, unused, or incorrect Buddy’s from your list by using the Remove button on the screen. Select the Buddy from the list, and then hit the Remove button.

Add a Buddy to Your List

There are two ways to add a unit to your buddy list. The first method is to find the unit in the directory listing screen and then add it to the buddy list from there. This is useful if you don’t know the exact name or spelling of the unit name, and may be faster than typing the name of the unit from the front panel. The second method is to enter the unit name and group yourself.

Manual Method

To add an entry manually, click the "Add" button. The Add dialog will be displayed.



Enter the device name, group name and group password. If the unit is a member of the "public" group you may leave the password blank.

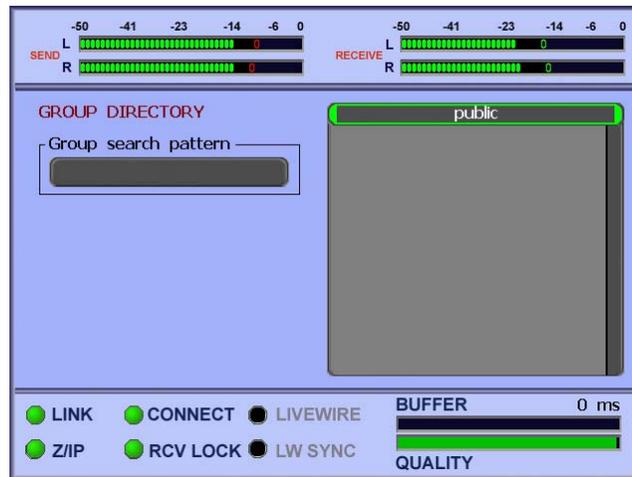
Now, enter the name of the entry as you would like it to appear in the buddy list. If you leave this blank the device name will be used as the buddy list entry name.

If you would like this Buddy to be connected to one of the Panic Dial pins on the Parallel Port on the back panel of your Zephyr/IP, assign it to one of the 8 inputs pins using the Panic Dial Input Bit field. NOTE: You must also enable this pin for Panic Dial functionality from the Settings/Parallel Port submenu.

Click the Save button to save the entry to the buddy list. Press the AUTO key on the front panel to return to the AUTO menu. If you have entered a valid unit name in the DEVICE NAME field, you should now see the new entry and the status of the unit in your list. If the status appears as a question mark (but you have a green light for the Z/IP server connection) then there is a problem with the device or group name entered. The server does not know about this device. Check the device and group names for possible misspellings. You may also try to find the device in the directory listing perhaps using a wildcard or soundex search.

Directory Method

You can add a unit to your buddy list directly from the directory listing screen. Click the Directory button on the buddy list screen. The following dialog will be shown:



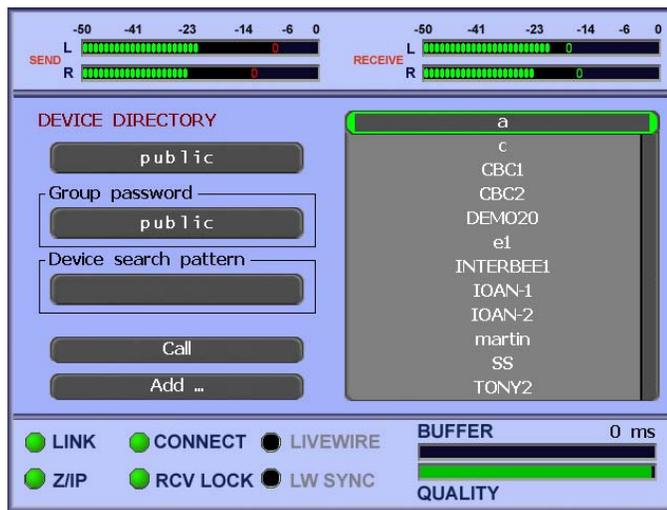
On the right side of the screen, you will see a list of the various groups on the Z/IP Server. If you see the name of the group in which you would like to search, select it from the list to enter the Device Search screen. If not, enter the first few letters of the group name in the Group Search Pattern field and press OK. The list will now be populated only with those group names that begin with those letters.



When searching for groups or devices by name, entering the first few characters will return all names that begin with those characters. The directory also supports soundex² searches which are useful when you're not sure of the exact spelling of the name. Adding a % character to the end of a name tells the server to perform a soundex search.

² Soundex is a phonetic algorithm for indexing names by the way they sound in English.

Select the appropriate group from the list to enter the Device Search screen.



If you know the password for the selected group then enter it in the Group password field. If you do not enter a password then only the devices that are publicly visible will be displayed.

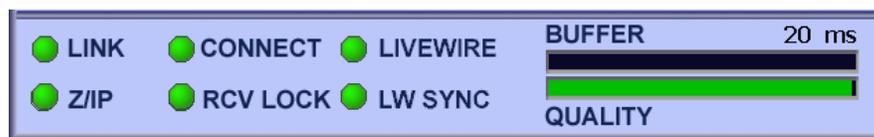
Now enter a search pattern in the Device Search Pattern to limit your search, or leave it blank and press OK twice on this field to see the first 100 or so devices in the group, listed alphabetically.

Select the device name from the list once you have located the appropriate name.

You can now add the device to your buddy list by clicking the “Add ...” button.

6.3 The Status Bar

The Zephyr/IP displays important status information at the bottom of the screen in the Status Bar.

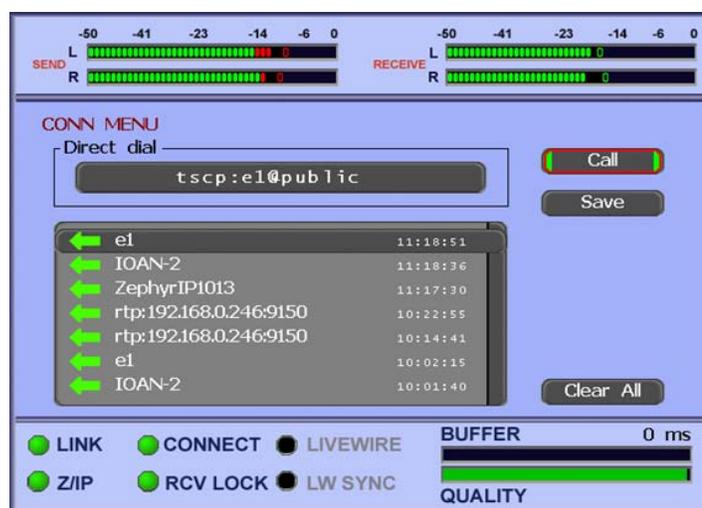


- The CONNECT light will illuminate when a connection is established with another unit. A yellow light indicates that the Z/IP server is being queried for the remote side’s IP address; a blue light indicates that the far end is being accessed; a green light indicates that the call has been successfully established.
- The RCV LOCK light illuminates green when the decoder recognizes an incoming bitstream and is able to decode it. This LED may be lit yellow in case the validity of a bitstream cannot be determined (ie. When receiving G711 or G722 audio).
- The LIVEWIRE is lit when the unit receives advertisements for Livewire streams from the IP network.

- The LW SYNC is lit green when the unit's internal samplerate was successfully PLL-locked to the Livewire network clock.
- The BUFFER meter indicates how many frames of audio are currently being buffered by the receiver to overcome network jitter. The actual number of milliseconds of buffering is displayed as well (this is *in addition to* the delay inherent in the coding scheme being used).
- The QUALITY meter indicates an aggregate of the network information from the Graph screen. The higher the meter, the higher the quality of the connection (lower packet loss, lower jitter).

6.4 Calling a Unit Directly

In addition to placing calls from the buddy list you may also call by entering the other unit's name and group or by using the call history log. You may reach the connection screen by pressing the physical CONN button on the front panel of the unit or by navigating to and selecting the CONN option on the main screen. The following dialog will be displayed:



To place a call to another Z/IP, enter that unit's name and group ("name@group") in the Direct dial field then click the Call button. You may also select an entry from the Call history log and redial it using the Call button (more on this below).

For other types of calls you need to use a protocol prefix to indicate the type of call. To call another Z/IP directly (without the Telos server) you would enter "tscp:address:port". For example, if the other unit's IP address is 192.168.0.123 and its Listen Port (see chapter 4- Z/IP Server Config) is set to 11926 then you would enter "tscp:192.168.0.123:11926".

For SIP calls you would enter "sip:name@address". The SIP default port is 5060. If the other device is configured to use a different SIP port then you may append the port to end of the address by using the colon separator (e.g. if the address is 192.168.0.101 and port is 5070 then

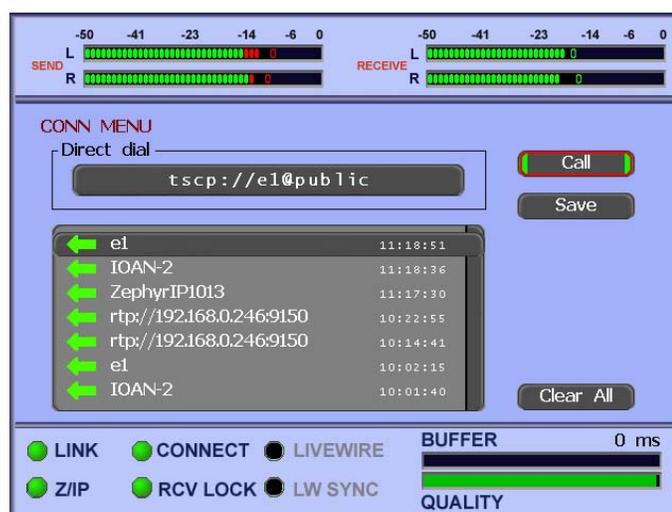
you would enter "sip:phone1@192.168.0.101:5070"). For one way RTP push streams you would enter "rtp:address:port".

Call History

The Call history log is below the Direct Dial field. Each call in the list is preceded by a symbol indicating an *incoming* or *outgoing* call. A Green Arrow pointing to the left indicates an *outgoing* call. A Blue Arrow pointing to the right indicates an *incoming* call. The time of the event is shown on the right list of the list.

To place a call to a unit listed in the Call History, simply browse the list and select the unit by pressing the OK button. Then select the "Call" button on the screen to place the call.

You can also add a unit to your Buddy List from the Call History Log. Find the unit in the list, select it, and hit the "Save" button on the screen (instead of "Call"). You will be taken directly to the ADD BUDDY menu where you can enter a screen name and panic dial bit if desired.



6.5 Relay Connection over the Server

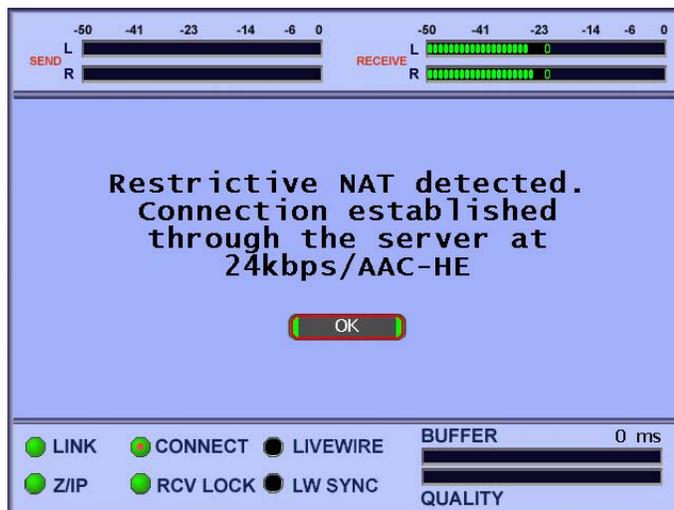
In certain cases, when both ends are behind very restrictive NATs it may not be possible to establish a direct connection between the two units. In such cases, the Zephyr/IP Server provides a limited backup mode that will still allow you to make a connection. Unit A will send its compressed audio data to the Z/IP Server, which will, in turn, relay this data to Unit B. The same occurs in the opposite direction.

Please note that, because of the amount of bandwidth used in these cases, the connection is *strictly limited* to using High Efficiency AAC at 24kbps in both directions.



When a connection is established using the Server Relay method, the unit will display a warning message on the screen alerting you that it is switching to HE-AAC mode at 24kbps. Changing the Codec Mode or bitrates will have no effect during these connections.

The Status Bar on the front panel of the Zephyr/IP will show a small red dot inside the CONNECT light when a Server Relay Connection is in progress:



6.6 SIP Calls

The Zephyr/IP fully supports the Session Initiation Protocol (SIP). SIP is a signaling protocol widely used for voice over IP (VoIP) applications. Using SIP, the Zephyr/IP is able to accept and make calls to a variety of devices, including some VoIP phones. This section describes how to configure the Z/IP for SIP and how to make and receive SIP calls.



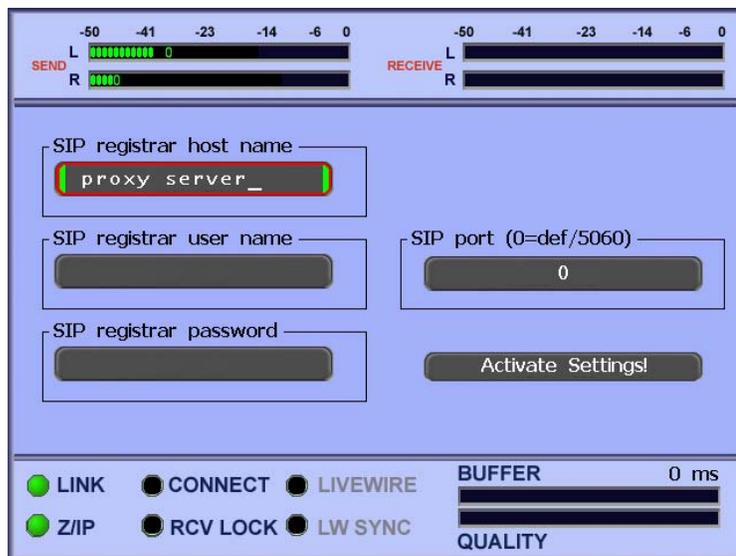
In order for a SIP call to be successful the two devices involved in the call must agree on a common codec. This is done through a codec negotiation step during the initial SIP call establishment. If no common codec can be selected then the call will fail. The Z/IP supports the following codecs for SIP calls: G.711, G.722, MPEG Layer 2, MPEG AAC (Zephyr Xstream compatible) and linear PCM.

SIP Configuration

SIP can be used in two modes: direct or with a proxy server. Direct mode is just what you would expect, one device calls another directly. A proxy server is used when you have established VoIP service and all VoIP calls need to be routed through that provider. Another

case when a proxy server may be used is when your facility has a VoIP PBX and the calls need to be routed through the PBX.

No special configuration is required for direct mode. When using a proxy server, the proxy server information must be configured on the Network/SIP Server dialog screen.



Here you need to enter the IP address of the proxy server, the name (or phone number) to register with the proxy server and the password if one is required. Once you save the settings the Z/IP will register with the proxy server and all outgoing calls will be routed through the proxy server. Incoming calls are always accepted either directly or through the proxy server.

Making SIP Calls

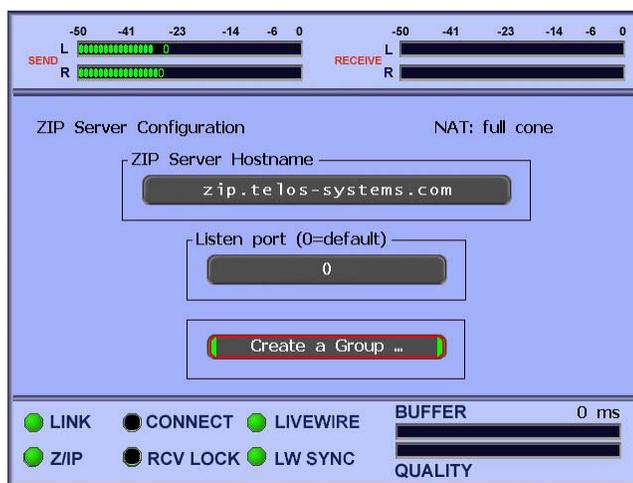
You can make SIP calls by entering the address of the device to call or by adding a SIP speed dial entry. A SIP address has the following format: "sip:name@address". Using the "sip:" prefix tells the Z/IP that this is going to be a SIP call. The "name" portion is either the name or phone number of the remote device and the "address" is the IP address of the device or of that device's proxy server (if it has one).

Adding SIP Devices to the Speed Dial List

You may add SIP devices to the speed dial list for convenience and easy access. In the name field add the "name@address" (or just "address" if no name is needed on direct calls). Then use "sip:" for the group name. This will tell the Z/IP that this is a SIP speed dial entry.

7 The Zephyr/IP Server

In the Quick Start Guide section on page 13 you have been asked to enter settings for the Z/IP server. This section describes the purpose of the server and the functions it provides.



The Z/IP server is configured and maintained by Telos Systems and it provides a set of services to enhance the functionality of your Zephyr/IP: the directory service, the presence server, NAT traversal service, media relay service and geolocation service. The following subsections describe each service in more detail.

7.1 Directory Service

The directory service allows your Z/IP to register itself with a unique group and device name. The group and device name together form a persistent "phone number" for your Z/IP. Other users can always find and call your Z/IP regardless of what IP address you happen to be using that day. This is especially important when your ISP has given you a dynamic IP address or when you take the Z/IP on the road.

The directory service also allows you to locate other Z/IPs by browsing the server directory right from your Z/IP. Wildcard and soundex searches allow you to find the device you're interested in even if you don't remember the exact spelling of the other device's name or group.

Of course, you are in complete control over how your Z/IP appears in the directory. You may list your Z/IP as "visible to all", "visible only to others in the same group" or even "hidden". While in hidden mode, your Z/IP does not appear in the directory but it is still reachable by people that know your Z/IP's name and group.

7.2 Presence Service

The presence service allows you to see the state of the other Z/IPs in your "buddy" (or speed dial) list. This way you know if the other Z/IP is online, offline or busy before you even attempt the call.

The state information is updated a few times per minute to always keep the list up to date.

7.3 NAT Traversal Service

Many networks make use of network address translation (NAT) devices to get around the shortage of public IP addresses. NATs can be very useful but they also make it difficult to reach devices that are behind the NAT (section 9.6 below describes NATs in more detail). The Z/IP server allows your Z/IP device to detect when it is installed behind a NAT and to determine the NAT type. It also helps the devices to reach each other even when both sides are installed behind NATs.

7.4 Media Relay Service

Not all NATs behave the same way. Some NATs are very restrictive and go to great lengths to prevent data from outside the network to reach devices on the inside. This is a great security feature especially for PCs but not so good for devices that need to receive calls from the outside. The Z/IP together with the server's NAT traversal service can automatically get through most types of NATs.

When both sides are behind very restrictive NATs it may not always be possible to get through the NAT in a manner that allows the two end devices to communicate directly. In these extreme cases the media relay service allows the two Z/IPs to communicate by having the server exchange the audio data.



Direct communication between Z/IPs is always preferred over using the media relay service. Devices using a direct communication path have a lower end-to-end audio delay. Using the media relay service may also restrict the bitrate and codec used to encode the audio.

If you find yourself behind a very restrictive NAT but you have control over it (or can ask a network administrator) then it is best to configure port forwarding on the NAT (section 9.6 below describes how). This will allow your Z/IP to communicate directly with any other device without having to rely on the media relay service.

7.5 Geo-Location Service

The Z/IP displays an approximate path taken by the audio packets to reach the destination. The geo-location service allows the Z/IP to display the path as a trace on a world map rather than a confusing list of IP addresses. The server does this by maintaining a database of IP addresses and their locations and communicating this information to the Z/IP as needed.



IP address assignment changes at times, especially with dynamic IP addresses. If you find that the location for your IP address is not correct, please let us know and we'll do our best to fix it.

8 Groups and Directory Services

This chapter describes the ideas behind organizing your Zephyr/IPs with groups. It also covers how your device(s) appear in the server directory.

During configuration a Zephyr/IP is assigned a device name. This name is used to refer to this Zephyr/IP when connecting to other units; it becomes part of this unit's address or "phone number". The other part of the unit's address is the group to which the unit belongs. Together the unit name and the group form a unique device address.

Why Groups?

Groups are useful because they allow you to keep your Zephyr/IPs logically grouped. They make it easier for others to find you and simplify the task of selecting a name for the device. A device name needs to be unique only within your group; it does not have to be unique among all other Zephyr/IPs in the world. We've all been frustrated when trying to select a login name for services like Yahoo™ mail and finding that most obvious names have already been taken by others. Group passwords prevent others from becoming part of your group and from viewing the names of the Zephyr/IPs within your group, except for the ones you allow.

The Public Group

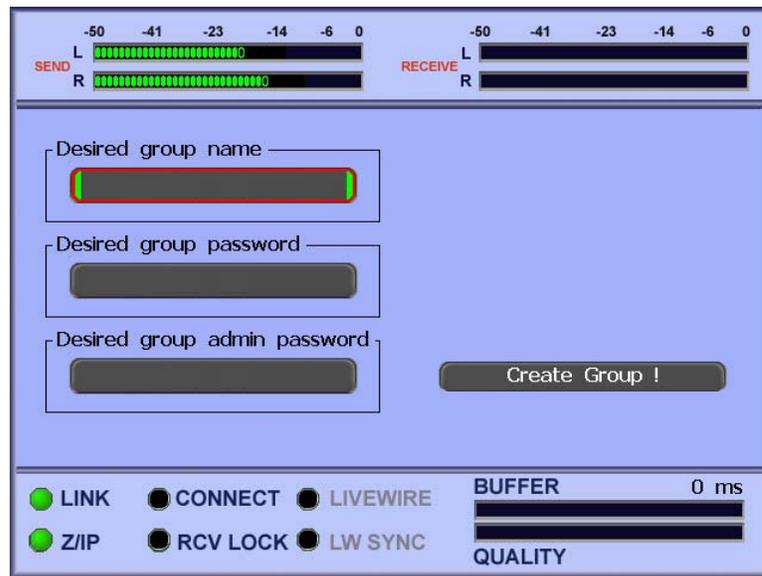
Every Zephyr/IP is initially configured to be a member of the "public" group. The "public" group is a special group that exists by default on the server. It is special because anyone has access to it (the group password is also "public") and it is never deleted.

When you first connect to the server, your Zephyr/IP will join the public group. You may use any device name you like but if the name is already in use by another device the server will assign you a unique name. At this point you may keep this name, try to select another or better yet, create your own group.

Creating Groups

Groups can be created at any time and you may create as many groups as you need. Groups are created by going to the Z/IP Server Configuration dialog and selecting the "Create a Group" option.

A new dialog will prompt you for the desired group name, group password and group administrative password.



Click the "Create Group" button to create the group. A message will indicate if the operation succeeded or failed. If the group creation failed due to a duplicate name then you will need to change the name and try again. Selecting the name of your organization or department for the group name may be more likely to succeed.

A group uses two passwords. The first is the password that others will need in order to be able to join the group or to see devices that are listed as group private (more on this a bit later). The group administrative password is used to change the group passwords later if needed.

You should give your group password out only to people that you want to have as members of your group. You should NEVER give out your group administrative password.

Directory Listing Visibility

The server directory allows users to find other Zephyr/IPs without having to know their currently assigned IP address. But there are times when you may want to limit the visibility of your Zephyr/IP.

When you register with the server, your Zephyr/IP can select one the following visibility modes:

1. **Visible to all:** Anyone is able to see your Zephyr/IP's directory listing.
2. **Visible to group:** Only visible to those devices that know your group's password. Of course, this option is not useful for the public group since anyone knows the public group's password.
3. **Hidden:** Your Zephyr/IP is not shown in the server directory. Others are still able to call you if they know your device's name.

Group and Device Name Longevity

Groups remain active on the server as long as they have at least one Zephyr/IP that belongs to that group. If a group has no members then the server will delete the group after 24 hours.

Zephyr/IP names remain valid on the server for six months. After six months of inactivity the name is removed from the server directory. In most cases this is not a problem; even if the name was removed from the server when the Zephyr/IP connects again the name entry will be created again.

There is a case (perhaps rare) that you should be aware of. If your Zephyr/IP is the only member of its group and it has been inactive for six months then the server will remove it from the directory. Twenty four hours later the group would be deleted as well since it is now empty. If the device is powered on at a later time, it would not be able to connect to the group (since the group is no longer there). Should this happen you will need to create the group again. Or just avoid this situation altogether by making sure that your Zephyr/IP gets online at least once every six months.

Reusing a Zephyr/IP Name

The server does not allow two Zephyr/IP devices to use the same name. A name is registered to a particular device and the server does not allow other devices to accidentally take a name that is already in use. There are times however, when you do need to use the same name again. For example, you may replace a unit and want to use the same name on the new one. This section describes how you can assign an existing name to a new unit.



Please note that you may only take an existing name within your own group. You can never do this in the public group or in a group to which you don't have the password.

If there is a time when you need to use the same name on another Zephyr/IP you simply configure the new Zephyr/IP with the same name and group as the old device. Since no two devices can have the same name at the same time you should make sure there is no other device connected to the server that is currently using the selected name.

Once you connect to the server you will get a warning telling you that the name has been previously used by another device and are given a choice to select another name or to take over this name. If you choose to take over the name then the new device becomes associated with the name.



Please use this feature cautiously. Taking over the name of a unit that is currently online could cause the units to fight over the name potentially resulting in loss of service to both units.

9 When an IT Department is not available

There are times when an IT department is not on hand to guide through some of the networking ins and outs. This chapter covers some of the basics to get you started.

9.1 IP Addresses, Subnet Masks and Gateways

This section describes the terms used in IT environments. You probably already know these terms but we included them here for completeness. The terms covered are IP Addresses, subnet masks, gateways, DNS and DHCP. Network Address Translation (NAT) is covered in its own section below.

IP Addresses

Internet Protocol (IP) addresses identify electronic devices that are part of an IP network. The protocol uses these addresses to properly route the data to the destination. Without Network Address Translation (see section 9.6 below), every device connected to a common network would require a unique address.

There are two versions of IP. The current version is called IPv4 and is what we refer to in this manual. IPv6 is a new standard that is not yet widely deployed.

IPv4 addresses consist of a 32-bit number. To make it easier for humans to describe, IP addresses are written in a form called dotted decimal notation. To come up with a dotted decimal representation the 32-bit number is broken down into four parts, each part 8 bits long. Each part is converted to a decimal number and written out with a dot in between.

For example, a device that has a 32-bit IP address of 3,232,235,841 is commonly written out as 192.168.1.65. The figure below shows how this conversion takes place.

IP number	3,232,235,841			
	↓			
Binary	11000000	10101000	00000001	01000001
	↓	↓	↓	↓
Decimal	192	. 168	. 1	. 65

I hope you agree that 192.168.1.65 is easier to remember and talk about than 3,232,235,841.

Subnet Masks

Larger networks are often broken down into subnets. Subnets make the network easier to manage. Subnets are connected to each other by routers: devices that route the packets to the destination. The Internet Protocol differentiates between local addresses (addresses on the same subnet) and remote addresses (on different subnets). It uses the subnet mask to accomplish this task. Subnet masks might also be called netmasks or IP masks.



Before we get too deep into binary numbers, host and network address parts you should be aware that you can safely treat the subnet mask as just another parameter to set when you configure an IP address. No deep understanding is required to find out what the local subnet mask is and to configure it for your IP device. We should also mention that one of the most commonly used subnet mask is 255.255.255.0. Read on to find out why.

Network and Host IDs

To deal with subnets, IP treats the IP address as consisting of two separate IDs: a network ID and a host ID. The network ID identifies the subnet while the host ID identifies the actual device on the subnet. If two devices have addresses with the same network IDs then they are on the same subnet and are able to exchange data directly. If not then they are on different subnets. Any data exchange between them would have to go through a router.

The protocol needs to split the IP address into the network and host parts so that it knows where to send the data packets. It accomplishes this splitting by using the subnet mask.

A subnet mask is a 32-bit number and it is commonly written out in dotted decimal notation just like an IP address. If you write it out as a binary number you will notice that it consists of a string of ones followed by a string of zeros. The ones indicate (they "mask") the network portion of the IP address while the zeros indicate the host portion.

An example might explain this better. Using the same IP address as above, 192.168.1.65 with a subnet mask of 255.255.255.0 we find out that the network ID is 192.168.1.0 while the host ID is 65. Here is how we did it:

Step 1: Convert the mask to binary and we get 11111111 11111111 11111111 00000000.

Step 2: Convert the IP Address to ones as well.

Decimal	192	. 168	. 1	. 65
	↓	↓	↓	↓
IP Address	11000000	10101000	00000001	01000001
Mask	11111111	11111111	11111111	00000000
	⏟			⏟
	Network			Host

Step 3: For each 1 in the subnet mask, keep the corresponding IP address bit as is and for each 0 convert the corresponding bit to zero. We end up with:

11000000 10101000 00000001 00000000 (or 192.168.1.0)

This is the network ID part of the IP address.

Step 4: Now we invert the mask, for each 0 in the subnet mask, keep the corresponding IP address bit as is and for each 1 set the corresponding bit to zero. We get:

00000000 00000000 00000000 01000001 (or 65)



As you might know, computers love ones and zeros and built in binary operations make it a breeze to perform the network/host splitting. In a language like C or C++ the splitting would look like this:

```
network_id = ip_address & mask;
host_id = ip_address & (~mask);
```

IP Address Classes

Fine, you say. That was mildly entertaining. But why muck about with subnet masks and binary operations? Why can't they just always use the first 3 bytes for the network ID and the last byte for the host ID?

That is a fair question. The answer is that not every subnet is the same. Some corporate subnets are very large and have lots of hosts while some small subnets may have only a handful. The number of bits allocated to the host id determines the maximum number of IP devices you can have on the subnet. An 8-bit host id would allow for a subnet with a maximum of 255 hosts. That would not be enough in some cases.

The subnet mask solves this problem (although perhaps in an awkward way). On subnets with lots of hosts you can use fewer bits for the network ID and more bits for the host ID. On subnets with fewer hosts you can use more bits for the network ID and fewer bits for the host ID.

If you're managing a private network, you're free to select your subnet mask as you like. But on the Internet subnet masks are assigned by IP address class.

There are three common IP address classes: A, B and C. There is also a class D used for multicast addresses and a class E reserved for future use but here we'll only look at the first three.

Class	IP Address Range	Subnet Mask
A	0.0.0.0 to 127.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0

Class C is the most common IP address class so most of the subnet masks you see will likely be 255.255.255.0.

It is possible to have different subnet masks in addition to the ones above. The one thing to remember is that when converted to a binary number, subnet masks are always a continuous string of 1s followed by a string of 0s.



Windows Calculator can perform decimal, binary, hex and octal number conversions as well as some binary operations but by default these capabilities are hidden. To reveal these functions, select "Scientific" mode from the View menu.

Most of the time you will not have to give subnet masks much thought. But there may be times when you are given an invalid subnet mask and this information may help you to detect it, saving you some aggravation.

Gateways

We talked about networks having multiple subnets. Hosts on a subnet are able to communicate directly with each other. But what happens when a host needs to communicate to another that is on a different subnet? Simple: it uses the netmask to compare the network part of its address vs. the network part of the other device's address. If they are different then it sends the packet to the gateway address.

The gateway is the router device that will take care of sending the packet on its way to the destination when the packet cannot be delivered on the local subnet. In a way, it is similar to dropping off a piece of mail at the local post office. They will take care of getting it to the destination for you.



Gateway addresses often end with .1 or .254. This is not a requirement; they could end with any number between 1 and 254. It is only a convenience because it leaves a continuous range of numbers that can be used by local hosts.

What about ending with .255 you ask? It is true that the largest possible value is 255 (or 11111111 in binary). But addresses that end with .255 have a special meaning in the Internet Protocol. They are local broadcast addresses. A packet sent to such a broadcast address will be delivered to all hosts on the local subnet.

DNS

DNS stands for Domain Name System and in some ways it is similar to how the telephone book works: if you know the name, you can find the corresponding phone number to dial. DNS servers allow IP devices to find the IP address that corresponds to a given name (like telos-systems.com). The device can then use the IP address to talk to the host that has the name. Without a DNS server you would not be able to use address names; only dotted decimal IP addresses.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a method to hand out IP addresses to IP devices on a network in a dynamic fashion. When an IP device that is configured to use DHCP is powered up (or connected to the network) it broadcasts a request for IP configuration information on the subnet. If a DHCP server is available, it will allocate an unused IP address (from a user specified range) and respond back to the device. The device can then configure itself with this IP address.



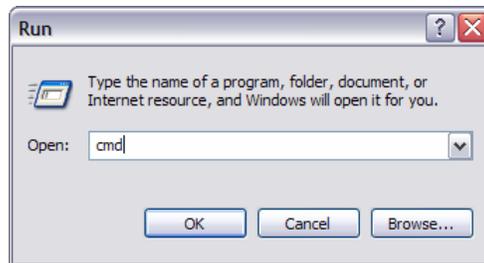
Using DHCP is a convenient method to configure an IP device but is not always the best course of action. When you use DHCP you don't know the assigned IP address of the device plus this address may change from time to time. This is usually not a problem but in some cases it can be. If you need to configure the Zephyr/IP via a web interface you will have to check the currently assigned IP address on the device via the front panel. Another situation where you do not want to use DHCP is if you wish to configure port forwarding on your NAT (see section 9.6 below).

9.2 Discover the Local Network Settings

You need to plug in your Zephyr/IP into a network but you don't know the network settings. If there is no one to ask, what can you do?

Well, if there is a PC already plugged in into the same network then you can check the network configuration on the PC to determine the available network settings. The directions here are for a Windows PC.

1. Click the Start button on the task bar then select the Run option. The following dialog will appear:



2. Type "cmd" then click the OK button. This will open up a command prompt window.

- Type "ipconfig /all" then press Enter. You should see some entries similar to the ones shown below:

```

C:\WINDOWS\system32\cmd.exe
Ethernet adapter Wireless Network Connection:
    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/Wireless 2915ABG Network
    Connection
    Physical Address. . . . . : 00-16-6F-3B-D9-E3

Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . : 
    Description . . . . . : Marvell Yukon 88E8053 PCI-E Gigabit
Ethernet Controller
    Physical Address. . . . . : 00-0E-7B-68-27-6A
    Dhcp Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 192.168.123.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.123.254
    DHCP Server . . . . . : 192.168.123.254
    DNS Servers . . . . . : 69.75.169.15
    . . . . . : 69.75.169.16
    Lease Obtained. . . . . : Sunday, November 04, 2007 9:51:18 AM
    Lease Expires . . . . . : Monday, November 05, 2007 9:51:18 AM

C:\>

```

If the PC has multiple adapters you will see multiple entries displayed. In the example above, the PC has a wireless adapter and the Media State for it is shown as disconnected which indicates that the wireless is currently disabled.

Following this is an entry for the "Local Area Connection" Ethernet adapter. In our case this is the entry of interest because it is plugged in the same Ethernet network that we want to learn more about. The section of interest is under the heading "Ethernet Controller" and contains the following interesting entries:

Dhcp Enabled – Yes => Indicates that this PC was configured for DHCP so there must be a DHCP server available.

IP Address – 192.168.123.101 => IP address assigned by DHCP server.

Subnet mask – 255.255.255.0 => This is the netmask for this subnet. We can use the same netmask for the Zephyr/IP.

Default Gateway – 192.168.123.254 => Another important entry, we can use the same gateway address on the Zephyr/IP.

DNS Servers – 69.75.169.15 and .16 => DNS server addresses. Use the first one on the Zephyr/IP. NOTE: The values in this example are not valid. Do not use these values on your Zephyr/IP!

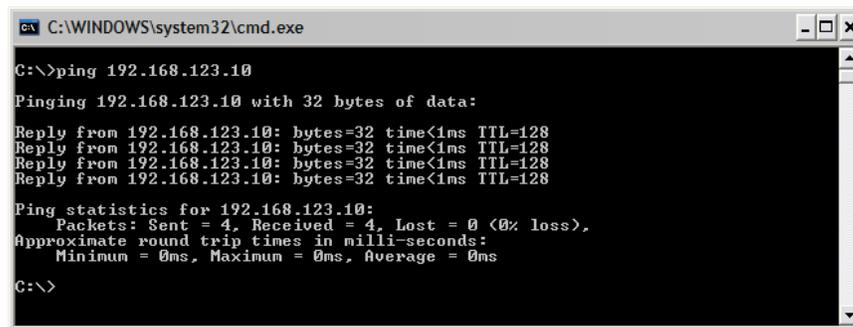
The ipconfig command will give you the subnet mask, gateway and DNS server addresses. It does not directly give you the IP address you should use on the Zephyr/IP. If DHCP is available, as it is in this example, you can just configure the Zephyr/IP to use DHCP. It will obtain an IP address automatically. If DHCP is not available then read on; the next section will describe this case.

9.3 Find an Available IP Address without a DHCP Server

What can you do if a DHCP server is not available on your network? In this case we'll search for an IP address by pulling one out of a hat then testing to see if it is already in use.

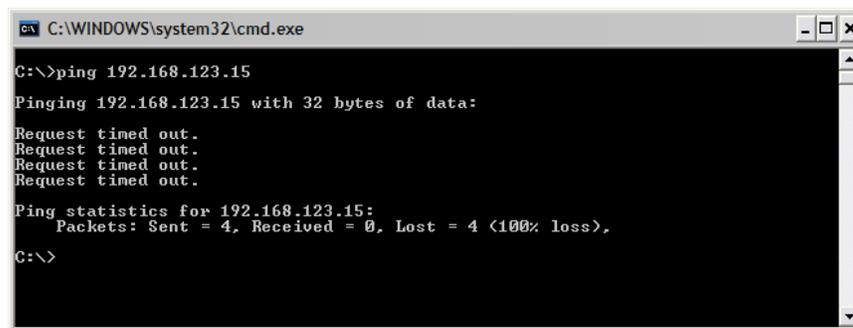
In the example above, the PC's IP address was 192.168.123.101 and the subnet mask was 255.255.255.0. This means that the last 8 bits indicate the host portion of the address. On this network, valid IP addresses would run from 192.168.123.1 to 192.168.123.254. Right away, we'll avoid .1 and .254 because they are often assigned to the gateway. That leaves numbers from 2 to 253, still a pretty big range. So just choose a number; I prefer to start with the lower numbers for no particular reason. For this example, I choose 10 so my first IP address to test will be 192.168.123.10.

1. Go to the Start menu on the task bar and select Run. Type "cmd" then click OK. A command prompt window should come up.
2. Type "ping " followed by the trial IP address you selected (I'll use 192.168.123.10 here) then press enter.



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.123.10
Pinging 192.168.123.10 with 32 bytes of data:
Reply from 192.168.123.10: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.123.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

3. Well, we got a reply to our "ping". This means that the IP address I selected is in use by another device so we can't use it. Let's try another. I will choose .15 this time:



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.123.15
Pinging 192.168.123.15 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.123.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

4. Much better. The time out messages indicate that no device responded at this address. This is a pretty good indication that we can use this address. But let's double check to be sure; there are some IP devices that may be configured to not reply to pings.
5. At the command prompt, type "arp -a". Make sure to do this right after the unsuccessful ping command. This command displays the physical addresses associated with IP addresses that have been recently used.

```

C:\WINDOWS\system32\cmd.exe
C:\>arp -a
Interface: 192.168.123.101 --- 0x5
Internet Address      Physical Address      Type
192.168.123.10       00-13-20-1b-65-5f    dynamic
C:\>

```

- The table shows one entry for the 192.168.123.10 address which we discovered in step 2 above. It does not show an entry for 192.168.123.15 which indicates that no device answered to this address. If there would have been an IP device that does not answer pings we would expect to see its address in the arp table.

With this last test complete, we can be pretty confident that AT THIS TIME, the 192.168.123.15 address is available. There is no guarantee that this address will remain valid forever. There may be a PC that uses this address that just wasn't turned on yet. So keep an eye out for signs of duplicate IP addresses on the network. Read the following section for the gory details.

9.4 Duplicate IP Addresses

Duplicate IP addresses can be difficult to diagnose. Some PCs may give you a warning at boot up that the currently configured IP address is in use. But other times, duplicate IP addresses are only discovered when an IP device behaves strangely.

For example, you know you assigned a particular IP address to your Zephyr/IP but now you cannot open the web configuration page at that address. Or perhaps, sometimes it works but other times it does not.

The method to diagnose a duplicate IP address conflicting with your Zephyr/IP is to learn the hardware address (also called the physical or MAC address) of your Zephyr/IP and to use the "arp -a" command from a PC to watch the hardware address associated with your Zephyr/IP's IP address.

If you ever find a different hardware address associated with your Zephyr/IP's address then it is time to call your IT department. Or if an IT department is not available (since you're reading this section anyway) just assign a different IP address to your Zephyr/IP.

9.5 Use Traceroute to Find the Communication Bottlenecks

There are times when you're exchanging data across the Internet and you notice that the transfer rate is really slowing down. One way to find out where the slow down is coming from is to perform a traceroute command. The Zephyr/IP does this and shows you the information on the right side of the connection screen. But you can perform this bit of magic from any PC.

- Click the Start button on the task bar and select Run. Type "cmd" and press Enter. This will open up our trusty command line window.
- Type "tracert " followed by the IP address or name of the host involved in the data exchange. I used www.google.com in this example:

```

C:\WINDOWS\system32\cmd.exe
C:\>tracert www.google.com
Tracing route to www.l.google.com [74.125.19.147]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    192.168.123.254
  1  15 ms    10 ms    13 ms    10.112.192.1
  2  14 ms    13 ms    12 ms    wcsdca1-gsr1-ge2-1-7.san.rr.com [24.25.193.73]
  3  11 ms    13 ms    13 ms    wcsdca1-gsr3-ge5-0-0.san.rr.com [24.25.192.14]
  4  14 ms    13 ms    13 ms    so-0-1-0.gar1.SanDiego1.Level3.net [4.79.36.13]
  5  14 ms    14 ms    14 ms    ge-7-0-0.mpl.SanDiego1.Level3.net [4.68.113.93]
  6  25 ms    22 ms    23 ms    as-1-0.bbr1.SanJose1.Level3.net [209.247.9.114]
  7  187 ms   219 ms   210 ms   ae-22-79.car2.SanJose1.Level3.net [4.68.18.68]
  8  24 ms    53 ms    24 ms    GOOGLE-INC.car2.SanJose1.Level3.net [4.79.43.146]
  9  29 ms    35 ms    35 ms    209.85.251.98
 10  27 ms    29 ms    28 ms    cf-in-f147.google.com [74.125.19.147]
Trace complete.
C:\>

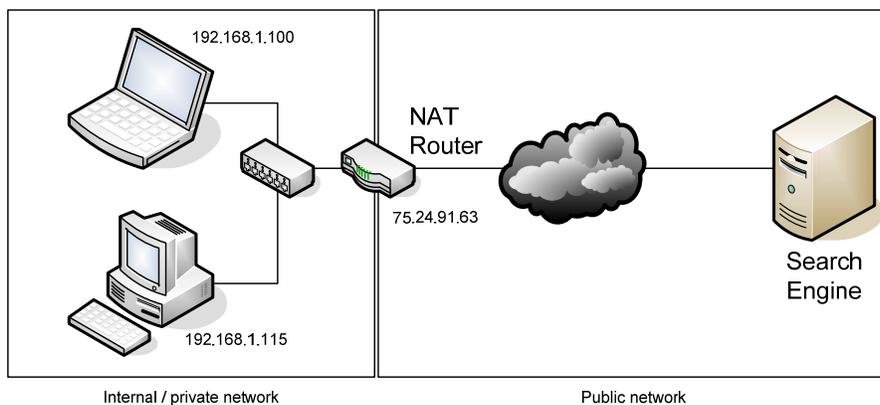
```

- The traceroute above shows the path of the data packets across the Internet. In this example the connection speed of every link was below 40 milliseconds except for hop #8, somewhere in San Jose (if we can trust the name). There it went up to about 200 milliseconds, indicating a bit of a bottleneck.

9.6 Network Address Translation

What is it?

Network Address Translation (NAT) is a technique that allows multiple IP devices on a private network to share a single public IP address. A NAT device has two network ports, one for the private side and the other for the public side. As the name suggests, the NAT router translates the internal IP addresses to the public IP address.



In the example drawing above, the laptop sends a request to a search engine. The packet is labeled with the IP address of laptop, 192.168.1.100. The NAT router intercepts the packet and changes the packet to replace the laptop's IP address with the public IP address assigned to the router, in this example 75.24.91.63 then sends the packet to the destination. The server

responds to the IP address embedded in the packet so the packet is sent to the NAT router. The NAT remembers that the initial request came from the laptop so it forwards the packet to it. As far as the laptop is concerned, it does not know nor does it care that there is a NAT device in between.

Are all NAT devices the same?

Not all NAT devices are the same as there is no defined standard on how a NAT should behave. Each vendor implements the NAT functions in a proprietary manner. You may hear NATs described as "full cone", "restricted cone", "port restricted cone" or "symmetric". Not everyone agrees on the exact definition of these terms. A Wikipedia article (http://en.wikipedia.org/wiki/Network_address_translation) does a good job attempting to describe them. Perhaps counter intuitively, symmetric NATs are among the most restrictive.

How do NAT devices affect communication devices?

NAT has some benefits and drawbacks. It is a lower cost solution compared to obtaining multiple public addresses and it adds to security by hiding the internal structure of the network. However, internal devices are no longer reachable from the outside because the NAT does not know which internal device the packet is destined for.

To get around this drawback, NATs have configuration capabilities which allow the user to forward specific ports to a given internal device or to add a single device DMZ zone (where this device is now visible to the public).

How does the Z/IP server help?

Making NAT configuration changes can be cumbersome. The Z/IP uses the Z/IP server to detect if it is installed behind a NAT and then determine the type of NAT as well. It is then able to accept calls from the outside without requiring you to make special configuration changes to your NAT. In addition to NAT traversal assistance, the Z/IP server also allows you to see the status of your "buddy" devices, to get a directory listing of available devices or to dial another device by name.

How do I use port forwarding with the Z/IP?

A common technique to help devices behind NATs to communicate is to use port forwarding. When you use port forwarding you tell the NAT that any time it receives data at a particular port that it should forward that data packet to a specific internal device.

The Z/IP is able to communicate through most types of NATs without requiring any special configuration of the NAT. But some NATs are much more restrictive than others. Establishing a connection becomes even more difficult when both ends are behind very restrictive NATs. Port forwarding can help in these cases. If at least one of the sides uses port forwarding then a direct connection can be established much faster.

You can use port forwarding with the Zephyr/IP in two steps:

1. On your Zephyr/IP in the Z/IP Server Configuration page enter a value for the listen port. The default value is zero which tells the Zephyr/IP to select a port on its own.

You can choose any value from 1024³ to 65,535 but please make a note of it. Also make a note of the IP address you assigned to the Zephyr/IP (this is one of those cases when you should not use DHCP).

2. On your NAT's configuration page, specify that the port you selected in step 1 above should be forwarded to the Zephyr/IP's address.



If you have more than one Zephyr/IP behind a NAT and you use port forwarding you need to make sure that each Zephyr/IP uses a different port. Some NATs may get very confused otherwise.

³ Ports range from 0 to 65,535. Ports from 0-1023 are referred to as the well-known ports and are usually reserved for special services. While there is nothing to prevent you from using a port number between 0 and 1023, you are much more likely to encounter a port conflict.

10 Option Cards

The Zephyr/IP has several option cards available for use in expanding your networking possibilities. Check the Telos Systems web page for the latest list of available adapter cards and their price and availability.

10.1 Installation of Option Cards



PLEASE FOLLOW ALL INSTRUCTIONS CLOSELY. ENSURE THAT YOU ARE PROPERLY GROUNDED AND HAVE TAKEN ESD PRECAUTIONS BEFORE YOU INSTALL ANY CARD INSIDE THE ZEPHYR/IP. THE Z/IP CONTAINS SENSITIVE ELECTRONIC DEVICES THAT CAN BE DAMAGED BY IMPROPER HANDLING. CONTACT TELOS SYSTEMS CUSTOMER SUPPORT WITH ANY QUESTIONS REGARDING THESE PROCEDURES.

1. Power down the unit and unplug the AC power cord before opening the chassis.
2. Remove the lid screws and store them in a safe place. Remove the lid of the unit.
3. Remove the aluminum slot cover from the PCI slot you will be using for the option card. Keep these screws in a safe place as well.
4. Remove the option card from its protective packaging and insert carefully in the PCI slot of your choice.
5. Press firmly to ensure that the card is properly seated in the card-slot.
6. Reinstall the mounting screws for the slot cover plate.
7. Place the lid of the Zephyr/IP back into its proper position. Reinstall the lid screws.
8. Attach the AC power cord and power on the unit.

11 The Parallel Port and Contact Closures

As stated in the Installation section , the Zephyr/IP has a DB25 connector on the back panel that provides contact closure (close-to-ground) inputs and outputs. There are 8 open-collector outputs, and 8 open collector inputs, each configurable from the Settings menu in the user interface. The DB25 connector is pinned out as follows:

<i>PIN</i>	<i>FUNCTION</i>
1	+5 Volts DC 400 mA max
2	Output 0
3	Output 1
4	Output 2
5	Output 3
6	Output 4
7	Output 5
8	Output 6
9	Output 7
10	No Connection
11	No Connection
12	No Connection
13	No Connection
14	Input 0
15	Input 1
16	Input 2
17	Input 3
18	Input 4
19	Input 5
20	Input 6
21	Input 7
22	Not Connected
23	Not Connected
24	Not Connected
25	Ground

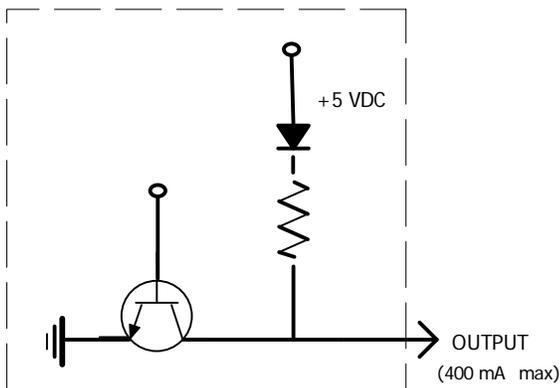
Parallel Outputs 0-7

Outputs are open collector to ground and can sink up to 125 mA of current each (actually, any output can sink up to 400 mA, however the maximum combined current should be kept below 1000 mA).

You must provide an external pull-up resistor (2.2 kOhm to 10 kOhm is appropriate) the voltage level you desire for your inputs. You cannot use a voltage level less than 5V, however, but you may use up to 50V.

If used with a relay or LED, then tie your external power source ground to pin 25 (or use the 5 VDC power supplied on pin 1) and run this power source through your device, with a resistor in series to limit maximum current to less than 125 mA.

The outputs can also be used for monitoring the status of the unit. This functionality can be set by several menu selections in *Settings* menu.



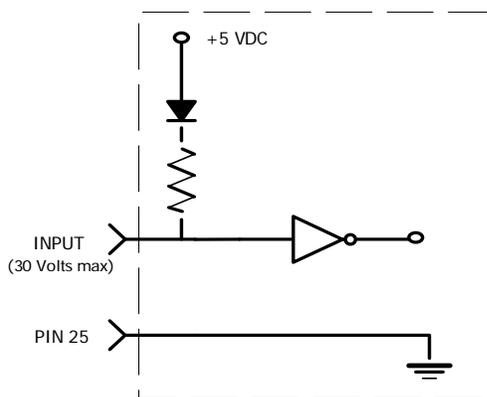
Equivalent schematic for the Parallel Outputs.

An external pull up resistor must be used. Alternatively, a voltage source (such as the 5 volts on pin 1) can be driven through an external device (such as a relay or LED) into the input.

Parallel Inputs 0-7

All inputs are specially treated to accept either a voltage (up to 24 VDC), or a closure to ground, which may be provided by switches, relays, or logic outputs. The inputs are active low. In other words, shorting the input to ground causes it to become true (i.e. "asserted").

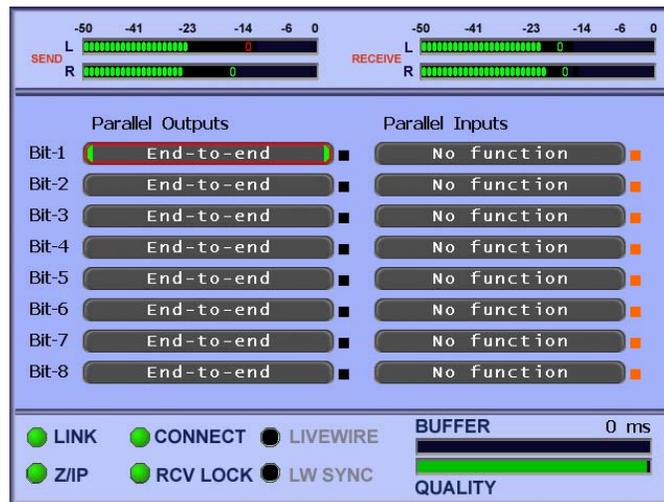
You must provide an external pull-up resistor to provide a TTL logic "High" (e.g. 2.2 kOhm to 5V).



Parallel logic input circuit

The inputs can be transmitted to the far end Zephyr/IP when using the AAC-HELD, or to a Zephyr Xstream in AAC mode. The inputs can also be used for local control functionality such as triggering auto dialing to your speed dial members.

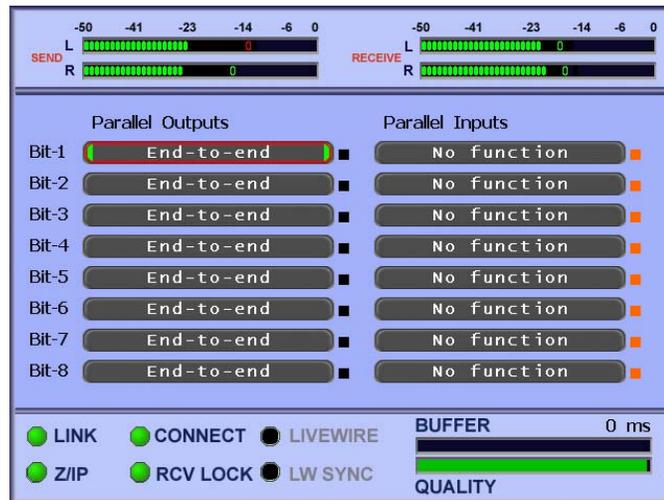
11.1 Parallel Port Output Modes



The 8 Parallel Contact Closure Outputs can each be set to one of four operating modes:

1. OFF: The open-collector output is left floating, and will remain so.
2. ON: The open-collector output is closed to ground, and will remain so.
3. END-TO-END: The Output will reflect the state of the corresponding INPUT pin at the far-end of the call, provided that a coding mode supporting contact closures is used (AAC or HELD-AAC).
4. CONNECTED: The contact closure will remain OFF until a call is connected, at which time it will close-to-ground. This function effectively mirrors the CONNECT light on the front panel GUI.

11.2 Parallel Port Input Modes



1. The 8 Parallel Contact Closure Inputs can each be set to one of four operating modes:
2. NO FUNCTION: The input is not used, and any activity on this pin is ignored.
3. END-TO-END: The state of this input pin will be sent to the far end codec where, if the appropriate OUTPUT pin is also set to “END-TO-END”, the status will appear. This function will only work in AAC and HELD-AAC coding modes.
4. DISCONNECT: If this input is closed-to-ground, the Z/IP will immediately disconnect any connected calls.
5. PANIC DIAL: If this pin is closed-to-ground, the Z/IP will immediately dial the buddy list member that has been configured for this pin. See Chapter 8 for more information on Buddy Lists, and how to configure them for Panic Dials.

12 Audio Coding Reference

12.1 Introduction to Audio Coding Technology

Introduction

Audio takes up a lot of data. Just a regular phone call uses 64,000 bits per second.

Without data reduction, CD-quality quality audio — 16 bits at 44.1kHz sample rate — requires a transmission capacity of about 706 thousand bits per second (kbps) for each audio channel. But, the wires we use for remote broadcasting are on a telephone system designed for voice-grade communications: 8 bits at 8kHz sample rate, or 64 thousand bits per second (kbps) per channel. That's 11% of what we need.



CURIOSITY NOTE!

*You can arrive at these same numbers with nothing more complicated than grade-school math. Just multiply the sample rate by the sample depth: 44,100 samples per second * 16 bits per sample = 705,600 bits per second for CD-quality mono audio. Multiply by 2 for stereo.*

You can reduce the data requirements by lowering the quality somewhat. 13 bits would yield a respectable 78 dB dynamic range, certainly adequate for casual home listening. And a 32kHz sample rate — with careful equipment design — will give you flat response to 15kHz, the practical limit for analog FM broadcasting in North America. Unfortunately, that still leaves us with telephone data channels about 93% too small to do the job. Besides, 13 bits is an awkward bit depth (resolution) for computers to deal with, and the audio it produces isn't clean enough to survive today's transmitter processors.



CURIOSITY NOTE!

Bit depth and sample rate translate easily into audio specifications. Digital audio must have a sample rate of at least twice the desired bandwidth, so 15kHz audio requires (after a safety margin) 32kHz sampling.

Each bit of sample depth represents slightly more than 6dB of dynamic range.

The first practical coding methods used a principle called ADPCM, Adaptive Delta Pulse Code Modulation. This takes advantage of the fact that it takes fewer bits to code the difference, or delta, between successive audio samples compared to using the individual values. Further efficiency is had by adaptively varying the difference comparator according to

the nature of the program material. G.722 and APT-X are examples of ADPCM schemes. They achieve around a factor of 4:1 reduction in bitrate.

G.722 achieves additional efficiency by allocating its bits to match the patterns in the human voice, and it's considered adequate for news and talk programming over ISDN. But, for high-fidelity transmission, algorithms with more power are required. These are based on psychoacoustics, where the coding process is adapted to the way we hear sounds. There are several algorithms available, with varying complexity and performance levels.

Some years ago, the international standards group ISO/IEC established the ISO/MPEG (*Moving Pictures Expert Group*), to develop a universal standard for encoding moving pictures and sound for digital storage and transmission media. The standard was finalized in November 1992 with three related algorithms, called Layers, defined to take advantage of psychoacoustic effects when coding audio. Layer 1 and 2 are intended for compression factors of about 4:1 and 6 or 8:1 respectively, and these algorithms have become popular in satellite and hard-disk systems. Layer-3 achieves compression up to 12.5:1 — 8% of the original size — making it ideal for ISDN.

Basic Principles of Perceptual Coding

With perceptual coding, only information that can be perceived by the human auditory system is retained.

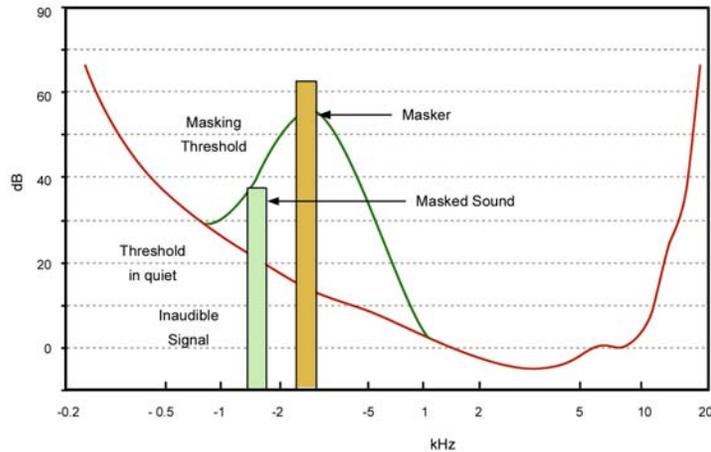
Lossless — which, for audio, translates to noiseless — coding with perfect reconstruction would be an optimum system, since no information would be lost or altered. It might seem that lossless, redundancy-reducing methods (such as PKZIP, Stuffit, Stacker, and others used for computer hard-disk compression) would be applicable to audio. Unfortunately, no constant compression rate is possible due to signal-dependent variations in redundancy: There are highly redundant signals like constant sine tones (where the only information necessary is the frequency, phase, amplitude, and duration of the tone), while other signals, such as those which approach broadband noise, may be completely unpredictable and contain no redundancy at all. Furthermore, looking for redundancy can take time: while a popular song *might* have three choruses with identical audio data that would need to be coded only once, you'd have to store and analyze the entire song in order to find them. Any system intended for a real-time use over telephone channels must have a consistent output rate and be able to accommodate the worst case, so effective audio compression is impossible with redundancy reduction alone.

Fortunately, psychoacoustics permits a clever solution! Effects called “masking” have been discovered in the human auditory system. These masking effects (which merely prove that our brain is also doing something similar to bit rate reduction) have been found to occur in both the frequency and time domains and can be exploited for audio data reduction.

Most important for audio coding are the effects in the frequency domain. Research into perception has revealed that a tone or narrow-band noise at a certain frequency inhibits the audibility of other signals that fall below a threshold curve centered on a masking signal.

The figure below shows two thresholds of audibility curves. The lower one is the typical frequency sensitivity of the human ear when presented with a single swept tone. When a single, constant tone is added, the threshold of audibility changes, as shown in the upper curve. The ear's sensitivity to signals near the constant tone is greatly reduced. Tones that were previously audible become “masked” in the presence of “masking tones,” in this case, the one at 300 Hz.

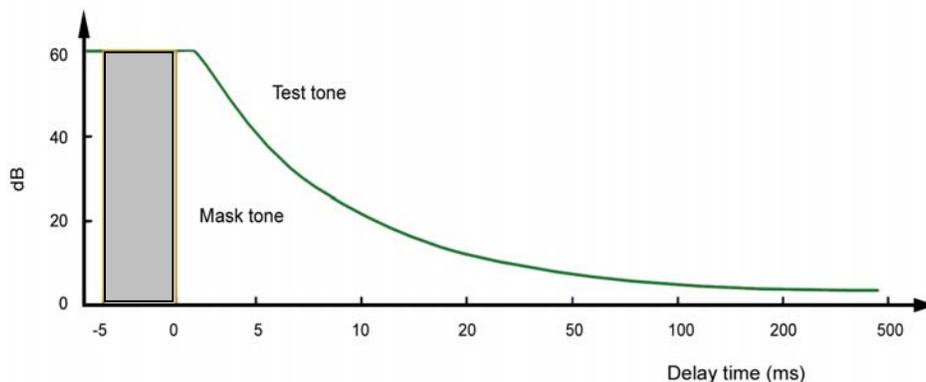
All signals below the upper “threshold of audibility” curve, or Masking Threshold are not audible, so we can drop them out or quantize them crudely with the least number of bits. Any noise which results from crude quantization will not be audible if it occurs below the threshold of masking. The masking depends upon the frequency, the level, and the spectral distribution of both the masker and the masked sounds.



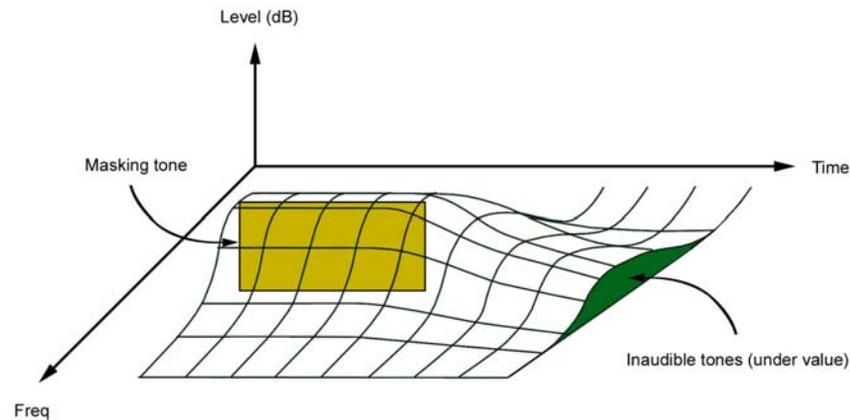
Masking effects in the frequency domain. A masking signal inhibits audibility of signals adjacent in frequency and below the threshold.

To benefit from the masking effects, perceptual coders use a filter bank to divide the input audio into multiple bands for analysis and processing. The maximum masked noise level is calculated depending upon the spectral content, and the available bits are allocated so as to keep the quantization noise below the masking threshold at every point in the spectrum.

While coding efficiency increases with more bands and better frequency resolution, the time domain resolution decreases simultaneously owing to an inevitable side-effect of the band filtering process: higher frequency resolution requires a longer time window – which limits the time resolution. Happily, masking works also in the time domain. A short time before and a longer time after a tone is switched on and off, other signals below a threshold amplitude level are not noticeable. Filter banks with higher frequency resolution naturally exploit the ear’s time-masking properties.



Masking effects in the time domain. Masking occurs both before and after the masking signal.



The combined results of time and frequency vs. masking. Signals under the curve are inaudible.



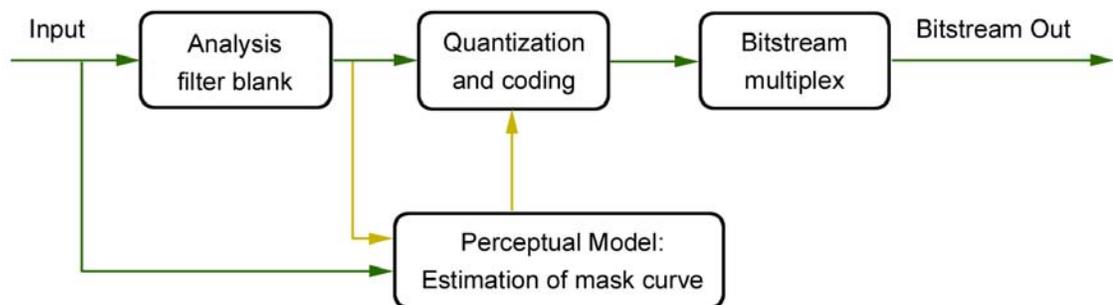
IMPORTANT!

Due to a perceptual coder's reliance on precisely modeling principles of human perception, audio to be coded should not be processed with any non-linear dynamics-processing such as clipping, multi-band compression, or hard limiting. Wideband compression, or AGC, is acceptable, and may be desirable if a consistent level cannot otherwise be achieved.

The same is true of audio that has been decoded, after passing through a perceptual coding cycle, but to much lesser degree.

For more information on this follow the link to our Omnia Audio website that has a paper delivered at the AES by Frank Foti on this topic.
<http://www.omniaaudio.com/techinfo/default.htm>

The steps involved in the perceptual coding process are shown below:



The components work as follows:

- The analysis filter bank divides the audio into spectral components. Sufficient frequency resolution must be used in order to exceed the width of the ear's critical

bands, which is 100 Hz below 500 Hz and 20% of the center frequency at higher frequencies.

- The estimation of masked threshold section is where the human ear/brain system is modeled. This determines the masking curve, under which noise must fall.
- The audio is reduced to a lower bit rate in the quantization and coding section. On the one hand, the quantization must be sufficiently coarse in order not to exceed the target bit rate. On the other hand, the error must be shaped to be under the limits set by the masking curve.
- The quantized values are joined in the bit stream multiplex, along with any side information.

Doing audio coding effectively means managing several tradeoffs. Most important is the number of samples coded together in one frame. Long frames have high delay, but are more efficient because the header and side information is transmitted less frequently. Longer frames offer the possibility to use filter banks with better frequency resolution. A fundamental principle in signal processing is that spectral splitting filters may have either good time resolution, or good frequency resolution, but not both. This makes sense when you consider that a longer time window means that the analyzer has more complete information, more full audio cycles, to work with⁴.

In the case of rapidly changing input signals (transients) long frames are poorer than short ones because the time spread will lead to so called *pre-echoes*. For such signals, the size of the frame should correspond to the temporal resolution of the human ear. This can be achieved by using short frames or by changing the frame length according to the immediate characteristics of the signal.

MPEG

By far, the most popular high fidelity audio coders rely upon techniques developed under the MPEG umbrella. MPEG stands for Motion Pictures Expert Group, a Joint Committee of the International Standards Organization (ISO) and the International Electrotechnical Commission. Over a decade ago, when the CD had just been introduced, the first proposals for audio coding were greeted with suspicion and disbelief. There was widespread agreement that it would simply not be possible to satisfy golden ears while deleting 80% or more of the digital audio data. But the audio coding pioneers were persistent and the MPEG audio group was formed. Since 1988, they have been working on the standardization of high quality audio coding. Today, almost all agree not only that audio bit rate reduction is effective and useful, but that the MPEG process has been successful at picking the best technology and encouraging compatibility across a wide variety of equipment.

The MPEG process is open and competitive. A committee of industry representatives and researchers meet to determine goals for target bit rate, quality levels, application areas, testing procedures, etc. Interested organizations that have something to contribute are invited to submit their best work. A careful double blind listening test series is then conducted to determine which of the entrant's technologies delivers the highest performance. The subjective listening evaluations are done at various volunteer organizations around the world that have access to both experienced and inexperienced test subjects. Broadcasters are the most common participants with many of the important test series conducted at the BBC in

⁴ Perhaps this is the DSP designer's equivalent to the economist's TANSTAAFL: There ain't no such thing as a free lunch.

England, the CBC in Canada, and NHK in Japan. Finally, results are tabulated, a report is drafted and ultimately a standard is issued.

In 1992, under MPEG1 (the first of the MPEG standards), this process resulted in the selection of three related audio coding methods, each targeted to different bit rates and applications. These are the famous layers: 1, 2 and 3. As the layer number goes up, so does performance and implementation complexity. Layer 1 is not much used. Layer-2 is widely used for DAB in Europe, audio for video, and broadcast playout systems. Layer-3 – which Telos was the first to use in the Zephyr – is widely used in broadcast codecs and has gone on to significant Internet and consumer electronics fame under the moniker derived from the file extension: *MP3*. MPEG2 opened the door for new work, and some minor improvements were added to both Layers 2 and 3. In 1997, the first in the AAC family was added to the MPEG2 standard. MPEG4 is ongoing now, but it has already been decided that AAC will be the “general audio” coder under this umbrella. (MPEG3 was skipped for reasons unknown.)

MPEG4 AAC (Advanced Audio Coding)

The MPEG4 AAC system is the newest audio coding method selected by MPEG. It is a fully state-of-the-art audio compression tool that provides performance superior to any known approach at bit rates greater than 64 kbps and excellent performance relative to the alternatives at bit rates reaching as low as 16 kbps.

The idea that led to AAC was not only to start fresh, but also to combine the best work from the world’s leading audio coding laboratories: Fraunhofer, Dolby, Sony, and AT&T were the primary collaborators that offered components for AAC. The hoped for result was ITU (International Tele-communications Union) “indistinguishable quality” at 64 kbps per mono channel. That is, quality indistinguishable from the original, with no audio test item falling below the “perceptible, but not annoying” threshold in controlled listening tests.

The MPEG test items include the most difficult audio known to codec researchers, so this was daunting challenge. The thinking was that if a codec could pass this test, it would surely be transparent for normal program material like voice and pop music, which are much more easy to encode. AAC designers chose to use a new modular approach for the project, with components being plugged-in to a general framework in order to match specific application requirements and the always-present performance/complexity/delay tradeoffs.

Compared to the previous layers, AAC takes advantage of such new tools as temporal noise shaping, backward adaptive linear prediction and enhanced joint stereo coding techniques. AAC supports a wide range of sampling rates (8–96 kHz), bit rates (16–576 kbps) and from one to 48 audio channels.

AAC is a lot more sophisticated than the previous MPEG layers 2 &3, providing significantly more coding power. Because it uses a modular approach, new ideas can be developed and plugged in to the basic structure. This had the additional advantage that it was possible to combine the various components from different developers, taking the best pieces from each. AAC was built on a similar structure to Layer-3, and thus retains most of its features. Nevertheless, compared to the previous MPEG layers, AAC benefits from some important new additions to the coding toolkit:

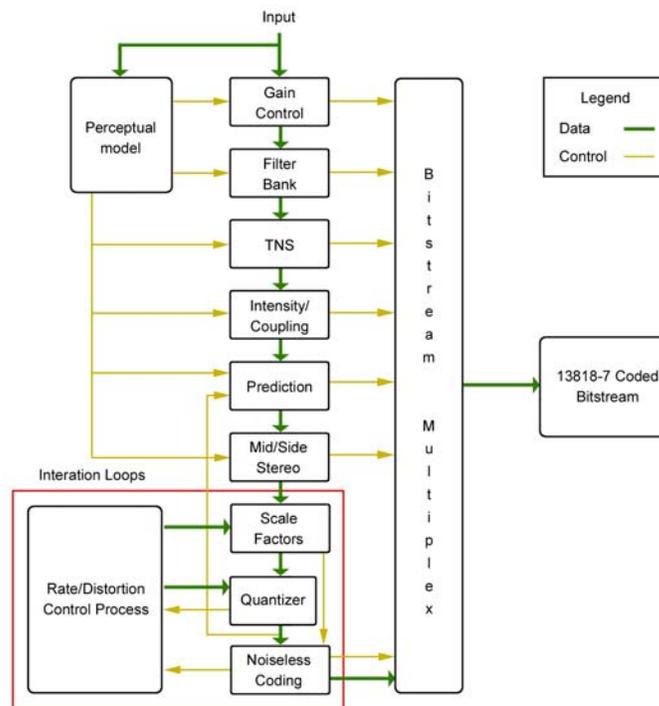
- An improved filter bank with a frequency resolution of 2048 spectral components, nearly four times the number used by Layer-3.
- Temporal Noise Shaping, a new and powerful element that minimizes the effect of temporal spread. This benefits voice signals, in particular.

- A Prediction module guides the quantizer to very effective coding when there is a noticeable signal pattern, like high tonality.
- Perceptual Noise Shaping allows a finer control of quantization resolution, so bits can be used more efficiently.

Because it uses this modular approach, an implementer may pick and choose among the component tools to make a product with appropriate performance/complexity ratios. Or, new modules can be developed later and "plugged in" to its basic structure. Three default profiles have been defined, using different combinations of the available tools:

- **Main Profile.** Uses all tools except the gain control module. Provides the highest quality for applications where the amount of random accessory memory (RAM) needed is not constrained.
- **Low-complexity Profile.** Deletes the prediction tool and reduces the temporal noise-shaping tool in complexity.
- **Sample-rate Scalable (SRS) Profile.** Adds the gain control tool to the low complexity profile. Allows the least complex decoder.

The block diagram of the AAC encoder is shown below. It is considerably more sophisticated than the previous MPEG Layer-2 and Layer-3 systems, and therefore offers more coding power.



Because AAC was built on a similar structure to Layer-3, it therefore retains some of its powerful features:

- **Redundancy Reduction.** A Huffman encoding process causes values that appear more frequently to be coded with shorter words, while values that appear only rarely are coded with longer words. This results in an overall increase in coding efficiency – with no degradation, since it is a completely lossless process.

- Bit Reservoir buffering. Often, there are some critical parts in a piece of music that cannot be encoded at a given data rate without audible noise. These sequences require a higher data rate to avoid artifacts. On the other hand, some signals are easy to code. If a frame is easy, then the unused bits are put into a reservoir buffer. When a frame comes along that needs more than the average amount of bits, the reservoir is tapped for extra capacity.
- Ancillary Data. The bit reservoir buffer offers an effective solution for the inclusion of such ancillary data as text or control signaling. The data is held in a separate buffer and gated onto the output bit stream using some of the bits allocated for the reservoir buffer when they are not required for audio.
- The Joint Stereo mode takes advantage of the redundancy in stereo program material. The encoder switches from discrete L/ R to a matrixed L+R/ L-R mode dynamically, depending upon the program material.

The result of all this is that the researchers succeeded: AAC provides performance superior to any known codec at bitrates greater than 64kbps, and excellent performance relative to the alternatives at bitrates reaching as low as 16 kbps.

And the researchers succeeded in achieving the ITU goal: AAC is the first codec system to fulfill the ITU requirements for indistinguishable quality at 128 kbps/stereo⁵. It has approximately 100% more coding power than Layer-2 and 30% more power than the former MPEG performance leader, Layer-3. For more information on AAC, and the tests of it, see our web site for a paper on the subject: www.zephyr.com.

It offers:

- 20 kHz mono or stereo audio bandwidth.
- Significantly less delay than Layers 2 or 3.
- Full-fidelity mono on a single 56kbps channel.
- Affordable, transparent, audio transmission for AM/FM radio or television audio.

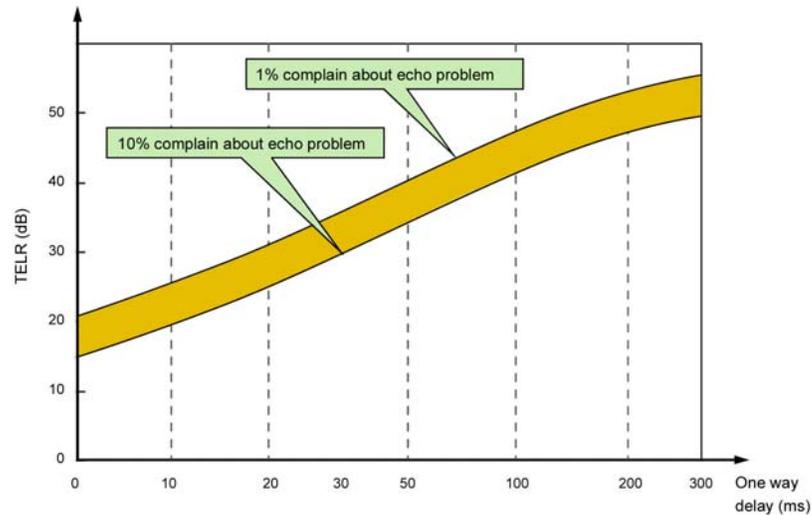
AAC-LD (AAC Low Delay)

When announcers use codecs for broadcast remote applications, they often need to have natural two-way interaction with other program participants located back at the studio, or callers. Because it is a hot topic for engineers working in the field of Internet telephony, a number of studies have been conducted to determine user's reactions to delays in telephone conversations. The data apply directly to the application of professional codecs to remotes, so it is interesting to take a peak over the shoulder of the telecom guys to see what they have learned.

For broadcast remotes, we try to arrange our system so that there is no path for the field announcer's voice to return to his/her headphones. Nevertheless, sometimes echo is unavoidable. For example, this can happen when a telephone hybrid has leakage or when a studio announcer has open-air headphones turned-up loud and the audio makes its way into the studio microphone.

⁵ Subjective Evaluation of State-of-the-Art Two-Channel Audio Codecs, G. A. Soulodre, T. Grusec, et al. Journal of the Audio Engineering Society; Vol. 46, #3; March 1998, Pg 164 - 177.

When there is no echo, it has been discovered that anything less than 100 ms one-way delay permits normal interaction between participants. Between 100 and 250 ms is considered “acceptable.” ITU-T standard G.114 recommends 150 ms as the maximum for “good” interactivity. Echo introduces a different case. As you might expect, echo is more or less annoying depending upon both the length of time it is delayed and its level. Telephone researchers have measured and quantified reactions, and ITU-T G.131 reports the findings and makes recommendations.



Summary of ITU-T G.13, with recommendations for designers of telephone systems that must cope with echo. This shows Talker Echo Loudness Rating vs. delay.

There are codecs using other than perceptual technologies that have lower delay, but they are not as powerful. That is, for a given bitrate, they do not achieve fidelity as good as the MPEG systems we have been examining. The common G.722 is an example. It uses ADPCM (Adaptive Delta Pulse Code Modulation), which can have delay as low as 10 ms, but with much poorer quality. So the question arises: Is it possible to have high quality and low delay in the same codec? Until recently, the answer was no. But new developments in codecs have changed the picture. One of the main objectives in audio coding is to provide the best tradeoff between quality and bit rate. In general, this goal can only be achieved at the cost of a certain coding delay. Codecs for voice telephone applications have used ADPCM and CELP because they have much lower delay than perceptual codecs. These are optimized for voice and can have reasonably good performance.

Zephyr users have known for years that Layer-3 offers all the fidelity needed for most broadcast situations. However, they also know that the delay of Layer-3 can be frustrating, particularly if high fidelity is needed in both directions and parties at the two ends must carry on a conversation.

The folks at Fraunhofer were aware of these factors, and have developed an extension to AAC called "AAC Low Delay," or "AAC-LD" for short. AAC-LD offers quality equivalent to Layer-3 with less than 25% of the delay!

AAC-LD combines the advantages of perceptual coders (such as Layer-3) with certain principles of speech coders. Compared to speech coders, AAC-LD handles both speech and music with good quality. Unlike speech coders, however, audio quality scales up with bit rate,

and transparent quality can be achieved. AAC-LD's coding power is roughly the same as Layer 3, meaning that mono high fidelity 15 kHz audio may be sent via one ISDN channel. With ISDN's two channels, you achieve near CD quality stereo.

Delay in perceptual codecs is dependent on several parameters:

- Frame length. Time is required to collect all the samples for a frame. The longer the frame, the more the delay.
- Filter bank delay. This causes an additional delay equivalent in time to the frame delay.
- Look-ahead delay for block switching. Layer-3 and AAC use filter banks with high frequency resolution. For signals with high tonality, efficiency is high. But when there are transients, a dynamic switching process changes to a filter bank with lower frequency resolution and better time resolution. In order to correctly decide when to make this change, a look ahead process is required, adding delay.
- Bit reservoir. The length of this buffer determines how much delay this process contributes.

The overall delay is a combination of all of these components, divided by the sampling rate. The delay scales linearly and inversely with the sampling frequency.

How AAC-LD Gets its Low Delay

AAC-LD is based on the core AAC work, so much is similar, but each of the contributors to the delay had to be addressed and modified:

- The frame length is reduced to 512 or 480 samples, with the same number of spectral components at the filter bank output.
- No dynamic block switching is used because the required look-ahead delay is too big. The temporal problem that causes pre-echoes is handled by the Temporal Noise Shaping module.
- The "window shape" of the spectral filter is enhanced to be adaptive. Normally, the shape is a simple sine curve, but AAC-LD can use a shape that has a lower overlap between the bands. This significantly improves performance with transients, without adding any delay.

MPEG-4 High Efficiency AAC (HE-AAC)

HE-AAC is an extension of AAC with the addition of Spectral Band Replication, a technique (developed by Coding Technologies) of synthesizing high frequency audio content based on the lower frequency data and side-chain information. SBR dramatically increases the efficiency of coding when using low bitrates. HE-AAC v1 is AAC plus SBR, while HE-AAC v2 adds Parametric Stereo to further increase the efficiency of coding stereo signals.

MPEG-4 Enhanced Low Delay AAC

High audio quality, low coding delay and very low data rates: AAC Enhanced Low Delay (AAC-ELD) is the perfect choice for any delay critical application that demands full audio bandwidth at data rates down to 24 kbit/s.

AAC-ELD combines the strengths of its two main components, MPEG-4 AAC Low Delay, and Spectral Band Replication (SBR). Whereas MPEG-4 AAC-LD features low encoding/decoding latency, SBR provides high quality audio at very low bit rates. SBR is also used in MPEG-4 HE-AAC, one of today's most efficient audio codecs.

AAC-ELD became an MPEG standard in January 2008.

ISO/MPEG LAYER-2

MPEG Layer-2 was an extremely popular early perceptual coding method, primarily because it's easier and less expensive to implement — particularly at the encoder — and practical devices using it were available earlier than Layer-3. It's a preferred choice for applications where very large data capacity is available, such as satellite links, high-capacity Primary ISDN or T1 circuits, and hard disk storage systems using Ethernet for signal distribution.

We include it in Zephyr/IP to offer compatibility with the widest variety of codecs, and for use at high bit rates.

Layer-2 J-Stereo

The Layer-2 joint stereo mode uses an “intensity coding” method. This method has high coding power and is quite effective, but hurts stereo separation on some program material. Audio above 3 kHz or so is combined to mono and panned to one of seven positions across the stereo stage.

G.722

This technology pre-dates perceptual coding. It is much simpler than the transform methods, but suffers from poorer audio performance. It has the benefit of low cost and the unique advantage of low delay. It has been around as an international standard the longest, and is probably the most widely used system. In our view, this technology is acceptable for mono voice where high fidelity is not necessary. It is good also for cueing and intercom channels.

We have included G.722 in Zephyr/IP because:

- It had been the most popular coding method early on, so there are many of these codecs in use. Because it is a standard, codecs from various manufacturers have a good probability of being able to interwork with one-another. (We've tested with many units and have found no problems so far.)
- G.722 has the lowest delay of all popular coding methods.

This method was invented in the late 70s and adopted as a standard in 1984 by the CCITT, the *Consultative Committee for International Telephony and Telegraphy* (renamed as ITU-T in 1993). The technique used is Sub-Band ADPCM (Adaptive Delta Pulse Code Modulation), which achieves data reduction by transmitting only the difference between successive samples. G.722 does this in two audio frequency sub-bands: 50 Hz to 4 kHz and 4 to 7 kHz.



DEEP TECH NOTE!

Only two bits are allocated per sample for audio frequencies above 4 kHz – sufficient for conveying the sibilance in voice signals, but not very good for intricate musical sounds. Also, the “predictor model” used to determine the step size in the adaptive function is designed only for speech. This is why music transmitted via

G.722 has a distinct 'fuzzy' quality.

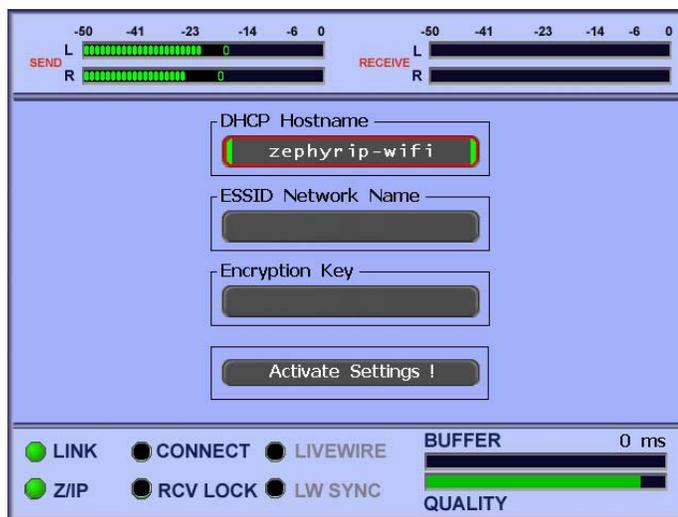
G.722 has a frequency response extending to 7.5 kHz with fairly poor fidelity. Unless there is no alternative, it should not be used for music.

13 Mobile Network Devices

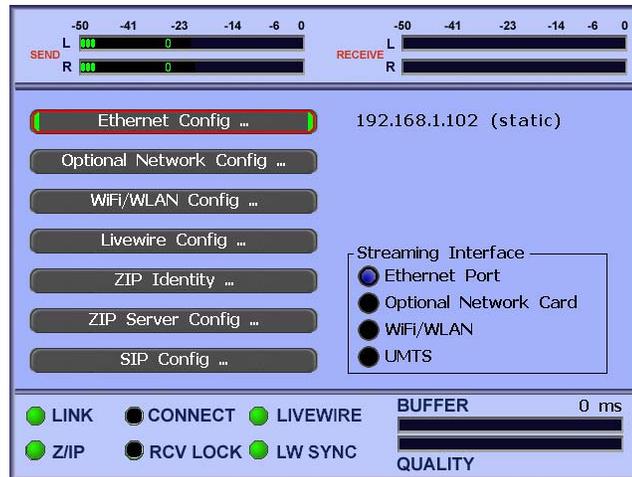
13.1 How to use Mobile Data Devices on the Zephyr/IP

The Zephyr/IP supports a variety of Mobile Network Devices through the USB port on the back of the unit. To use one of these devices is particularly simple:

1. Boot the Zephyr/IP **WITHOUT** the device plugged in (this is important because the Z/IP may not recognize the device unless it is plugged in while the unit is up and running).
2. Once the unit has completed the boot process and is showing the main menu screen, plug one of the approved mobile devices into either of the USB ports on the back of the Z/IP.
3. Navigate to the Network Menu and select Wi-Fi / WLAN. Enter the DHCP Hostname for the wireless network. For Wi-Fi also enter the ESSID Network Name and the encryption key. Currently only WEP is supported. Enter “s:password” for ASCII passwords or a hexadecimal key. Press “Activate Settings” to commit your settings to memory.



4. ESC back to the Network Menu and choose “Wi-Fi / WLAN” as the streaming device if you are using a Wi-Fi stick. For the Cellular Wireless stick, choose UMTS as the streaming device.



5. You will now be connecting over the mobile device when making a call.

13.2 Wi-Fi Devices

Currently the Zephyr/IP supports the following devices

1. Linksys Compact Wireless – G USB Adapter: WUSB54GC and WUSB54GSC
2. Netgear WG111v3 USB Adapter
3. Trendnet PCI Wireless adapter model TEW-423PI

13.3 EVDO or Mobile Broadband Modems

Currently the Zephyr/IP supports the following:

1. Sierra Wireless USB device AC595U for either Sprint or Verizon
2. Novatel Ovation U727
3. Novatel Ovation U720

Please contact customer support or the Telos Systems website for an update list of supported devices.

Also, note that your EVDO device must be activated with the software that comes with it. Please follow any directions that came with the device and contact your service provider for assistance if necessary.

Setting up one of these devices is done by the following steps:

1. Plug in the device when the unit is up and running.
2. Wait until the screen shows a message like “Sierra USB Modem inserted”.
3. Navigate to the network screen and chose UMTS as the streaming device.
4. Wait until the screen shows a message like “Sierra USB Modem installed & usable”.

14 Using the Field Upgrade Option

14.1 Updating the Software through the Web Interface

Although this will rarely be necessary, the Zephyr/IP provides the ability to upgrade to upgrade the internal software in the field.

ZephyrIP Audio Codec - Software Update

Select Firmware And Reboot

Select Firmware version to run after reboot:		
Bank 0:	(Version: 0.0.49 2007-10-17 10:41:50)	<input checked="" type="radio"/>
Bank 1:	(Version:)	<input type="radio"/>

Warning: System will reboot.

Update Firmware

Update Firmware in inactive bank 1:

Select firmware:

Update System-Software and Reboot

System version: Penguin V2.6.many

Select system zip file:

Warning: System will reboot.

The Zephyr/IP has two methods of software update, depending on the extent of the changes made in the software version. The Unit consists of two pieces of software embedded in the units flash memory: the application Firmware, and the Kernel. In some case you will only

need to update the current Firmware. In others, you may need to update the Kernel and the Firmware together: this is called a System Update.

Firmware Update:

From the software update menu, examine the contents of the firmware in Bank 0 and Bank 1 of the flash memory (the Zephyr/IP allows you to keep two different versions of firmware available, although only one will be running at a given time). Make sure that you are “running” out of the *Opposite* bank from the one which you will be updating. In other words, when you upload the update to the non-running bank, it will erase the current contents of that bank, so make sure that you preserve the correct firmware version in the other bank. If you are NOT running from the bank that you would like to preserve, then check the radio button next to that bank and click the “Reboot” button on the web page. When the unit comes back up, navigate back to this page, and continue with the update process.

You are now ready to begin the update:

1. Download the latest software version for the Zephyr/IP from the Telos Systems web page (www.telos-systems.com). Save it to a convenient place on your PC.
2. Connect to the embedded web page of the Z/IP you will be upgrading by typing its IP Address into the Navigation Bar of your browser.
3. Navigate to the “Update” page of the Z/IP.
4. Locate the “Update Firmware” section of the page and click the “Browse” button to locate the software package you just downloaded. Navigate through your computer’s directories and double click the file which you downloaded.
5. Now click on the “Update Firmware” button.
6. You should now refresh the page and see the new software in the opposite bank from which you had been running. Click the radio button next to the new bank, and reboot the system.



DO NOT TURN OFF THE UNIT OR DISCONNECT THE NETWORK CABLE DURING THE UPDATE PROCESS. INTERRUPTING THE PROGRAMMING OF THE Z/IP'S FLASH MODULE CAN CORRUPT THE DATA AND RENDER THE UNIT UNUSABLE. IF THIS HAPPENS, CONTACT CUSTOMER SUPPORT AND REQUEST A NEW FLASH CARD WITH THE LATEST SOFTWARE.

Update System Software

This procedure will replace BOTH banks of firmware as well as the Kernel.

1. Download the latest software version for the Zephyr/IP from the Telos Systems web page (www.telos-systems.com). Save it to a convenient place on your PC.
2. Connect to the embedded web page of the Z/IP you will be upgrading by typing its IP Address into the Navigation Bar of your browser.
3. Navigate to the “Update” page of the Z/IP.
4. Locate the “Update System-Software and Reboot” section of the page and click the “Browse” button to locate the software package you just downloaded. Navigate through your computer’s directories and double click the “xxxxx.gz” file which you downloaded.
5. Now click on the “Update System and Reboot” button.

The front panel of the Z/IP will indicate the progress of the update procedure. Follow the prompts displayed on the screen. After the unit reboots, it will retain your previous settings, but will be running the new software.

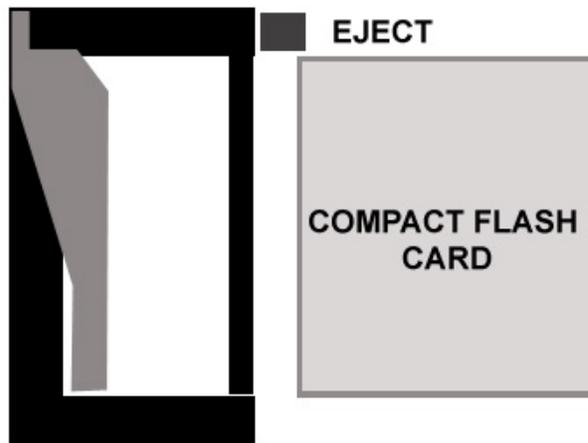
14.2 Installing a New Flash Card

In certain circumstances it may be necessary to replace the Compact Flash card containing the Zephyr/IP software. This card is located inside the unit.



PLEASE FOLLOW ALL INSTRUCTIONS CLOSELY. ENSURE THAT YOU ARE PROPERLY GROUNDED AND HAVE TAKEN ESD PRECAUTIONS BEFORE YOU INSTALL ANY CARD INSIDE THE ZEPHYR/IP. THE Z/IP CONTAINS SENSITIVE ELECTRONIC DEVICES THAT CAN BE DAMAGED BY IMPROPER HANDLING. CONTACT TELOS SYSTEMS CUSTOMER SUPPORT WITH ANY QUESTIONS REGARDING THESE PROCEDURES.

1. Power down the unit and unplug the AC power cord before opening the chassis.
2. Remove the lid screws and store them in a safe place. Remove the lid of the unit.
3. Locate the Compact Flash (CF) card and CF Slot on the motherboard of the Z/IP.
4. Press the ejector button to eject the CF Card.
5. Carefully slide the CF card out of the slot.
6. Insert the new CF card into the slot and firmly press it into place.
7. Place the lid of the Zephyr/IP back into its proper position. Reinstall the lid screws.
8. Attach the AC power cord and power on the unit.



The Compact Flash Card and Slot

15 Specifications

AUDIO SPECIFICATIONS

Pro / Pro Line Gain:	0dB ref: +4dBu input
Cons / Cons Line Gain:	+0.9dB ref:-10dBm input
THD+N Pro/Pro:	< 0.01% @ +18dBu, 1 kHz Sine
Freq Response:	+/- 0.5dB 20Hz – 20 kHz
Head Room:	18dB
SNR:	84.6dB Pro / Pro Unweighted 86dB “A” Weighted
Dynamic Range:	> 101dB Unweighted > 103dB “A” Weighted
Crosstalk:	< -92dB 10Hz – 1KHz < -79dB @ 10KHz
Output Clipping:	1% @ 22dBu Bridged Load (10.1 Vrms) 1% @ 22dBu 600 Ohm Load
Output Level Difference between bridged and 600 Ohm Load:	-0.67dB
Calculated Output Impedance:	45 Ohm < Zout < 50 Ohm differential
Calculated Input Impedance:	10 kOhm < Zin < 14K Ohm differential
Analog to Digital Converter:	24bits
Digital to Analog Converter:	24bits
AES3 Digital Inputs and Outputs (not available on MXP Version):	
	<ul style="list-style-type: none"> • Conform to AES3 Standards • Sample Rates Supported (input): 32KHz, 44.1KHz, 48KHz, 96KHz • Sample Rate Convert (output): 32, 44.1, 48KHz; Slave to Input, Slave to Sync

POWER

110 - 240 VAC 3 terminal plug

Switch-mode power supply

Input Power: 0.3A @ 115Vac 34.5Watts

Rails: 2.6A @ 5.22V 13.57 Watts

0.17A @ 13.1V 2.2 Watts

0.11A @ -12.3V 1.35 Watts

Total Rail Power: 17.12 Watts

Power Supply Efficiency: 50%

16 Warranty and Application Caution

ZEPHYR/IP LIMITED WARRANTY

This Warranty covers “the Products,” which are defined as the various audio equipment, parts, software and accessories manufactured, sold and/or distributed by TLS Corp., d/b/a Telos Systems (hereinafter “Telos Systems”).

With the exception of software-only items, the Products are warranted to be free from defects in material and workmanship for a period of one year from the date of receipt by the end-user. Software-only items are warranted to be free from defects in material and workmanship for a period of 90 days from the date of receipt by the end-user.

This warranty is void if the Product is subject to Acts of God, including (without limitation) lightning; improper installation or misuse, including (without limitation) the failure to use telephone and power line surge protection devices; accident; neglect or damage.

EXCEPT FOR THE ABOVE-STATED WARRANTY, TELOS SYSTEMS MAKES NO WARRANTIES, EXPRESS OR IMPLIED (INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE).

In no event will Telos Systems, its employees, agents or authorized dealers be liable for incidental or consequential damages, or for loss, damage, or expense directly or indirectly arising from the use of any Product or the inability to use any Product either separately or in combination with other equipment or materials, or from any other cause.

In order to invoke this Warranty, notice of a warranty claim must be received by Telos Systems within the above-stated warranty period and warranty coverage must be authorized by Telos Systems. If Telos Systems authorizes the performance of warranty service, the defective Product must be delivered, shipping prepaid, to: Telos Systems, 2101 Superior Avenue, Cleveland, Ohio 44114.

Telos Systems at its option will either repair or replace the Product and such action shall be the full extent of Telos Systems' obligation under this Warranty. After the Product is repaired or replaced, Telos Systems will return it to the party that sent the Product and Telos Systems will pay for the cost of shipping.

Telos Systems' authorized dealers are not authorized to assume for Telos Systems any additional obligations or liabilities in connection with the dealers' sale of the Products.

Telos Systems products are to be used with registered protective interface devices that satisfy regulatory requirements in their country of origin.



17 CE Declaration of Conformity

Supplementary Information for our European Users

Declaration of Conformity

Application of Council Directives: 93/68/EEC (CE marking); 73/23/EEC (safety-low voltage directive); 89/336/EEC (electromagnetic compatibility).

Standards to which conformity is declared: EN50081-1, EN50082-1.

Manufacturer's Name: Telos Systems, TLS Corporation

Manufacturer's Address: 2101 Superior Avenue, Cleveland, Ohio, USA

European Office: Telos Systems Europe
Johannisstrasse 6
85354 Freising
Germany
Telephone: +49.81.61.42.467
Fax: +49.81.61.42.402

Type of Equipment: Internet Audio Codec

Model No.: 4600-1000

Serial No.: _____

Year of Manufacture: 2000

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.

Place: Cleveland, Ohio, USA

Date: 30 January, 2000

Signature: _____

Full Name: Frank Foti

Position: President

1.0 Introduction

1.1 Scope This record is intended to document Telos Systems Omnia Stereo Generator conformance with Council Directives: 93/68/EEC (CE marking); 73/23/EEC (safety-low voltage directive); 89/336/EEC (electromagnetic compatibility).

Testing was conducted during the period December 1999 to January 2000.

1.2 Purpose Testing was performed to evaluate safety, emissions, and immunity, conformance to enable CE marking.

1.3 Conclusions The Telos Systems Omnia Stereo Generator was found to be compliant and CE marking was applied to the product.

2.0 HF Radiated Emissions

2.1 Standards Applied The unit was laboratory evaluated according to standard: EN50081-1 using Measurement Document: EN55022, Class B.

2.2 Testing The unit was tested and evaluated by: Smith Electronics *

2.3 Test Results The unit was found to be in conformance for both radiated and line-conducted emissions.

3.0 Immunity

3.1 Standards Applied

3.1.1 ESD Susceptibility Measurement Document: IEC 1000-4-2 (IEC 801-2). Immunity to static electricity.

3.1.2 Radiated Susceptibility – HF Electric Field Measurement Document: IEC1000-4-3 (IEC 801-3).

3.1.3 Conducted Susceptibility – Power Line Measurement Documents: Burst/Transients: IEC1000-4-4 (IEC 801-4) Surge: IEC1000-4-5 (IEC 801-5) Voltage fluctuations: IEC1000-4-1 (IEC 801-1)

3.2 Testing

3.2.1 ESD Immunity The unit was tested and evaluated by: Smith Electronics *

3.2.2 Radiated Immunity – RF Electric Field The unit was tested and evaluated by: Smith Electronics *

3.2.3 Conducted Immunity – Power Line Testing to IEC801-4 was conducted by: Smith Electronics *

* Smith Electronics
8200 Snowville Rd.
Cleveland, OH 44141 (USA)

4.0 Low Voltage Directive

4.1 Standards Applied

3.1.1 Low Voltage Directive EN60950



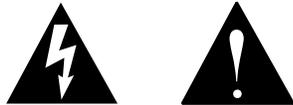
This device complies with the requirements of EEC Council Directives: 93/68/EEC (CE marking); 73/23/EEC (safety-low voltage directive); 89/336/EEC (electromagnetic compatibility)

Conformity is declared to the following standards: EN50081-1, EN50082-1, IEC/EN60950.

Use of Shielded Cables

In order to conform to the CE requirements for HF radiation, shielded cables should be used for the audio and data connections. For audio connections, the cable shield should be connected to the XLR shell.

18 Safety Notification



- 1. Read All Instructions.** All safety and instructions must be read before operating the product.
- 2. Retain All Instructions.** All safety and operating instructions must be maintained for future reference.
- 3. Heed All Warnings.** All warnings on the product and those listed in the operating instructions must be adhered to.
- 4. Follow All Instructions.** All operating and product usage instructions must be followed.
- 5. Heat.** This product must be situated away from any heat sources such as radiators, heat registers, stoves, or other products (including power amplifiers) that produce heat.
- 6. Water and Moisture.** Do not use this product near water.
- 7. Attachments.** Do not use any attachments not recommended by the product manufacturer as they may cause hazards.
- 8. Power Sources.** This product must be operated from the type of power source indicated on the marking label and the installation instructions. If you are not sure of the type of power supplied to your facility, consult your local power company.
- 9. Grounding and Polarization.** This product is equipped with a polarized AC plug with integral safety ground pin. Do not defeat the safety ground in any manner.
- 10. Power Cord Protection.** Power supply cords must be routed so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to the cords at AC wall plugs and convenience receptacles, and at the point where the cord plugs into the product.
- 11. Lightning.** For added protection during a lightning storm, or when the unit is left unattended or unused for long periods of time, unplug the unit from the AC wall outlet. This will prevent damage to the product due to lightning and power surges.
- 12. Overloading.** Do not overload AC wall outlets, extension cords, or integral convenience outlets as this can result in a fire or electric shock hazard.

- 13. Object and Liquid Entry.** Never push objects of any kind into this product through openings as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock. Never spill liquid of any kind on the product.
- 14. Accessories.** Do not place this product on an unstable cart, stand, tripod, bracket or table. Any mounting of the product needs to follow the manufacturer's instructions.
- 15. Servicing.** Refer all servicing to qualified service personnel.
- 16. Damage Requiring Service.** Unplug this product from the wall AC outlet and refer servicing to qualified service personnel under the following conditions:
 - a. When the AC cord or plug is damaged.
 - b. If liquid has been spilled or objects have fallen into the product.
 - c. If the product does not operate normally (following operating instructions).
 - d. If the product has been exposed to rain or water.
 - e. If the product has been dropped or damaged in any way.
 - f. When the product exhibits a distinct change in performance (outside of normally operating specifications).
- 17. Replacement Parts.** When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer. Unauthorized substitutions may result in fire, electric shock, or other hazards.
- 18. Safety Check.** Upon completing of any repairs to this product, ask the service technician to perform safety checks to determine that the product is in proper operating condition.
- 19. Cleaning.** Do not use liquid cleaners or aerosol cleaners. Use only a damp cloth for cleaning the exterior of the product.

Manual History

- 1.1 SS 10/2007
- 1.2 ILR 11/2007
- 1.3 SS/ILR 12/2007
- 1.4 THI 11/2008