

◀ ACCESS ▶
2USB

Product Manual

COMPREX

I. ACCESS 2USB MANUAL

I. INTRODUCTION	11
UNPACKING AND CHECKING CONTENTS	11
ABOUT ACCESS 2USB PORTABLE	12
ABOUT CROSSLOCK	13
ABOUT POTS	13
II. HARDWARE CONTROLS AND CONNECTIONS	14
III. A SIMPLE 2USB REMOTE BROADCAST	18
IV. INTRODUCTION TO CROSSLOCK	20
V. INTRODUCTION TO SWITCHBOARD	21
VI. NAVIGATING THE TOUCHSCREEN DISPLAY	22
TOP AND BOTTOM NAVIGATION BARS	22
VII. NETWORK MENU	24
MANAGE NETWORKS	24
CONFIGURE NETWORKS	24
ADD NETWORK	25
ENABLE AND DISABLE DEVICES	25
DELETE DEVICES	26
CONFIGURE MENU TABS	27
CONFIGURING 3G/4G DATA MODEMS	30
CONFIGURING THE ETHERNET PORT	30

SELECTING STATIC OR DYNAMIC	30
DYNAMIC ADDRESSING	31
STATIC ADDRESSING	31
WEB BROWSER	32
VIII. REMOTES MENU	34
<hr/>	
TEST REMOTE ENTRIES	34
REMOTES LISTED FROM SWITCHBOARD	34
CONNECTING AND DISCONNECTING TO REMOTES	35
ADD NEW REMOTE	36
EDIT REMOTES	37
DELETE REMOTES	37
IX. STATS MENU	38
<hr/>	
X. CONFIGURE MENU	40
<hr/>	
AUDIO CONTROLS	41
MIXER AUDIO	42
USER INTERFACE CONFIGURATION MENU	43
XI. PROFILES MENU	44
<hr/>	
VIEWING PROFILE DETAILS	44
DEFAULT PROFILE	45
XII. SYSTEM SETTINGS MENU	46
<hr/>	
CONNECTION SETTINGS	46
CONTACT CLOSURES SETTINGS	48

SECURITY SETTINGS	49
SWITCHBOARD SERVER	50
BRIC NORMAL SETTINGS	50
STANDARD RTP SETTINGS	51
TCP SETTINGS	52

XIII. PINOUTS **53**

PINOUTS - AUDIO	53
PINOUTS - SERIAL PORT	53
PINOUTS - CONTACT CLOSURES	54

XIV. ABOUT THE ALGORITHMS **55**

OPUS	55
LINEAR PCM	55
FLAC	55
G.711	56
G.722	56
AAC	56
HE-AAC	56
HE-AACV2	56
AAC-LD	56
AAC-ELD	56

XV. SWITCHBOARD TRAVERSAL SERVER (TS) **59**

CONFIGURING SWITCHBOARD	59
LOGGING IN AND SETTING UP SWITCHBOARD	59
CREATING USERS	61
CONTACT LISTS	62

SHARES	63
MANAGING MULTIPLE CONTACT LISTS	65
BULK ACTIONS FOR CONTACT LISTS	67
SWITCHBOARD THEORY AND CONCEPTS	69
XVI. CROSSLOCK DETAILS	73
<hr/>	
CROSSLOCK AND SWITCHBOARD	74
MAKING CROSSLOCK CONNECTIONS VIA SWITCHBOARD	75
MAKING CROSSLOCK CONNECTIONS WITHOUT SWITCHBOARD	76
CROSSLOCK STATS	77
DELAY SLIDER	78
XVII. DEVICE MANAGER	80
<hr/>	
USING DEVICE MANAGER	80
XVIII. TOOLBOX	83
<hr/>	
LOCATIONS	84
CONFIGURING WI-FI	84
ADVANCED NETWORK SETTINGS IN TOOLBOX	86
XIX. MAKING NON-CROSSLOCK CONNECTIONS IN FIRMWARE 4.0	87
<hr/>	
XX. OPERATING ACCESS IN A 24/7 ENVIRONMENT	88
<hr/>	
SETTING ACCESS FOR 24/7 OPERATION	89
XXI. MAKING EBU 3326/SIP COMPATIBLE CONNECTIONS	91
<hr/>	
MORE ABOUT EBU 3326	91

EBU 3326 IN ACCESS	91
EBU 3326/SIP MODES	91
UNREGISTERED MODE	92
REGISTERED MODE	92
SIP SERVERS	92
SIP URIS	92
REGISTERING WITH A SERVER	92
MAKING SIP REGISTERED CALLS	94
SIP TROUBLESHOOTING	95
OUTGOING CALL ISSUES	95
INCOMING CALL ISSUES	95
SOLUTIONS	96
STUNNING SUCCESS	96
FIX OF LAST RESORT	96

XXII. MULTI-STREAMING **97**

XXIII. IP MULTICAST **99**

MULTICAST PROFILES	99
SETTING UP A MULTICAST REMOTE	100
TIME-TO-LIVE	100
CHANGING PORT NUMBERS FOR MULTICAST	101

XXIV. LEGACY STATS **102**

CHANNEL STATS	102
PEER STATS	103

XXV. STREAMING SERVER FUNCTION	105
<hr/>	
DECODING A HTTP STREAM	105
SIMULTANEOUSLY CONNECTING ACCESS AND STREAMING	105
XXVI. WEB-BASED INTERFACE INTRODUCTION	106
<hr/>	
XXVII. WEB-BASED INTERFACE CONNECTIONS MENU	108
<hr/>	
CONNECTIONS TAB	108
TEST REMOTE ENTRIES	108
REMOTES LISTED FROM SWITCHBOARD	109
CONNECTING AND DISCONNECTING TO REMOTES	109
ADD NEW REMOTE	110
EDIT REMOTES	112
DELETE REMOTES	112
XXVIII. WEB-BASED INTERFACE STATISTICS MENUS	113
<hr/>	
XXIX. WEB-BASED INTERFACE PROFILES MENU	114
<hr/>	
VIEWING PROFILE DETAILS	114
DEFAULT PROFILE	115
XXX. WEB-BASED INTERFACE SYSTEM SETTINGS MENU	116
<hr/>	
GLOBAL SETTINGS	116
SWITCHBOARD SERVER	117
CONTACT CLOSURES SETTINGS	118
AUX SERIAL SETTINGS	119

SECURITY SETTINGS	120
BRIC NORMAL SETTINGS	121
MODEM SETTINGS	122
EBU 3326/SIP SETTINGS	122
CROSSLOCK VPN SETTINGS	122
SOFTWARE LICENSING	123
XXXI. GATEWAY OPERATION	124
<hr/>	
ABOUT GATEWAY OPERATION	124
CONNECTING AS A GATEWAY	124
GATEWAY SETUP	125
XXXII. ADVANCED 3G/4G NETWORK SETTINGS	126
<hr/>	
XXXIII. POTS (PLAIN OLD TELEPHONE SERVICE) CODEC CONNECTIONS	127
<hr/>	
POTS CODEC SET-UP FOR ACCESS COMPATIBILITY	127
USING ACCESS WITH POTS	127
RATE VS. RETRAIN	128
TROUBLESHOOTING POTS CONNECTION	129
XXXIV. ADVANCED SETTINGS	130
<hr/>	
ADVANCED NETWORK SETTINGS	130
ADVANCED REMOTE SETTINGS	131
PROFILE SETTINGS	132
LOCAL & REMOTE SETTINGS	134
ADVANCED PROFILE SETTINGS	135

ADVANCED SYSTEM SETTINGS	138
AUXILIARY SERIAL	138
CONNECTIONS	139
SECURITY	140
SWITCHBOARD SERVER	141
BRIC NORMAL SETTINGS	141
EBU 3326/SIP SETTINGS	143
HTTP SETTINGS	145
MODEM SETTINGS	146
STANDARD RTP SETTINGS	147
TCP SETTINGS	148
CROSSLOCK SETTINGS	148
HOTSWAP	151

XXXV. ADVANCED TOPICS **155**

Q: CAN I GET A REMOTE INDICATION THAT ACCESS IS CONNECTED TO SOMEONE?	155
Q: WHAT STEPS SHOULD I TAKE WHEN I'M HAVING CONNECTION PROBLEMS WITH ACCESS?	155
Q: HOW CAN I OPTIMIZE SETTINGS FOR EVDO, UMTS, OR OTHER WIRELESS ACCESS?	155
Q: MY IT GUY IS CONCERNED ABOUT SECURITY AND WANTS TO KNOW WHAT SERVICES ARE OPEN ON THIS BOX.	156
Q: I NOTICE IN THE ADVANCED OPTIONS THAT I CAN CHANGE MY STREAMING FROM UDP TO TCP. SHOULD I?	156

XXXVI. APPENDIX A - IP COMPATIBILITY **157**

XXXVII. APPENDIX B - INFORMATION FOR IT MANAGERS **159**

INCOMING SERVICES	159
OUTGOING SERVICES	159

XXXVIII. APPENDIX C - USING ACCESS ON UNIDIRECTIONAL NETWORKS **160**

DECODE SIDE SETTINGS ONLY **160**

ENCODE SIDE SETTINGS ONLY **160**

FULL-TIME OR TRIGGERED CONNECTIONS **160**

XXXIX. APPENDIX D - USING THE COMREX ACCESS DECODER DOWNMIX FUNCTION **161**

XL. APPENDIX E - SPECIFICATIONS **163**

CONNECTIONS **163**

AUDIO SPECIFICATIONS **163**

POWER **163**

PHYSICAL **163**

XL. APPENDIX F - MAKING CONNECTIONS TO MULTIRACK **164**

XLI. COMREX SWITCHBOARD TRAVERSAL SERVER USE **166**

XLII. LICENSE AND WARRANTY DISCLOSURES FOR COMREX ACCESS **167**

LICENSES **167**

WARRANTY **168**

XLIII. CONFORMITY INFORMATION **170**

EC DECLARATION OF CONFORMITY FOR R&TTE DIRECTIVE **171**

I. INTRODUCTION

Congratulations on purchasing the Comrex ACCESS codec system with BRIC technology. ACCESS products are the result of years of our research into the state of IP networks and audio coding algorithms. It is our hope that this technology will unleash the imagination of the user, enabling more creative and entertaining programming to be broadcast from more diverse and interesting locations.

UNPACKING AND CHECKING CONTENTS

The following items are shipped with a new ACCESS 2USB Portable:

- 1 ACCESS 2USB Portable Stereo BRIC IP Codec
- 2 Lithium-ion battery pack
- 3 Touch-screen stylus
- 4 USB POTS Modem
- 5 Edimax Wi-Fi USB Adapter
- 6 AC Power adapter with cord
- 7 Manual on CD
- 8 Printed QuickStart Guide
- 9 Warranty card*

*Please take a few moments to fill out and return the warranty card. This helps both us and you; us, so we know you got the unit successfully, and you, if for any reason you ever need to discuss any warranty issues with us.

ABOUT ACCESS 2USB PORTABLE

ACCESS 2USB Portable provides a robust, high quality, low-delay, full-duplex audio link over challenging IP networks like the public Internet.

ACCESS Portable has several features:

- Intuitive touchscreen user interface.
- Built-in Ethernet port.
- 2 USB ports for use with USB 3G/4G modems, the supplied Wi-Fi adapter, or POTS modem.
- Battery Pack with internal charger (capable of up to 6 hours of power when fully charged with no accessories).

ABOUT BRIC

The heart of ACCESS is called BRIC; Broadcast Reliable Internet Codec. Despite the many challenges the public Internet presents, ACCESS is designed to perform over the majority of available connections and be the most reliable connection possible.

BRIC is a breakthrough technology. BRIC hardware delivers audio over the public Internet in much the same way that ISDN and POTS codecs have done in the past.

BRIC consists of three elements:

- 1 ACCESS Rackmount: Designed for installation in a radio station's "remote rack" and configured to be "always-on".
- 2 ACCESS 2USB Portable: Engineered to be as easy to use as possible on the road. It features small size, battery power, and clip-on mixer and headphone drivers, along with an audio codec capable of remarkable quality on the public Internet.
- 3 Switchboard: Switchboard is a traversal server hosted by Comrex that exists on the public Internet and makes connections between ACCESS codecs simpler.

Although using Switchboard is optional, it removes worries about dynamic IPs, NATs, and other concerns that can make peer-to-peer connections over the Internet difficult. Comrex recommends that users take advantage of Switchboard to make remotes easier to set up and more robust.

ABOUT CROSSLOCK

CrossLock is a new software addition that, in conjunction with the Switchboard, does the “heavy lifting” of breaking through Network Address Translator (NAT) routers. This allows your codecs to see each other over a VPN as if it were a LAN.

Because CrossLock creates a VPN, it has its own rules. It can decide whether or not to resend information based on error correction. It can also handle preventative forward-error-correction (FEC). These decisions make up the “secret sauce” of Crosslock, and make it effective at navigating “bad” networks and avoiding networks that are “beyond repair”.

CrossLock can also signal encoders to “throttle down” their data rate if necessary. This reduces quality but maintains higher reliability.

The overall result of CrossLock’s function means a higher level of reliability for remotes. This goes a long way towards eliminating the frustration of dropouts and other failures during a broadcast.

ABOUT POTS

ACCESS is also a POTS codec. It comes with a USB POTS modem that can make phone calls over analog phone lines directly to other units. In this mode, ACCESS can communicate with other ACCESS devices, or with a range of previous generation Comrex POTS codec devices.

II. HARDWARE CONTROLS AND CONNECTIONS

To start, we are going to go over all of the connections and controls of the ACCESS 2USB.

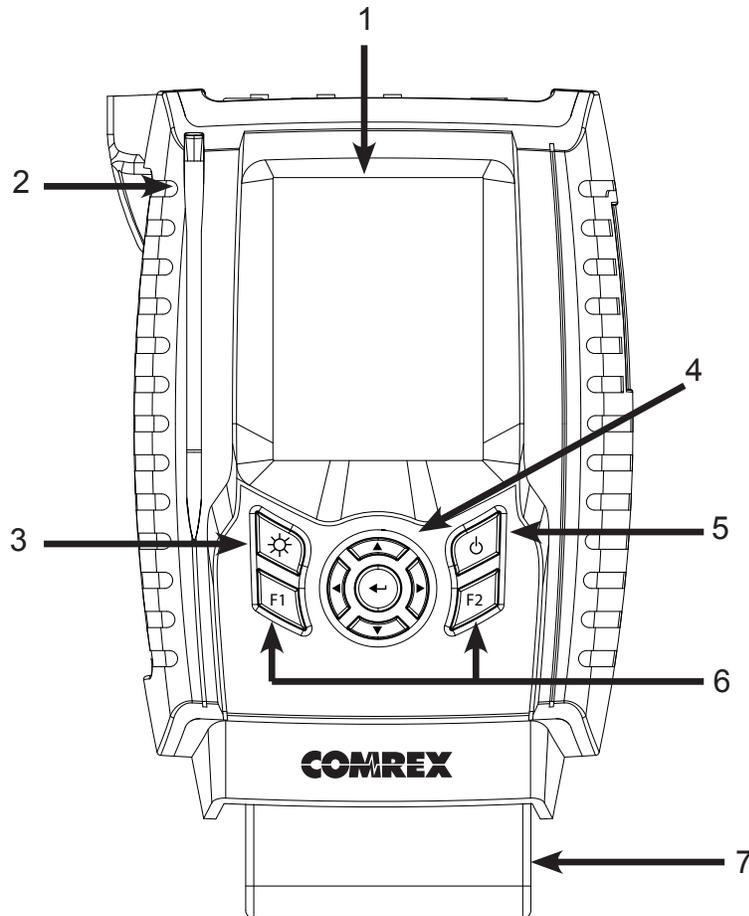


FIGURE 1 FRONT PANEL DIAGRAM AND DESCRIPTIONS

- 1 **DISPLAY** - Touchscreen display that responds to the attached stylus. This is where you initialize your broadcast from the 2USB to the studio unit (typically an ACCESS Rackmount), view and edit settings, and monitor connections.
- 2 **STYLUS** - Used on the 2USB display for navigating and selecting options in the user interface.
- 3 **BACKLIGHT KEY** - Controls operation of the display light.
 - a Hold for one second to enable power saving mode, which turns the LCD backlight off after ten seconds. In this mode, pressing the button again will turn the light on for another ten seconds.
 - b Hold for one second to enter toggle mode, where each short press will turn light on/off.
 - c Hold for one second to return to default "Always-on" mode.

- 4 **DIRECTION CURSORS & ENTER KEY** - May be used instead of touchscreen to navigate and select options in the user interface.
- 5 **POWER KEY** - Hold this button down for one second to turn the ACCESS 2USB Portable on or off.
- 6 **F1 & F2 KEYS** - The F1 key may be used to access the top menu bar. The F2 key is user programmable.
- 7 **BATTERY** - Lithium-ion clip-on battery pack. Can power the 2USB for up to 6 hours without any accessories plugged in.

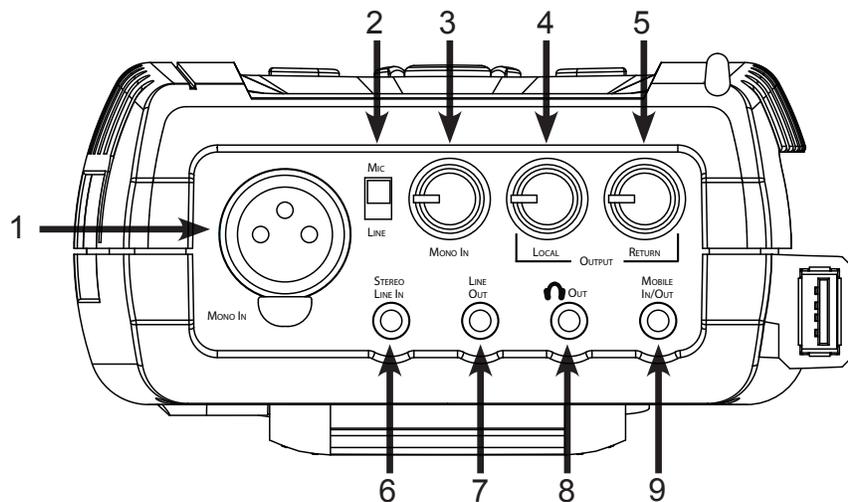


FIGURE 2 TOP PANEL DIAGRAM AND DESCRIPTIONS

- 1 **MONO IN** - This 3-pin female XLR connector is designed to accept a balanced, microphone or line level audio feed. This input level is adjustable via the **Mono In** control, shown as #3. +12 V of phantom power may be applied to this input through the **Audio Controls** menu.
- 2 **MIC/LINE SWITCH** - This switch determines whether the **Mono In** jack is configured to receive a microphone level (-70 to -40 dBu) or line level (-10 to +4 dBu) audio input.
- 3 **MONO IN control knob** - Use this knob to adjust the level of **Mono In** audio (the XLR input) that you are sending back to the studio. To adjust, press the knob in to extend, make adjustments, and then push back in.
- 4 **LOCAL OUTPUT control knob** - Adjusts the level of local audio to the headphone jack (#8). To adjust, press the knob in to extend, make adjustments, and then push back in.
- 5 **RETURN OUTPUT** - Adjusts the level of return audio to the headphone jack (#8). To adjust, press the knob in to extend, make adjustments, and then push back in.
- 6 **STEREO LINE IN** - This 3-conductor 1/8" (3.5 mm) connector is designed to accept unbalanced stereo input devices. The input level is not adjustable.
- 7 **LINE OUT** - This 3-conductor 1/8" (3.5 mm) connector delivers unbalanced output audio. The output is selectable in the software to be either **Local**, **Return**, or both.

- 8 **HEADPHONE OUT** - This 3-conductor 1/8" (3.5 mm) connector is designed to deliver audio to low impedance headphones. The output audio can be user-adjusted by the **LOCAL** and **RETURN OUTPUT** knobs.
- 9 **MOBILE IN/OUT** - This is a 3-conductor 1/8" (3.5 mm) connector for attachment of a hands-free cellular port. Program audio is sent to this port, and receive audio may be routed to the **HEADPHONE/LINE OUTPUT**.

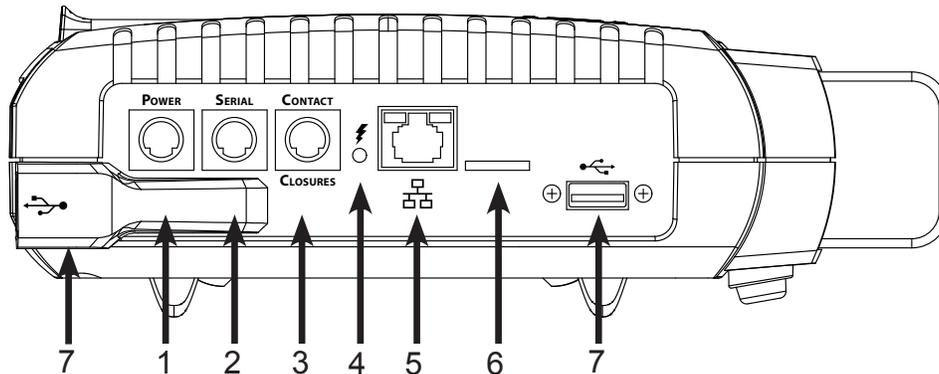


FIGURE 3 LEFT PANEL DIAGRAM AND DESCRIPTIONS

- 1 **POWER CONNECTION** - This is a 5-pin mini-DIN jack for connection of the included AC power adapter. Adapter works from 100-240 VAC. (Be sure to use only Comrex-supplied power adapter.)
- 2 **SERIAL JACK** - This is an 8-pin mini-DIN jack for connection of a serial cable to facilitate ancillary data transfer. See **Pinouts - Serial Port on page 53** for details.
- 3 **CONTACT CLOSURES** - This 9-pin mini-DIN jack is used for contact closure input and outputs. See **Pinouts - Audio on page 53** for details.
- 4 **CHARGE INDICATOR** - Indicates the battery charging state: Red = Charging; Green = Fully Charged.
- 5 **10/100BASET ETHERNET** - For connection to wired IP networks. Next to the Ethernet Port are two LEDs to indicate what type of network you are connected to: Green = 10 Mbit; Red = 100 Mbit. These LEDs also indicate network activity: Off = not connected; Solid = Link OK; Blinking = RX/TX Activity.
- 6 **MICRO SD CARD SLOT** - For future use.
- 7 **USB HOST PORTS** - These ports are for connections to the included USB Wi-Fi adapter, POTS modem, Comrex Connect Modems, and USB 3G/4G devices. (Not all USB 3G/4G devices are compatible. Check our website for the current compatible modems at: www.comrex.com/products/compatible-3g4g-modems/)

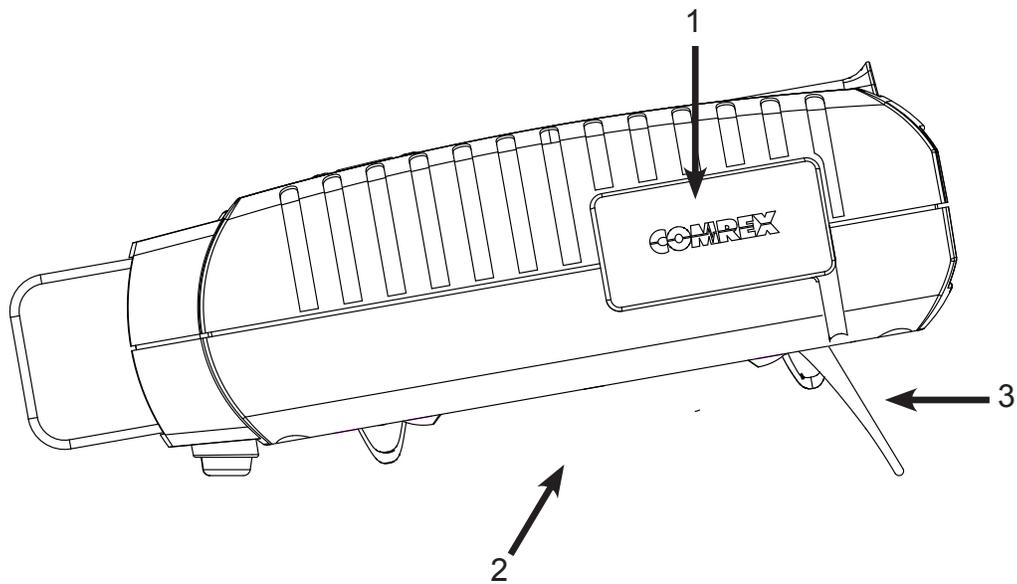


FIGURE 4 RIGHT AND BOTTOM PANEL DIAGRAM AND DESCRIPTIONS

- 1 **MIXER DOCKING PORT** - This connector is for docking to the optional five-channel ACCESS Mixer.
- 2 **ADJUSTABLE STRAP** - Use this padded adjustable strap to carry the unit.
- 3 **EASEL FEET** - Pull the feet out from the bottom of the unit to allow desktop use.

MONO VS. STEREO

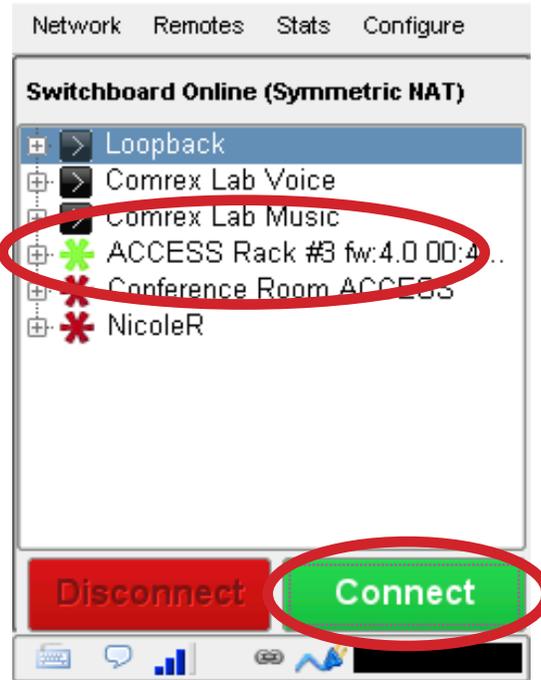
Because ACCESS can encode and/or decode in stereo and mono modes, it's important to understand how the audio inputs and outputs are handled in each mode.

Inputs - ACCESS 2USB Portable **Mono In** is always delivered to both the left and right encoder inputs in stereo encoder modes. In mono encoder modes, the left channel of the stereo line input is delivered to the mono encoder.

Outputs - In stereo decoder modes, left and right channels are delivered to the **Line Out** and **Headphone** connectors separately. In mono decoder modes, mono audio is delivered to both sides of the line out and headphone connectors.

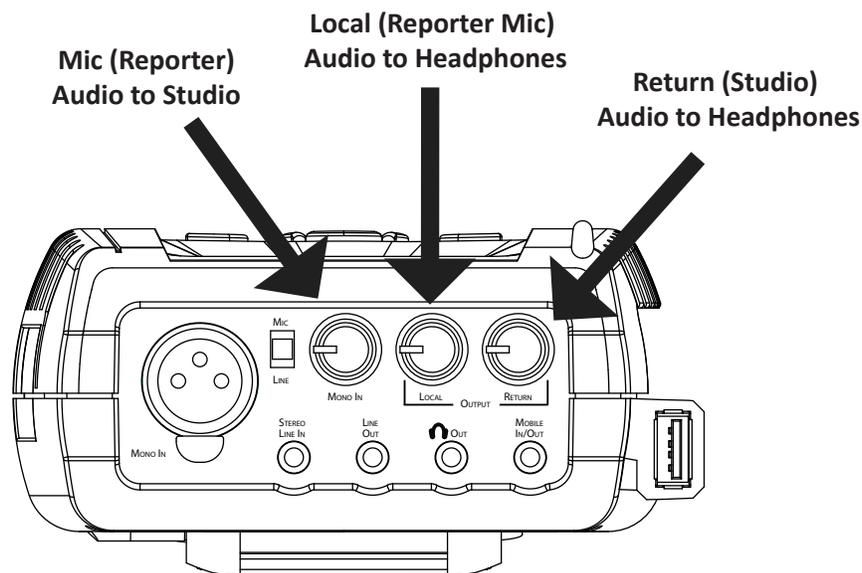
Let's assume your codec fleet has an account on the Comrex Switchboard server, and both ends of your connection are properly registered with it in advance. Navigate to **Remotes->Manage Connections**. This page contains the information needed to connect to a device. Units that are in your Switchboard account on the same contact list will automatically appear in this list with a gear icon next to it.

Select the remote in the list and select **Connect** at the bottom right of the screen. Your unit will now connect to the rackmount at the studio.



Once finished, select **Disconnect** at the bottom of the screen.

Audio level meters for both the local and return (remote) audio are in the bottom right of the display. Adjustments can be made on the audio levels being sent to the studio and on your headphones using the knobs on the top of the 2USB. To adjust, push the knob of the level you want to adjust in so that it extends out, make the adjustment, and then push the knob back in.



IV. INTRODUCTION TO CROSSLICK

CrossLock describes a new reliability layer that gets established between Comrex devices in advance of a connection. This layer takes the form of a virtual private network (VPN) between the devices. The ACCESS media stream is carried within this VPN.

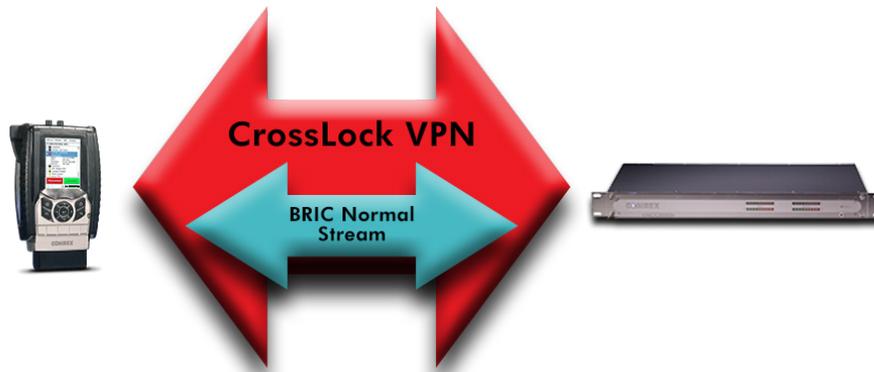


FIGURE 5

In addition to carrying the audio media, **CrossLock** allows lots of other information to be shared between the endpoints, including information about network quality and far-end delay settings. This provides for much better delay management on both ends of the link.

One or both ends of a **CrossLock** connection can utilize multiple network interfaces. This can take the form of two Ethernet connections, or any mix of wired and wireless networks. A common usage scenario would be attaching two 3G/4G modems to ACCESS 2USB. In the case of one network underperforming, the majority (or all) of the data will be sent on the good network.

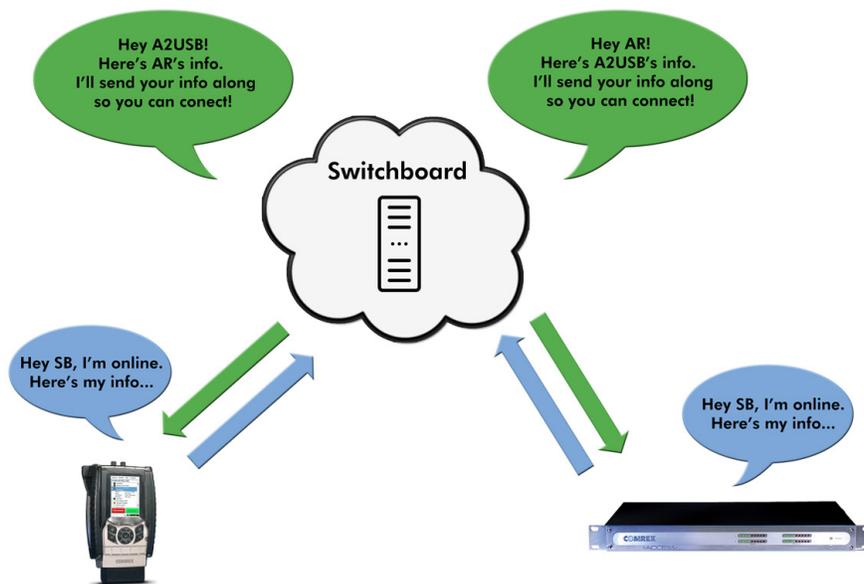
For more information on CrossLock, go to the **CrossLock Details on page 69**.

v. INTRODUCTION TO SWITCHBOARD

Switchboard is a feature that allows codecs to “sync” with a cloud-based server. Switchboard allows for easy connections to be made between codecs without any knowledge of IP addresses on both ends of the link. It also provides presence and status information about all the Comrex codecs in your fleet, and can help make some connections through routers and firewalls that might otherwise be difficult.

Comrex highly recommends setting up and utilizing Switchboard with your codecs. If you do not have an account, contact us at info@comrex.com or 978-784-1776/1-800-237-1776.

When codecs are turned on and have network connectivity, they open a channel to the **switchboard.comrex.com** server, and provide the current public IP address, connection status, firmware revision, and the type of router (if any) that exists in the link.



Switchboard recognizes devices by their Switchboard ID (MAC Address) and provides information to any units in the same Switchboard fleet that are also online.

To learn more about Switchboard and how to utilize it with your codecs, visit the section **Switchboard Theory and Concepts on page 64**.

vi. NAVIGATING THE TOUCHSCREEN DISPLAY

All options on the ACCESS touchscreen may be selected via the included stylus. To navigate through the menus, tap one of the menu items at the top of the screen and then select from the drop-down list. For text entry, a pop-up keypad (pickboard) is available to allow each character to be selected individually. It is located in the bottom left of the display. 

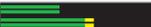
TOP AND BOTTOM NAVIGATION BARS

When navigating through the different menus on the 2USB touchscreen, the top and bottom navigation bars will always be available.

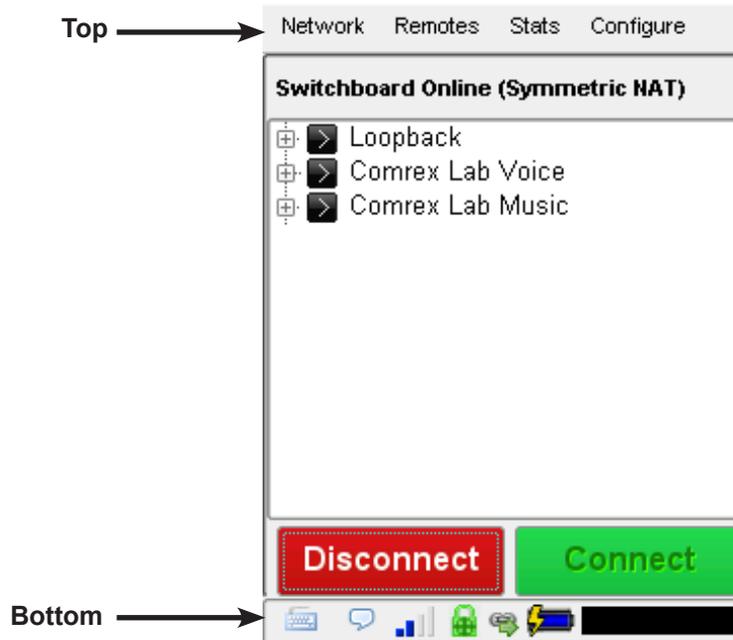
The top bar contains four tabs:

- **Network** - Enable and disable various network devices, and configure IP, Wi-Fi, and other Internet parameters.
- **Remotes** - Enter and configure the addresses and profiles of outgoing connections. Essentially, this tab contains an editable “phone book” of places you connect to.
- **Stats** - View network performance data of active connections
- **Configure** - Create profiles for outgoing connections, manage how incoming connections are treated, and change configurations of additional features like audio controls, CrossLock settings, contact closures and incoming password security.

The bottom bar contains the following:

-  **Pickboard** - Allows use of the pop-up keyboard for text entry.
-  **Chat** - Jumps immediately to the chat screen/pickboard, allowing text messaging to other ACCESS users.
-  **CrossLock status** - CrossLock connection indicator. Green = connected and active.
-  **Link status** - Unbroken Link = Network ready, not connected to remote.
 - ◊ **Broken Link** = Network unavailable.
 - ◊ **Link with Arrow** = Connected to remote.
 - ◊ **Link with Warning Triangle** = Connected to remote but no network (i.e. network connectivity lost during connection).
-  **Battery level** - Shows current battery level or charge status.
-  **External Power status** - Shows power supply is plugged into the unit and supplying power.
-  **Audio meters** - Displays current send/receive audio levels on the device. You may jump from this low-resolution meter to a larger, easier to read version by tapping the meter. Tap the smaller meter again to return.

- **Wireless signal strength** - Displays wireless signal strength when a Wi-Fi or other wireless adapter, such as a 4G modem, is plugged in. **Note: Not all 3G/4G adapters will show network strength.**
- **Number of wireless network devices** - This shows multiple wireless devices are connected to the 2USB with network connectivity. We do not recommend utilizing more than 2 networks at a time since it will cause the system to lag. Even if you have more than 2 wireless networks being utilized, it will still only show 2 on the bottom navigation.



Tip: The touchscreen may be locked by pressing the Backlight key along with F2. A warning message will be displayed when attempting to use the unit with the screen locked. Pressing the two keys a second time will unlock the touchscreen.

vii. NETWORK MENU

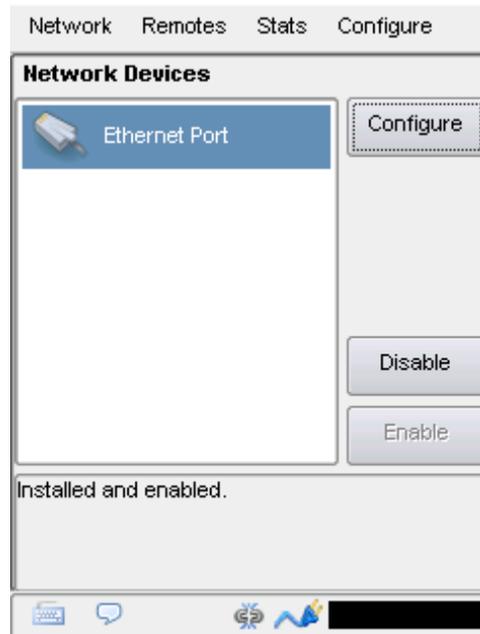
The **Network** menu has 4 drop-down options: **Manage Networks**; **Configure Network**; **Delete Network**; and **Web Browser**.

MANAGE NETWORKS

Manage Networks is where you can view, configure and enable your network devices.

ACCESS 2USB has the capability to work over several types of networks through the use of USB adapters attached to one of the USB ports. Once a compatible device is connected into one of the USB ports, an icon will appear on the **Manage Networks** screen. Devices can be individually enabled and configured via this interface.

At first, only the Ethernet port is available for enabling and configuration.

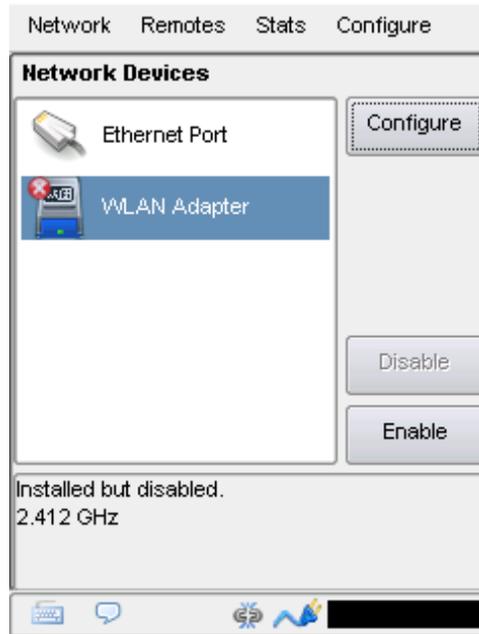


CONFIGURE NETWORKS

The following section will go over the basic configuration for the Ethernet port, the provided WLAN Adapter (Wi-Fi), and a typical 3G/4G USB device. To learn about POTS connections, visit the section **POTS Codec Connections** on page **123**.

ADD NETWORK

When a USB device is first plugged into the 2USB, a device entry will appear with a red “x” on the icon and the box below the list will say “Installed but disabled”.



ENABLE AND DISABLE DEVICES

Many new devices will need to be enabled by the user with the exception of the Ethernet port and POTS modem as they will be enabled automatically.

To enable a device, select the entry in the list and tap the **Enable** button towards the bottom right. To disable, select the entry in the list and tap the **Disable** button. When an accessory network device is disabled, it means that it is put into its low-power state, if applicable.

TIP: To change the name of the device entry so you can easily identify a device from the Manage Networks menu, select the device, select the Configure button, navigate to the Settings tab and select the name parameter. Click Edit, then click the keyboard icon in the bottom left to bring up the virtual keyboard. Enter a new name, select the keyboard icon to hide the keyboard, and then press Save.

DELETE DEVICES

If a device is removed from the 2USB, the entry will remain in the list, but the icon will be greyed out. This is when you can utilize the **Delete Network** menu option.

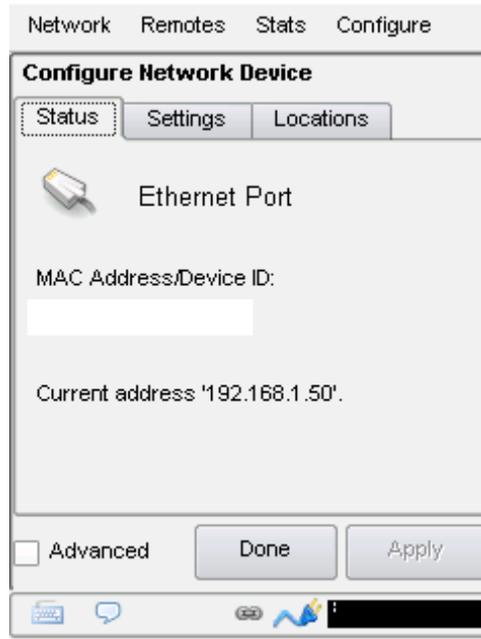


To delete a device, select it in the list (remember, it must be removed from the device), and navigate to **Network->Delete Network**.

Note: The Ethernet port entry does not behave the same as other device entries. It does not grey out and it can not be deleted.

CONFIGURE MENU TABS

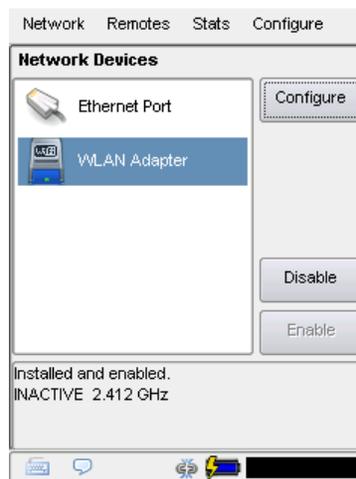
When you enter into the configuration of devices, there will always be three tabs: **Status**, **Settings**, and **Locations**. If configuring the WLAN Adaptor (Wi-Fi), there will also be a **Scan** tab. The MAC Address of the unit is displayed in the Status Tab. This is needed for the unit's Switchboard ID when adding to Switchboard, or in manual CrossLock connections.



CONFIGURING WLAN ADAPTER (WI-FI)

Insert a supported USB Wi-Fi adapter (such as an Edimax EW-7811UAC).

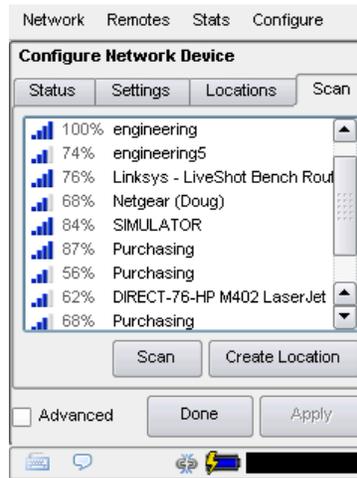
Go to **Network->Manage Networks** and select the appropriate WLAN Adapter entry.



Next, press the **Configure** button on the right-hand side of the screen.

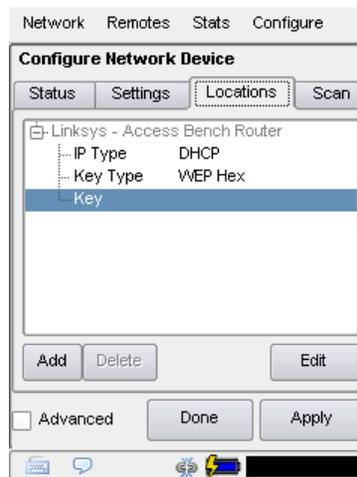
Select the **Scan** tab and press the **Scan** button near the bottom of the screen. This action will take a few moments to populate a list of the local hotspots.

Select your desired hotspot and press the **Create Location** button.



You will now be directed to the **Locations** tab.

Tip: Locations are entries you can save so that you can easily select and apply network configurations at different corresponding locations.



If the connection requires a password, select the **Key** parameter and press the **Edit** button near the bottom of the screen.

Press the keyboard icon in the lower left-hand corner of the screen to display the virtual keyboard. Enter in the password and press the keyboard button again. Press **Save**.

TIP: The **Locations** tab is where you can change the network location name (factory default is “Default”). Users may enter a name such as “Coffee Shop on the Corner” or “Weather Bureau” to help easily identify the network to connect to, depending on which location they are physically at.



Select the **Settings** tab and confirm that the **Active Network Location** is pointing towards the intended hotspot name, or is set to **Automatic***. If it is not, select the **Active Network Location** parameter and press the **Edit** button. Press the drop down list and select the appropriate location. Press **Save**.

*Automatic mode will scan for entries that are in your Locations list and connect to the first one in range that is recognized.



Press **Apply**.

You will be brought back to the **Manage Networks** screen and the adapter will negotiate with the hotspot to acquire a current IP address. This may take a few moments. When an IP address shows in the box below, you have successfully connected to the Wi-Fi hotspot and are now connected to the Internet. **Note:** The MAC Address of the adapter can be found in **Configure->Status Tab**.

CONFIGURING 3G/4G DATA MODEMS

3G/4G modems vary in their interface. Comrex is constantly updating drivers to work with the most popular devices. Visit our ACCESS Support section on our website to view our most recent compatible 3G/4G devices or contact us about specific devices. <http://www.comrex.com/products/compatible-3g4g-modems/>

If a device has driver support, it will appear automatically in the **Network Devices** list. Many of the devices will behave like a “plug-n-play” device. Once the device is enabled and an IP address is assigned, the 2USB will be capable of establishing connections for your broadcast.

Tip: Some devices require being plugged into a computer to perform necessary updates and configuration before being able to work with the 2USB. This is typically only needed before the first time you plug it into the 2USB.

CONFIGURING THE ETHERNET PORT

The following will be covering network topics and will be presented with the assumption that the reader has basic understanding on general networking and IP addressing.

The default network connection is via a standard 10/100baseT Ethernet jack. ACCESS 2USB contains an embedded computer with a Linux-based operating system and a full network protocol stack. This means that 2USB will typically look like an ordinary computer to a network.

There are 3 addressing options available with the 2USB when utilizing the ethernet port: **Dynamic**; **Static**; and **Gateway**. For this section, we will go over the **Dynamic** and **Static** addressing options only, as **Gateway** is an advanced option and will be covered in the advanced sections of this manual.

SELECTING STATIC OR DYNAMIC

When you select the Ethernet port in the **Network Device** list and select **Configure**, there will be three tabs available. Click on the **Locations** tab and either select the default entry and then **Edit**, or select **Add** to create a new entry.

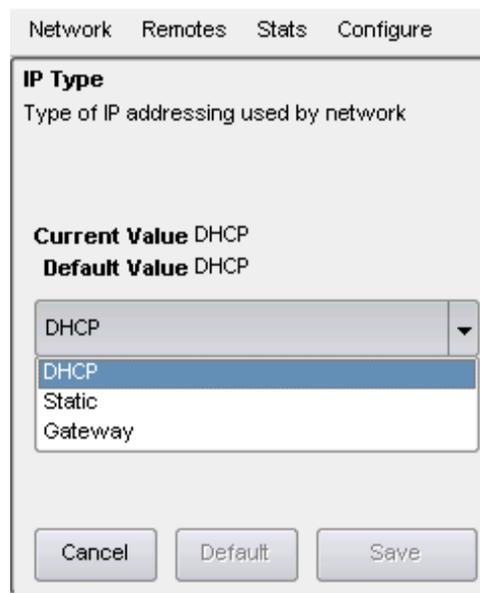
Once you have selected the default entry or created a new entry, you can expand to see the editable parameters by tapping the plus sign (+) next to the entry on the left. Here, you can edit/enter a name for the location as well as choose the IP type.

DYNAMIC ADDRESSING

If you leave the IP type set to dynamic, there should not be additional configuration needed. The 2USB should be assigned an IP address automatically when plugged into a network.

If you are not receiving an IP address and/or cannot establish an internet connection when you plug the unit into a network with the DHCP addressing type selected, then you will need to contact your IT department to help troubleshoot your network.

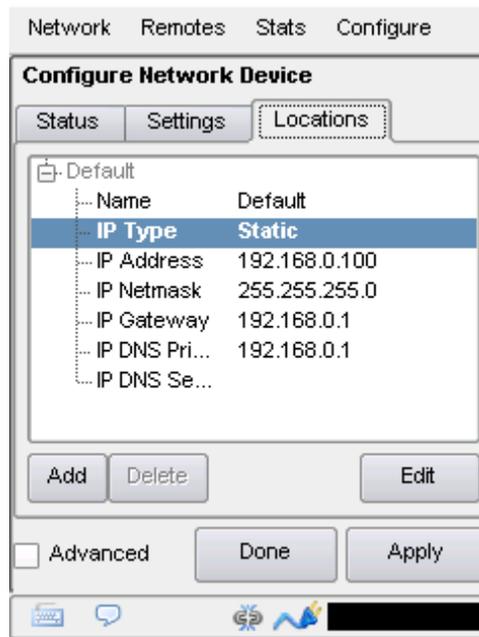
Tip: DHCP addresses change over time, so you may need to recheck the address if you are having trouble connecting.



The screenshot shows a configuration window with tabs for 'Network', 'Remotes', 'Stats', and 'Configure'. The 'Network' tab is active. Under the heading 'IP Type', there is a description: 'Type of IP addressing used by network'. Below this, it shows 'Current Value DHCP' and 'Default Value DHCP'. A dropdown menu is open, displaying three options: 'DHCP' (which is highlighted), 'Static', and 'Gateway'. At the bottom of the window are three buttons: 'Cancel', 'Default', and 'Save'.

STATIC ADDRESSING

Static IPs are IP addresses that your Internet Service Provider (ISP) or IT department provides that can be assigned to a network device. The device will always have that address when connected to the internet. When you select **Static** for your IP type, the following information fields will appear and need to be configured.



- **IP address** - The address for the 2USB your ISP provided. Make sure to check that nobody else on your LAN is using this address.
- **IP Netmask (subnet mask)** - This is a series of numbers that indicates the range of your LAN addresses. If in doubt, try 255.255.255.0.
- **IP Gateway** - The address of the Internet gateway on your account. If in doubt, try the first three numbers of your IP address with the last digit of 1 (e.g., xxx.xxx.xxx.1).
- **IP DNS Primary** - The address for the DNS (domain name system) that will be used by the 2USB to convert alphabetical names of addresses to numerical IP addresses. Provided by your ISP/IT department.
- **IP DNS Secondary** - The address of a backup DNS that will be used if the primary DNS fails.

The 2USB is perfectly capable of working over most LANs. However, if a LAN is heavily firewalled, subject to overloaded traffic conditions, or has security concerns, better performance is possible if ACCESS has its own Internet connection. Often, it's worth the trouble to install a DSL line specifically for ACCESS, especially if the cost is reasonable.

Since there may be bandwidth, firewall, and security concerns with installing ACCESS on a managed LAN, it is recommended that your IT manager be consulted in these environments.

WEB BROWSER

This option will open a graphical web browser and allow you to test your Internet connection by looking at a web page. This browser does not support Flash or other complex protocols, but is suitable for basic Internet use.

Once a network connection has been established, the browser is opened by navigating to **Network -> Web Browser**. This will open the browser into the main display window.



The browser has a factory default home page of <http://www.google.com>. However, in a public Wi-Fi environment, the home page is often rerouted to a log-in page of some sort, and this will usually be the first page to appear. The browser is intended to allow you to enter authentication information and gain access to the Internet. The browser is also helpful in scenarios where the local network requires that users log in through a web-based security page (as in many hotels). Our testing shows a high success rate in using this browser to get through these introductory pages. However, it may not be optimal for general-purpose web surfing.

It is not possible to end a browser session. This is intentional. Typically, closing the browser can end your session with a Wi-Fi provider and stop audio data flow. The browser will close when the unit is powered down.

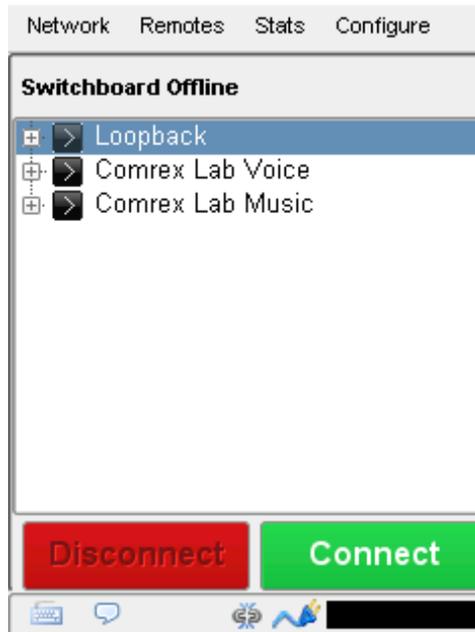
Even when the browser is open, you can navigate to other functions using the main navigation tabs.

To change the default homepage in the browser, navigate to **Configure->User Interface**. The field labeled **Web Browser Home URL** can be changed to the webpage of your choice.



VIII. REMOTES MENU

The **Remotes** menu is the first screen to appear when the system is turned on. The **Remotes** menu is like a “phonebook” for your 2USB. It allows you to define and edit your outgoing connections, and also indicates when there are incoming connections.



TEST REMOTE ENTRIES

By default, three remotes are already present on the **Remotes** menu, and can be used immediately for testing.

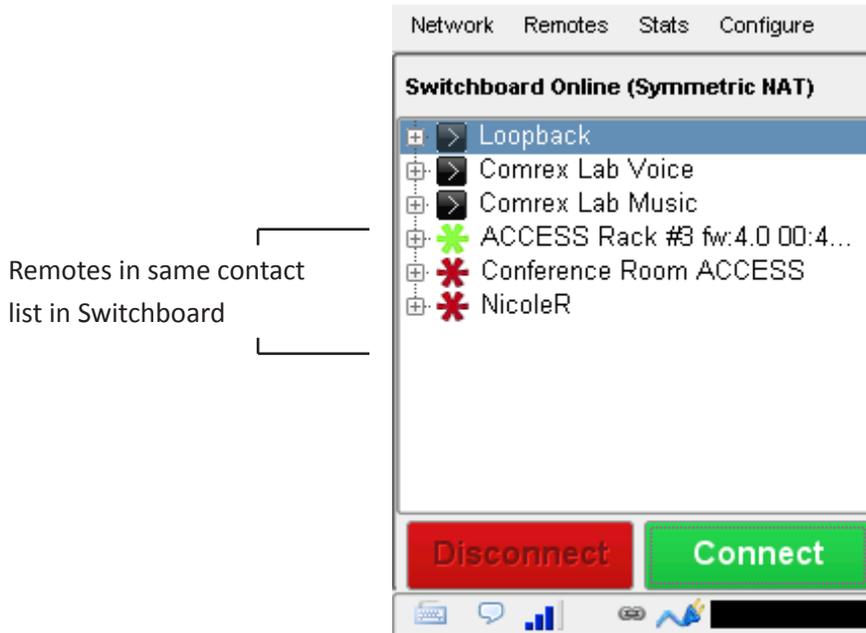
Loopback is a testing mode for estimating quality and best case delay, in which a single ACCESS encodes and decodes the same audio in a loopback configuration (the send and receive portions are connected together).

Comrex Lab Voice and **Comrex Lab Music** are codecs you can connect to for testing your unit. These test lines are located at the Comrex headquarters in Devens, Massachusetts.

REMOTES LISTED FROM SWITCHBOARD

Switchboard is a free service that Comrex provides. If you do not have an account set up with us, please contact us at techies@comrex.com or 978.764.1776 / 1.800.237.1776. To learn more about Switchboard and why you should be using it, visit the section **Switchboard Theory and Concepts on page 68**.

Comrex highly recommends that you utilize our Switchboard server in conjunction with your audio codecs. When your audio codecs have been added to your Switchboard account and placed in a contact list, those codecs will populate automatically in the device's remote list once it is powered up and registered with Switchboard. This makes connections for broadcasts quick and easy.



Units that are added from your Switchboard contact list will show up in the remotes list with different colored gear icons and a grey background. There are 3 different colors that associate with the status of that remote.

Items with a green gear are ready for connection. Yellow means busy, and red means offline.

TIP: Depending on how your network is set up, it is possible that a red gear icon will appear next to remotes that you still may be able to connect to. This “false” red gear can be generated when multiple NATs are within your network chain that may individually hinder the ability to reach Switchboard, but are able to connect when routed through the entire network chain.

CONNECTING AND DISCONNECTING TO REMOTES

To connect and disconnect remotes, select the device in the remotes list and select the **Connect** button to establish a connection or the **Disconnect** button to disconnect the connection.

Incoming connections are displayed by their IP address, or, if also configured as outgoing connections, by their names. Incoming POTS connections are displayed as “incoming”.

ADD NEW REMOTE

Although using Switchboard to generate your remotes is the preferred method, you can also add remotes manually and input the information needed to make a connection.

To add a new remote, navigate to **Remotes->Add New Remote**.

The following menu appears.



The screenshot shows a software window titled "Add New Remote" with a menu bar containing "Network", "Remotes", "Stats", and "Configure". The dialog box contains the following fields and options:

- Name:** A text input field.
- IP / Phone #:** A text input field.
- Switchboard ID:** A text input field.
- Password:** A text input field.
- Profile:** A dropdown menu with "(Default Profile)" selected.
- Backup:** A dropdown menu with "(No backup)" selected.
- Use Crosslock to Connect:** An unchecked checkbox.
- Auto fall-forward:** An unchecked checkbox.

At the bottom of the dialog are "Cancel" and "OK" buttons. The window's taskbar at the bottom shows several icons, including a keyboard icon in the bottom left corner.

To edit the entries, select the keyboard icon in the bottom left of the screen.

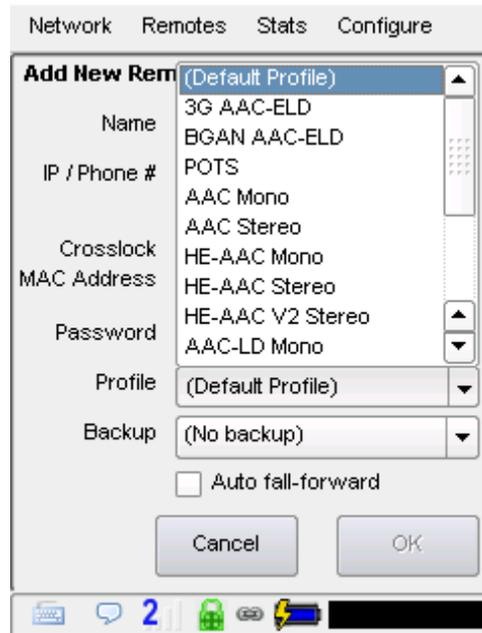
You will need to input a name for this remote (which can be anything), as well as the destination IP address (or dial-up phone number for a POTS call).

Next, you must decide if you intend to use CrossLock for the connection. Comrex recommends the use of CrossLock for most connections, because the VPN (Virtual Private Network) created by CrossLock increases connection reliability in most circumstances. Unless you know of a specific reason that your setup might not support CrossLock, we suggest enabling it. To learn about more about CrossLock, see the section **CrossLock Details on page 73**.

CrossLock connections that don't use Switchboard can be complex to set up. This is because the hardware on each end must know the Switchboard ID of the other for security purposes. This is the MAC address of the codec hardware. If you want to use CrossLock, check the **Use CrossLock to Connect** box and put the Switchboard ID (MAC address) of the unit you are going to connect to. Note that the codec being connected to must have a corresponding entry with this unit's Switchboard ID (MAC address).

If you do not want to use CrossLock, you can leave the box unchecked and the Switchboard ID (**MAC address**) entry blank.

Next, you need to choose a profile to use when making these connections. ACCESS includes several default profiles to choose from, each of which enable a simple full-duplex link using one of the available algorithms.



If you wish for a more complex feature set when making this connection, you will need to navigate to the top menu **Configure->Manage Profiles** and set up a specific profile using your custom parameters. To learn about creating Profiles, visit the section **Profiles Menu on page 44**.

Once defined on the **Manage Profiles** section, the new profile will be available in the **Profile Select** window and can be assigned to a remote connection.

Optionally, you may add a password to this outgoing remote for connection authentication. In this case, the incoming ACCESS must also be programmed with the matching incoming password, which is assignable under **Configure->System Settings->Connections->Incoming Connection Password**.

Finally, you may specify how the unit is to behave when connection is lost to this remote. To learn more about setting backups, visit the section **Backing Up A Connection on page 131**.

EDIT REMOTES

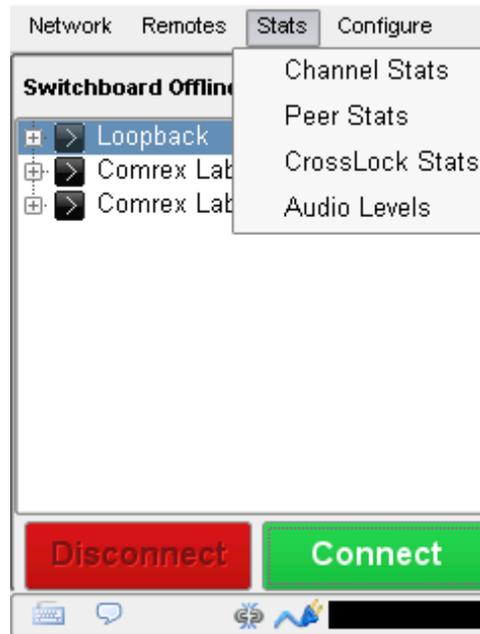
Existing remotes may be edited by highlighting a remote from the list and selecting **Remotes->Change Remote Settings**. **Tip: CrossLock Unit IDs (MAC Addresses) can not be edited - the remote entry must be deleted and recreated to edit outgoing CrossLock info.**

DELETE REMOTES

Remotes can be deleted by highlighting a remote from the list and selecting **Remotes->Delete Remote**.

IX. STATS MENU

The menu items under **Stats** show graphical and/or numerical representations of the network performance, utilization, and audio levels for both the local and remote codecs.



Channel Stats provide real-time graphs of outgoing and incoming data. **Channel Stats** are considered a legacy resource to view network performance. **CrossLock Stats** are recommended to be your source for this data.

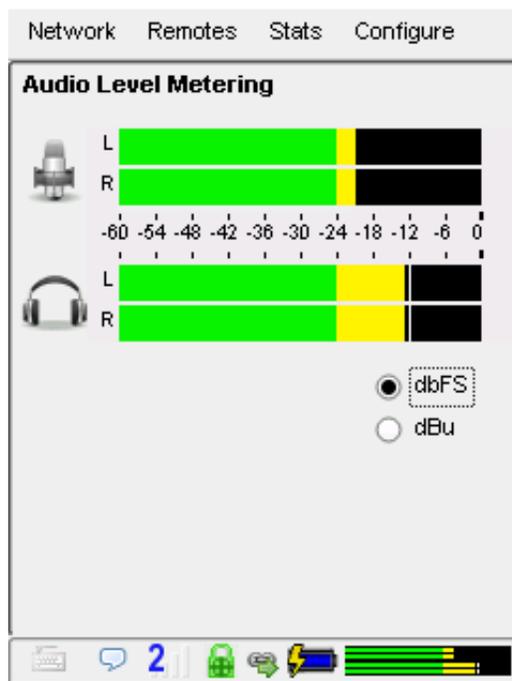
Peer Stats give detailed information regarding the decoder buffer manager's functions, such as call duration, transmit and receive delays, frame loss rates, overhead, and more.

For more information on **Channel Stats** and **Peer Stats**, go to the **Legacy Stats on page 102**.

CrossLock Stats allows you to see CrossLock in action. You can determine how many networks are being utilized, the delay associated with both ends of the connection, loss and recovery of packets, and more.

These stats are considered superior to the **Channel Stats**, and should be used when monitoring network performance. For details on CrossLock and the **CrossLock Stats**, visit the **CrossLock Details on page 73**.

Audio Levels allow you to monitor levels of both the local and remote audio during an active connection. Levels are available in dBu and dBfs **scales**.



x. CONFIGURE MENU

The **Configure** menu contains the following:

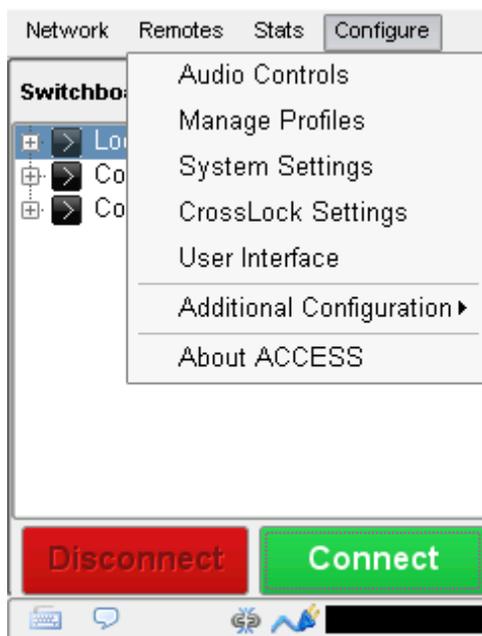
Audio Controls - Adjust audio routing and apply phantom power to the Mic Input.

Manage Profiles - Allows you to view, create, and edit profiles. See the section **Profiles Menu on page 44**.

System Settings - Adjust global settings including connection behavior, security parameters, contact closures, and Switchboard settings. See the section **System Settings menu on page 46** to learn more.

CrossLock Settings - Adjusts CrossLock parameters. See the section **CrossLock Details on page 73** to learn more.

User Interface - Adjusts F2 key behavior, changes web browser home URL, and enables restricted user mode.

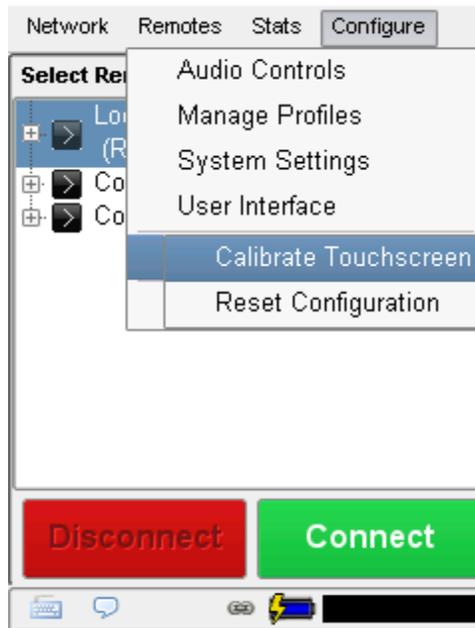


Additional Configuration - Two options appear under here: **Calibrate Touchscreen**; and **Reset Configuration**.

Calibrate Touchscreen - Calibrates the touchscreen through on-screen prompts.

Reset Configuration - This option will restore your ACCESS software to factory default settings.

WARNING: All settings, profiles, and remotes will be lost in this procedure. This function is not reversible.

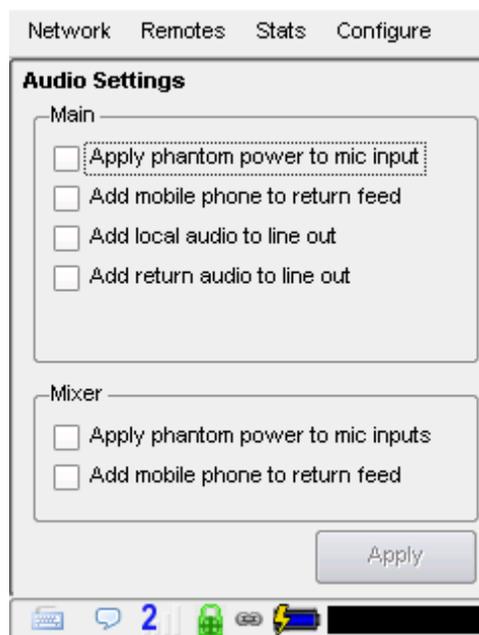


About ACCESS - This will provide the firmware version, licensed features on the device, and the software license disclosure.

To view more information on **Manage Profiles**, **System Settings**, or **CrossLock Settings**, go to the corresponding sections listed on the previous page.

AUDIO CONTROLS

This section allows you to determine how audio is routed through the system. Some of these settings affect the operation of the main ACCESS 2USB, while others affect the operation of the optional clip-on mixer.



Apply phantom power to Mic input - When selected, this function applies a 12 V phantom power signal to the **Mono In** connector when the **Mic/Line** switch is in the **Mic** position. This is for use with electret or condenser microphones. This setting should be in the off position for use with normal dynamic microphones.

Add mobile phone to return feed - If this option is selected, the **Mobile In/Out** connector input becomes active. It allows attachment of a mobile phone's hands-free port to the unit. The function of this input is to allow remote audio (sourced from the output of a mobile phone) to be added to the headphone output of the ACCESS. This audio is not applied to the **Line Out** signal.

Add local audio to line out/Add return audio to line out - Here you can select which audio feeds are being sent to the fixed-level **Line Out** jack: Audio being generated locally (**Local**); Audio being sent from the far-end connection (**Return**); or a mixture of both.

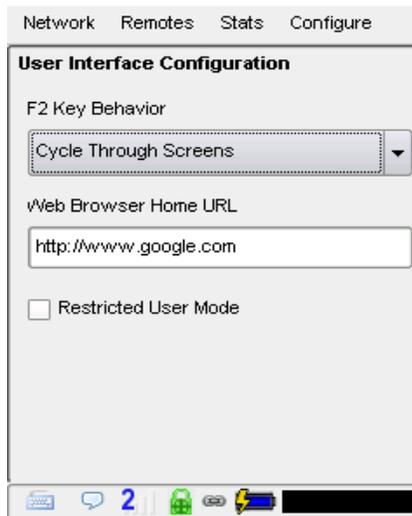
MIXER AUDIO

The following settings apply to the optional ACCESS clip-on mixer:

Apply phantom power to mic inputs - When selected, this function applies a 12 V phantom power signal to the mixer Input XLRs when **Mic/Line** switch is in the **Mic** position. This is for use with electret or condenser microphones. This setting should be in the off position for use with normal dynamic microphones. Phantom power cannot be individually selected to each mixer input; it must be on or off for all channels.

Add mobile phone to return feed - If this option is selected, the **Mobile In/Out** connector input becomes active. It allows attachment of a mobile phone's hands-free port to the unit. The function of this input is to allow remote audio (sourced from the output of a mobile phone) to be added to the headphone output of the ACCESS.

USER INTERFACE CONFIGURATION MENU



If you find you commonly use one particular function, and are often scrolling through multiple menus to get there, simply use the **F2 Key Behavior** drop-down to choose a shortcut to that function.

The **Web Browser Home URL** setting allows you to change the default homepage for the web browser.

ACCESS has many administrative features that are often unnecessary for the casual user. Checking the **Restricted User Mode** allows you to hide options that would confuse non-technical users. When this mode is enabled, users can only connect and disconnect calls, enable and disable available networks, and change the audio settings.

xi. PROFILES MENU

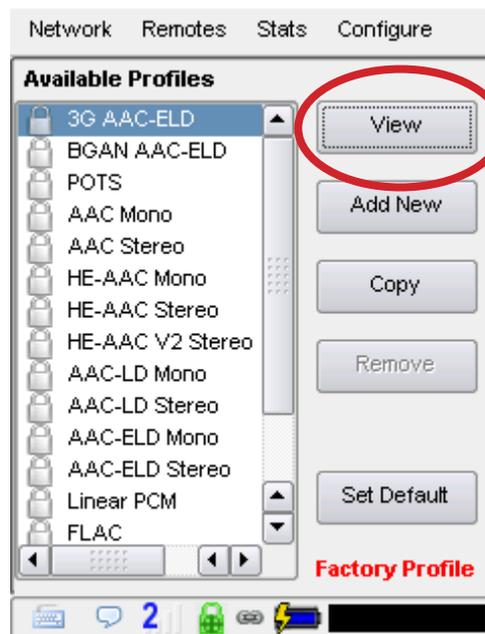
Profiles are what define the behavior and type of connection for your codecs in both directions. Profiles are separate from remotes, which define the address to connect with.

ACCESS has many options to optimize connections based on your broadcasting needs (the number of locations you broadcast to, the diversity of connections you use, network availability, etc.). Your specific needs will dictate how simple or intricate your profile and remote settings will be. ACCESS comes with a series of profiles that are optimized for the majority of IP and POTS connections. Many users may never need to define their own profiles.

When using ACCESS, the point where the connection originates controls all available connection parameters in both directions. Keep in mind that these profiles are useful only for connections initiated from the local ACCESS. Incoming connections are defined by the ACCESS at the other end.

VIEWING PROFILE DETAILS

To view the parameters set for a profile, navigate to **Configure->Manage Profiles**. Select the profile in the list you want to view and select the **View** button on the right hand side. From here, you can also edit parameters of the profile.



EDITING AND ADDING PROFILES

Custom profiles are easy to create on ACCESS. You can create one from scratch by selecting **Add New** on the **Manage Profiles** menu, or copy an existing profile using the **Copy** button.

TIP: You cannot edit factory profiles. Comrex recommends that, when creating a new profile, you copy a factory profile that is close to what you would like the settings to be, and edit that copied profile.

Profile creation is segmented into commonly used and advanced options. In order to simplify the interface, **Advanced Options** are normally hidden from the user. Once a profile is defined, it will be available from the **Profile** drop-down menu.

To build a new profile, select **Add New** and a new profile appears on the list labelled **New Profile**.

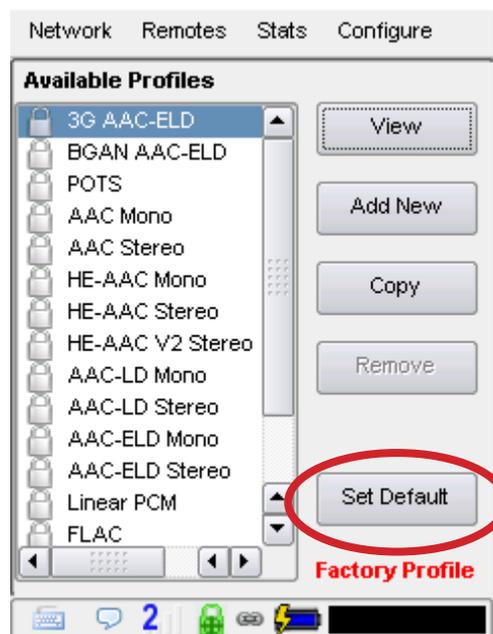
Select it and press **Edit**, and you'll see a list of options.

IMPORTANT: Building a profile doesn't change how any remotes connect until that profile is assigned to a remote.

DEFAULT PROFILE

When a new remote is created, a default profile is assigned unless a different profile is selected from the drop-down menu under **Profile**. The default profile, when shipped from the factory, uses an OPUS algorithm.

TIP: You can change the default profile by Navigating to **Configure->Manage Profiles**, highlighting the desired profile and pressing the **Set Default** button. This profile will be used on all new remotes unless a different one is selected in the **Create New Remote** screen. The default profile shows an asterisk (*) next to it in the Profiles list.



xii. SYSTEM SETTINGS MENU

System Settings define parameters that are not specific to a particular remote connection. Examples are how incoming (POTS and IP) calls are handled, global modem settings, and how the contact closures are assigned. Basic options are shown by default. Less used options are hidden until the **Advanced** box is checked. To learn more about Advanced settings, visit the section **Advanced Settings on page 130**.

CONNECTION SETTINGS

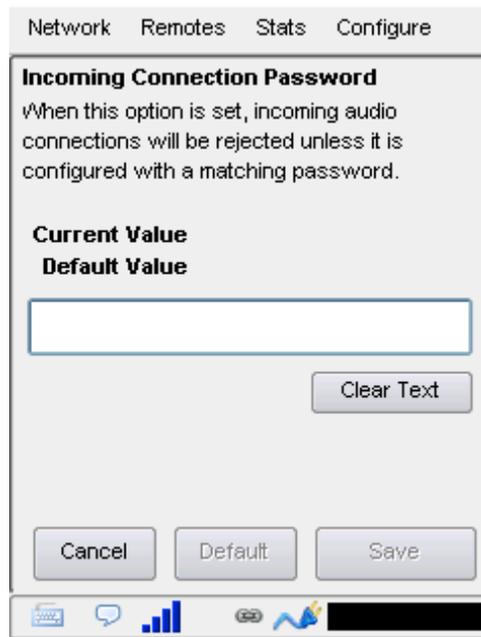


Unit Name - Users are encouraged to name their codecs here. The default name of a codec is the unique MAC address (Switchboard ID) of the Ethernet port. When this is changed to something familiar and unique (such as "Roving reporter", "Weather guy", etc.), the new name is reflected in several places:

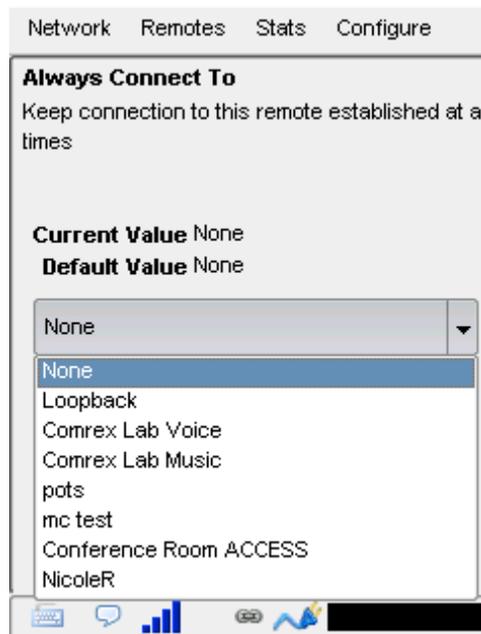
- In the Web-based Interface;
- In Comrex-provided utility software such as **Device Manager**;
- In Switchboard Contact Lists.

Note: This can be reset at any time to the unit's MAC address (Switchboard ID) by selecting the Default button.

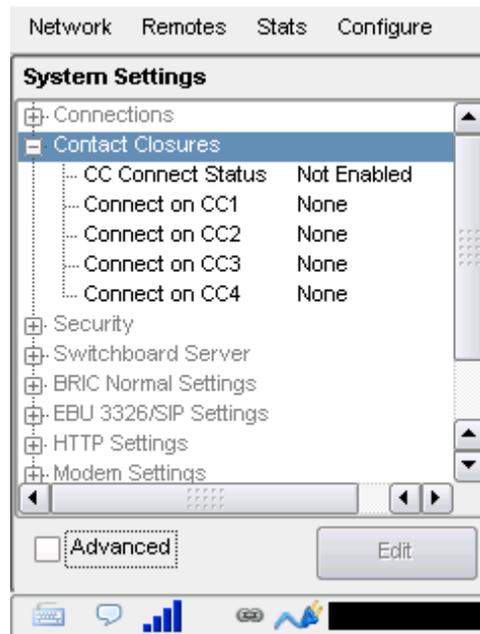
Incoming Connection Password - Allows you to define a password that must be attached to all incoming connections before they are accepted. Units contacting you must know this password and apply it to their outgoing stream, or the connection will not be completed. Leaving the field blank will disable this function.



Always Connect To - This setting is available to designate a remote for “always-on” operation. This is useful in environments where a signal is required to be on 24 hours a day. To assign an “always-on” remote, pull down the menu and select which remote to designate as “always-on”. A connection will be made and sustained to the chosen remote.



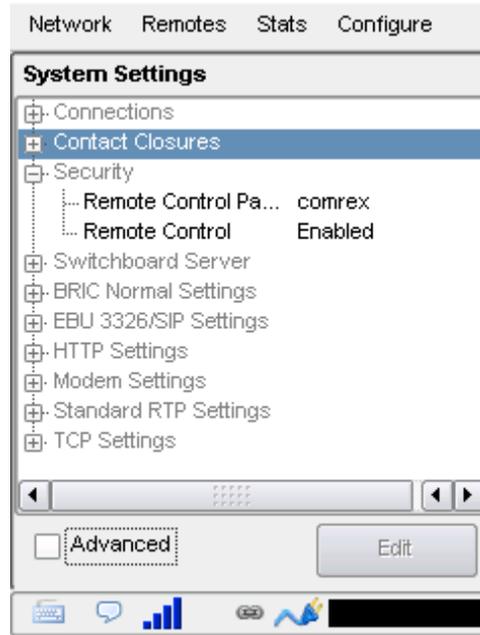
CONTACT CLOSURES SETTINGS



CC Connect Status - Alters the performance of output contact closure #4. Under normal circumstances, the contact will close when commanded by the other end of the connection. If this option is enabled, that function is no longer available. This contact will be closed when a valid connection is present, and open when no connection is present.

Connect on CC (1,2,3,4) - These choices define auto-connect rules for remotes to be triggered by the four external input triggers available. NOTE: These inputs are shared with the end-to-end contact closure signals, so if a remote is designated as **Auto Connect** on a closure, that closure signal is not available for use in the direction from this ACCESS. To assign a remote connection to a contact closure, pull down the menu box next to the desired closure and select the proper remote. A connection attempt will be made whenever the contact is triggered, and will disconnect whenever the contact is released. (You can also assign the **F2** key to trigger **Contact Closure #1** at the remote codec.)

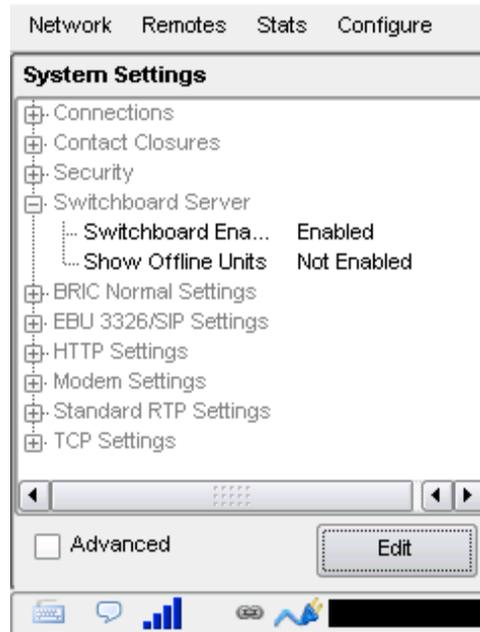
SECURITY SETTINGS



Remote Control Password - Allows you to define a password for the webpage login screen and firmware updater. The default password is **comrex** (lowercase). You can disable the remote control and firmware updating functionality completely by disabling the **Remote Control** option.

Remote Control - If this function is disabled, the unit will not serve any webpage from its IP address, and the firmware updater will not function. If this option is enabled, you should define a password that will be used to enable both functions.

SWITCHBOARD SERVER

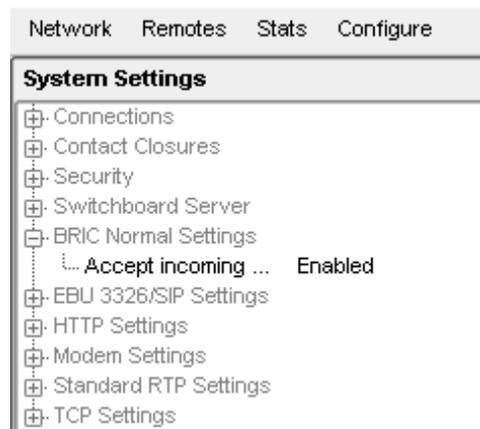


Switchboard Enabled - Allows the use of the Switchboard Server to connect to remotes.

Show Offline Units - When enabled, offline remotes will be shown in the **Remotes** list.

BRIC NORMAL SETTINGS

The default way ACCESS codecs connect between each other is called BRIC normal. The options in this section define if and how these connections are completed.

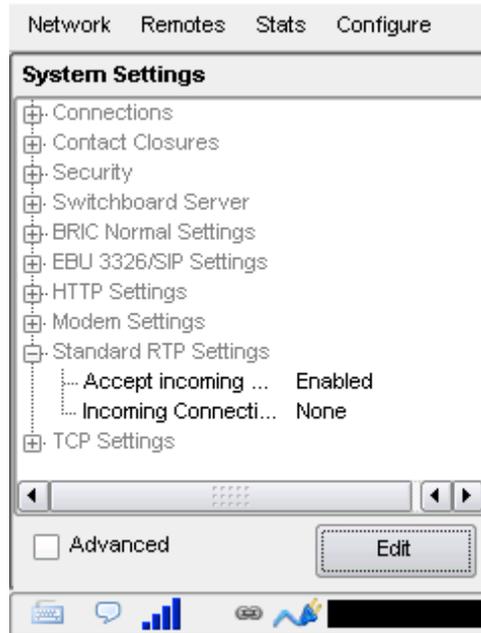


Accept Incoming Connections - This determines if this ACCESS is to be used for incoming normal IP connections. If this function is not enabled, ACCESS will only support outgoing calls using BRIC Normal Mode.

STANDARD RTP SETTINGS

Standard RTP is a protocol ACCESS uses to connect to some non-Comrex devices. It's not commonly used. It's one of the possible connection modes of Luci Live™ and Telos Zephyr XStream™. Standard RTP is not a complex protocol, so you must manually apply settings for both outgoing and incoming profiles.

For complete details, please review **Appendix A - IP Compatibility on page 157**.



Accept Incoming Connections - Allows the unit to automatically answer incoming calls.

Incoming Connection Profile - Shows which profile has been selected for incoming connections.

TCP SETTINGS

ACCESS performs best when using UDP for connections, but there are some rare circumstances when the system may need to be switched over to TCP operation. This advanced option defines how incoming TCP calls are handled.

Outgoing calls are defined as TCP in profile configuration. ACCESS normally listens for incoming calls on both TCP and UDP ports, and chooses the first to arrive. If a TCP call is detected, ACCESS will attempt to use the same TCP link to transmit in the reverse direction.



Accept Incoming Connections - Allows you to turn **TCP Auto Answer** on and off. Disabling this function means only outgoing TCP calls can be established.

XIII. PINOUTS

PINOUTS - AUDIO

XLR Pinout

Pin 1	Ground
Pin 2	Audio +
Pin 3	Audio –

1/8" Jack In/Out Pinout (excluding Mobile In/Out)

Tip	Left Channel In/Out
Ring	Right Channel In/Out
Sleeve	Ground

Mobile In/Out

Tip	Send Audio To Phone
Ring	Receive Audio From Phone
Sleeve	Ground

PINOUTS - SERIAL PORT

The serial port is pinned to match serial connections on older Macintosh computers, so commercially available adapter cables should have the proper pinning.

Serial Port Pinout

Pin #	Function	Direction
1	CTS	To ACCESS
2	RTS	From ACCESS
3	RX Data	To ACCESS
4	Ground	
5	TX Data	From ACCESS
6		
7		
8	Ground	

PINOUTS - CONTACT CLOSURES

Contact closures are available via the 9-pin mini-DIN connector on the side panel of the ACCESS 2USB. Inputs are triggered by shorting the respective input to **Pin 9**. Outputs consist of an open collector circuit which, when inactive, will offer a high-impedance path to **Pin 9** and, when active, will offer a low impedance path to **Pin 9**. These outputs are capable of sinking up to 200 mA at a voltage up to 12 V. Do not switch AC mains power using these contacts.

Contact Closure Pinout

Pin 1	Output #1
Pin 2	Output #2
Pin 3	Output #3
Pin 4	Output #4
Pin 5	Input #1
Pin 6	Input #2
Pin 7	Input #3
Pin 8	Input #4
Pin 9	Ground

Note: Adapter cables for the serial and contact closure ports are available for purchase from Comrex—contact us for more information.

xiv. ABOUT THE ALGORITHMS

ACCESS offers a very wide range of encoding algorithms. To some this may seem daunting. Here's a short guide on how to choose what's best for your application:

- 1 Do I have lots and lots of bandwidth? If you're running on an entirely unconstrained network like a campus LAN or local Wi-Fi, Mono or Stereo Linear PCM Mode will offer the highest audio quality with lowest delay. If you're hitting the public Internet at any point in the link, however, avoid Linear PCM Mode.
- 2 Do I require interactivity? If you need to chat back and forth across the link, choose one of our low delay algorithms like AAC-ELD or Opus. The deciding factor between these algorithms is digital bandwidth.
- 3 Is audio quality the paramount concern? AAC or HE-AAC are the best choices for applications that need excellent audio quality. If delay is also a concern, consider AAC-ELD, which along with Opus, should be the default choice for radio remote broadcasts. If you are running on an unconstrained network, Linear PCM or FLAC would be a good choice.
- 4 Do I need to deliver two unrelated audio signals to the same location? AAC, HE-AAC, and AAC-LD offer Dual Mono options that allow uncorrelated signals (such as dual language broadcasts) to be combined to a single outgoing stream. Note: It isn't possible to send one stream to location A and one to location B. However, it is possible to send the combined stream to locations A and B and have them tap only their respective channels (although this can be a confusing solution that is subject to operator error).

OPUS

Opus is an audio coding format that is gaining in popularity on the web. It has a good balance between audio quality and delay over a range of bitrates. It allows interoperation with web services like WebRTC and apps like Liphone. It's a good choice for remote broadcasts for most users.

LINEAR PCM

This encoder does not compress audio at all. It uses a 48 kHz sampling rate and simply applies small frames of linear audio to IP packets. This mode is only useful on high bandwidth LAN or managed WAN environments. Mono Mode requires a network capacity of 768 kbps while Stereo Mode requires a network bandwidth over 1.5 Mb/s.

FLAC

This encoder compresses the audio data using a lossless algorithm. This means that the audio extracted from the decoder is identical to the audio input to the encoder, with no coding artifacts. FLAC typically removes 30-40% of the network data compared to Linear PCM, but the actual data rate is variable and is based on the complexity of the coded audio. Using FLAC over Linear PCM typically results in a slightly higher (5 ms) overall delay.

G.711 (μ -law and a-law)

These are the coding algorithms used by standard digital POTS calls, and provide about 3 kHz (telephone quality) audio. μ -law is utilized in North America, while a-law is prevalent in Europe. These algorithms are provided for compatibility with SIP-style VOIP phones, but don't provide much benefit over standard telephony in audio terms.

NOTE: If you are running on firmware 4.0 or higher, this algorithm is no longer available.

G.722

This is a well known 7 kHz (medium fidelity) algorithm used in some VOIP telephones and codecs. It is provided for compatibility purposes, but is not considered a superior algorithm for audio codecs.

AAC

This algorithm is a highly regarded standard for compressing audio to critical listening standards. It has been judged to produce "near transparent" audio at a coding rate of 128 kbps stereo. The standard is a collaborative of several audio companies' best efforts, and has become popular as the default audio codec of the Apple™ iTunes™ program. AAC should be considered the highest quality codec in ACCESS; enhancements like HE-AAC and AAC-ELD attempt to maintain a similar quality and reduced bandwidth and delay.

HE-AAC

This is a newer version of AAC defined for increased efficiency. The goal of the algorithm is to produce AAC-comparable quality at a lower bit rate. It does this by encoding lower frequencies to AAC, and higher frequencies using Spectral Band Replication (SBR), a technique that partially synthesizes these high frequencies. HE-AAC is trademarked by other companies as AACPlus™. HE-AAC (and close derivatives) are often used as the main audio codec for digital radio and satellite networks.

HE-AACV2

This algorithm further increases the efficiency of HE-AAC by adding intensity stereo coding. This results in a lower bit rate for stereo signals. We also cluster a very reduced-rate HE-AAC mono into this category, although technically it does not contain v2 coding.

AAC-LD

This algorithm is an extension of AAC developed by the Fraunhofer IIS, who are the contributors to AAC and primary inventors of the MP3 algorithm. Its quality is superior to MP3 at similar bitrates (64-128 kbps) but it exhibits very low delay (100 ms). This choice is best when reasonable network throughput is assured, near-transparent audio is required, and interactivity is needed.

AAC-ELD

This latest algorithm is a combination of the LD and HE-AAC variants. It provides the network-conserving benefits of SBR along with the dramatically reduced delay time of LD. For low delay applications, it's usually the best choice.

Algorithm Comparison Chart for ACCESS Codecs

Required Bitrate	Coding Delay	Audio Bandwidth	
			AAC: Provides near transparent audio at relatively high data rates. Best used on non-constrained data networks - for situation where latency is not important.
64 kb/s	69 ms	20 kHz	D1 Mono
96 kb/s	69 ms	20 kHz	D2 Stereo
128 kb/s	69 ms	20 kHz	D3 Dual Mono allows independent programming to be sent on both L&R channels
128 kb/s	69 ms	20 kHz	D4 Stereo 128Kb
256 kb/s	69 ms	20 kHz	D5 Dual Mono 256Kb allows independent programming to be sent on both L&R channels
56 kb/s	69 ms	20 kHz	D6 Mono 56Kb
96 kb/s	69 ms	20 kHz	D7 Mono 96Kb
160 kb/s	69 ms	20 kHz	D8 Stereo 160Kb
			HE-AAC: Provides near transparent audio at low data rates - for situations where latency is not important.
48 kb/s	146 ms	20 kHz	E1 Mono
64 kb/s	146 ms	20 kHz	E2 Stereo
96 kb/s	146 ms	20 kHz	E3 Dual Mono allows independent programming to be sent on both L&R channels
			Linear PCM: Delivers transparent audio with no compression and very low delay - for use on high throughput networks.
768 kb/s	19 ms	20 kHz	F1 Mono
1536 kb/s	19 ms	20 kHz	F2 Dual Mono
512 kb/s	19 ms	15 kHz	F3 Mono
1024 kb/s	19 ms	15 kHz	F4 Dual Mono
			HE-AAC V2: Provides medium quality HE-AAC implementation using Spectral Band Replication.
18 kb/s	212 ms	12 kHz	G1 Mono 18Kb
24 kb/s	269 ms	12 kHz	G2 Stereo 24Kb adds Parametric Stereo to SBR for higher quality audio at low data rate
32 kb/s	184 ms	20 kHz	G4 Stereo 32Kb adds Parametric Stereo to SBR for higher quality audio at low data rate
48 kb/s	184 ms	20 kHz	G3 Stereo 48Kb adds Parametric Stereo to SBR for higher quality audio at low data rate
56 kb/s	184 ms	20 kHz	G5 Stereo 56Kb adds Parametric Stereo to SBR for higher quality audio at low data rate
			AAC-LD: Requires higher data rates but provides near transparent voice or music with low delay.
96 kb/s	30 ms	20 kHz	I1 Mono
128 kb/s	30 ms	20 kHz	I2 Stereo
192 kb/s	30 ms	20 kHz	I3 Dual Mono allows independent programming to be sent on both L&R channels
256 kb/s	30 ms	20 kHz	I4 Stereo 256Kb
128 kb/s	30 ms	20 kHz	I6 Mono 128Kb
64 kb/s	30 ms	20 kHz	I7 Mono 64Kb
			AAC-ELD: combines the aspects of HE-AAC and AAC-LD to provide low delay, good audio quality and low bitrate. The best choice for low delay applications on the Internet.
48 kb/s	47 ms	20 kHz	J1 Mono
64 kb/s	46 ms	20 kHz	J2 Stereo
96 kb/s	47 ms	20 kHz	J3 Dual Mono allows independent programming to be sent on both L&R channels
24 kb/s	47 ms	20 kHz	J4 Mono 24Kb
			FLAC: Free Lossless Audio Compression provides transparent audio while conserving bandwidth. FLAC bitrate is variable and based on audio input.
~537 kb/s	26 ms	20 kHz	K1 Mono
~1075 kb/s	26 ms	20 kHz	K2 Dual Mono
~358 kb/s	26 ms	15 kHz	K3 Mono
~717 kb/s	26 ms	15 kHz	K4 Dual Mono

			Opus: A newer offering that combines low delay and low network utilization. Opus is included primarily for compatibility with softphone apps and Internet connections using WebRTC. (Special CBR modes are offered for compatibility with Tieline products - avoid these in other applications).
48Kb/s	41 ms	20 kHz	N4.1 Mono 48kbps
56Kb/s	41 ms	20 kHz	N4.2 Mono 56kbps
64Kb/s	41 ms	20 kHz	N4.3 Mono 64kbps
64Kb/s	41 ms	20 kHz	N5.1 Stereo 64kbps
96Kb/s	41 ms	20 kHz	N5.2 Stereo 96kbps
128Kb/s	41 ms	20 kHz	N5.3 Stereo 128kbps
48Kb/s	41 ms	20 kHz	N6.1 CBR Mono 48kbps
64Kb/s	41 ms	20 kHz	N6.3 CBR Mono 64kbps
64Kb/s	41 ms	20 kHz	N7.1 CBR Stereo 64kbps
96Kb/s	41 ms	20 kHz	N7.2 CBR Stereo 96kbps
128Kb/s	41 ms	20 kHz	N7.3 CBR Stereo 128kbps
			VoIP: G.711 and G.722 coding algorithms for compatibility with SIP-style VoIP phones.
64 kb/s	35 ms	3 kHz	X1 G.711 a-law
64 kb/s	35 ms	3 kHz	X2 G.711 μ-law
64 kb/s	35 ms	7 kHz	X3 G.722

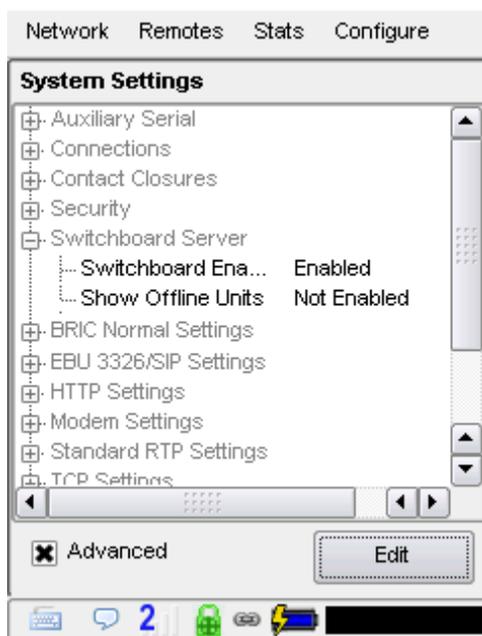
xv. SWITCHBOARD TRAVERSAL SERVER (TS)

The Switchboard Traversal Server is a service built and maintained by Comrex on the public Internet that provides users a directory of other users, facilitating connections to devices that would normally have trouble accepting incoming IP connections. Use of Switchboard is free and comes activated from the factory.

The next section describes how to set up and configure Switchboard.

CONFIGURING SWITCHBOARD

Navigate to **Configure->System Settings->Switchboard Server**.



The two choices under the Switchboard Server are **Switchboard Enabled** and **Show Offline Units**. To use Switchboard, the **Switchboard Enabled** setting must be enabled. Setting the **Show Offline Units** to "Enable" will allow you to see the other units on the account, even if they are not currently online.

LOGGING IN AND SETTING UP SWITCHBOARD

In order to use Switchboard, you must first have an account with the server. You can obtain an account by contacting Comrex at 978-784-1776 / 800-237-1776, or by emailing techies@comrex.com / info@comrex.com. Only one account is required for each group of codecs.

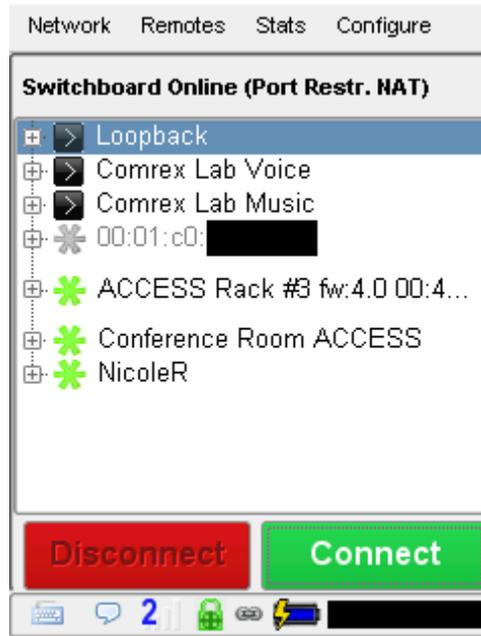
Once a username and password is provided, navigate to switchboard.comrex.com in a browser.

The first time you log in to Switchboard, you will see a notice stating that no units have been added to the account. By clicking on **Add New Unit**, you will be prompted to input the MAC address (Switchboard ID) of the ACCESS you wish to add. The MAC address (Switchboard ID) is available via the touchscreen under **Configure->About** or **Configure->System Settings->Connections->Unit Name**. You can also find it by scanning for the unit via **Device Manager**. The MAC address of the ACCESS must be input in a format with colons between each pair of characters.

Once the unit’s MAC address (Switchboard ID) is input correctly, you will see it appear in the unit list. Once a codec is added, you should break the network connection to the codec unit in order for the device to properly sync with Switchboard. The next time the properly configured codec goes online, it will sync with the server. The codec name and other information will be updated.

	Unit Name MAC	Connection Status	Firmware	
 ACCESS Rack Audio Codec	City Hall 00:40: [REDACTED]	Offline Last seen 2012-06-13 14:28:44	2.8-p11-test1	Details
 ACCESS Rack Audio Codec	Master Control 00:40: [REDACTED]	Offline Last seen 2013-11-06 23:00:14	devel	Details
 ACCESS Portable Audio Codec	00:01: [REDACTED]	Offline Last seen 2013-10-31 13:45:17	2.8-p23	Details
 ACCESS Portable Audio Codec	Weather C 00:01: [REDACTED]	Offline Last seen 2013-05-16 04:08:56	2.8-p10	Details
 ACCESS Portable	Kabul office	Offline	2.7.1-p3	Details

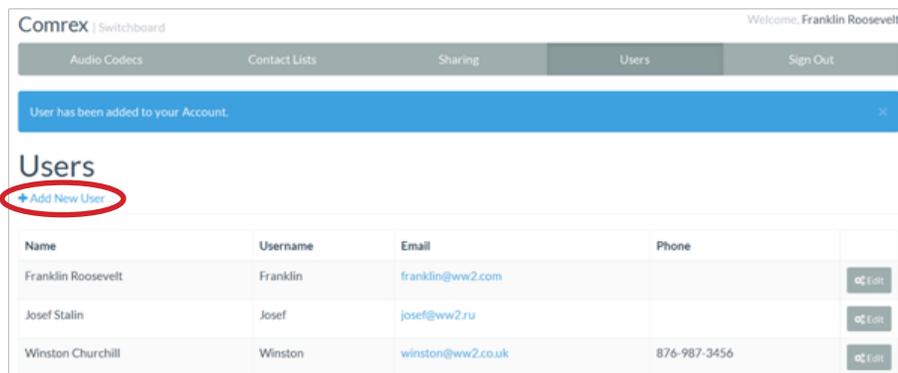
Once Switchboard is enabled and you have correctly created your group on the server, a list of all other codecs in your contact list will populate automatically in the Remote List on the codec user interface.



To make calls with the help of Switchboard, simply click one of the entries with the green gear icon and click **Connect**. Switchboard will handshake with the remote unit and make the connection automatically.

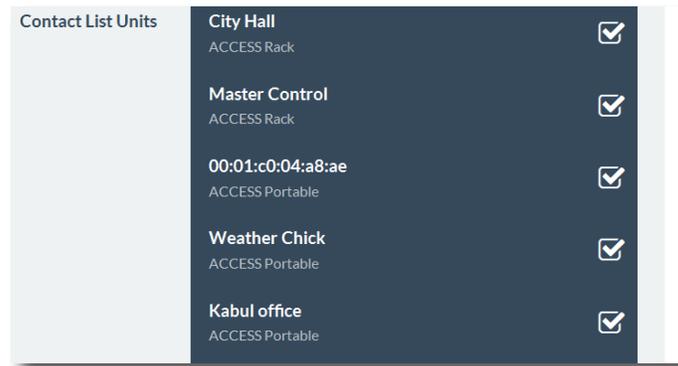
CREATING USERS

You may wish to add additional Switchboard users who can access the Switchboard interface. You can do this via the **Users** tab at the top of the main codec list. This allows you to create accounts for users that can later be deleted. Several user accounts can be created with unique passwords.



CONTACT LISTS

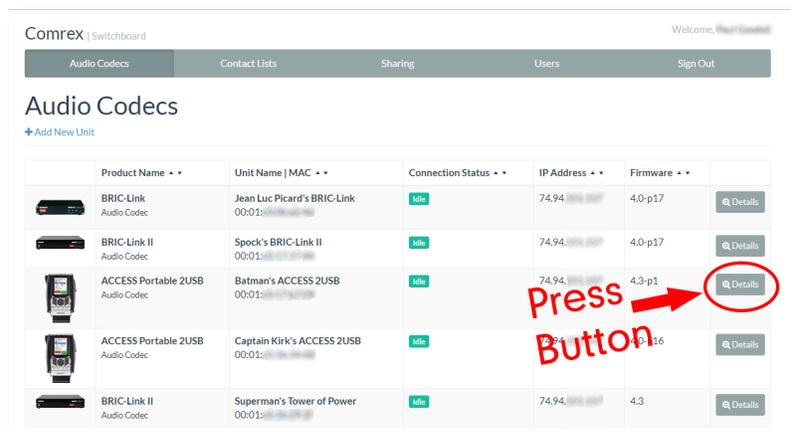
In some situations, it might not be desirable for each codec in your fleet to be able to see the Switchboard status of every other codec. To help filter what's displayed on a codec's interface, Switchboard has implemented **Contact Lists**, which can each contain a subset of your codec fleet on your account. You can create multiple Contact Lists that consist of different subsets. With the exception of Shares (discussed below), only units within your Switchboard account may be assigned to Contact Lists.



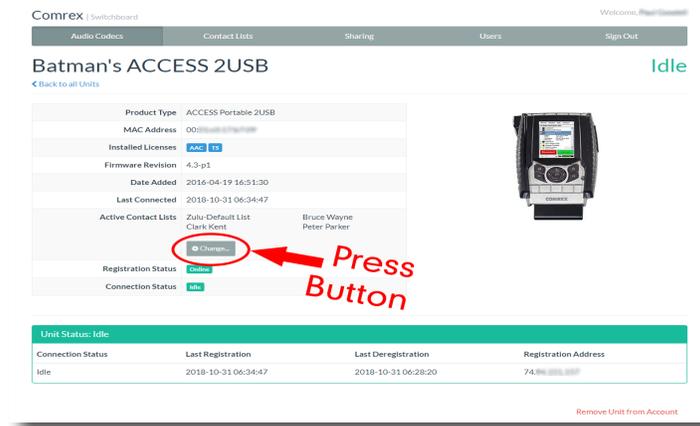
By default, Switchboard creates a master Contact List that contains all of the codecs in your account and which every codec in your fleet uses. If you're not interested in segregating codecs on your account any further, this default Contact List should be sufficient.

Each unit also has the ability to **Follow** a Contact List. This is a view-only function that allows a codec to see the status and presence of units in a Contact List. All units are set to Follow the master Contact List by default.

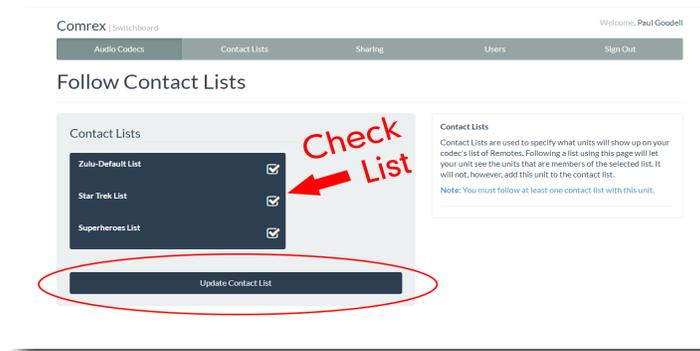
To Follow a Contact List on a codec, first click on the "Details" button for that codec on the main screen in Switchboard (as shown below).



Next, press the “Change” button near the middle of the following screen.



On the next screen, check the Contact List(s) that you want this codec to Follow and press “Update Contact List”.

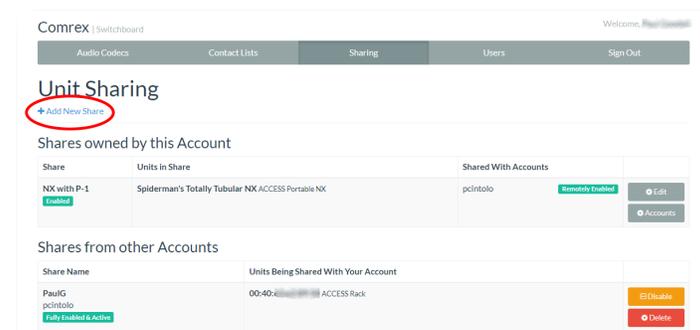


One important point to remember: Following a Contact List on a codec only determines which units get displayed on that codec's own list. It has no impact on how that codec itself is displayed on other devices.

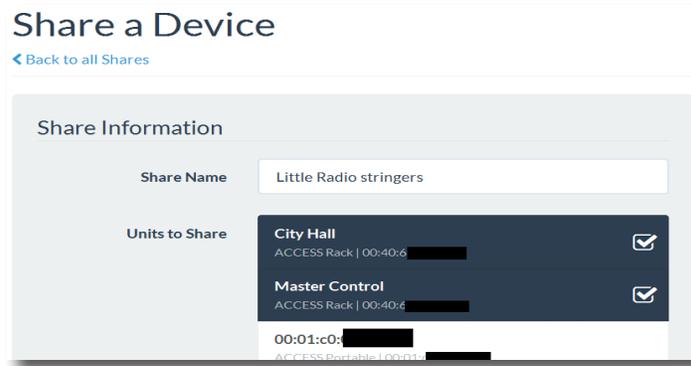
SHARES

If you want to allow users outside of your account to see the status of some of the devices in your fleet, Switchboard has implemented **Shares**—which, like Contact Lists, are also subsets of your codec fleet that you can define. You can invite other Switchboard accounts to add your Shares, and your codecs become visible to them.

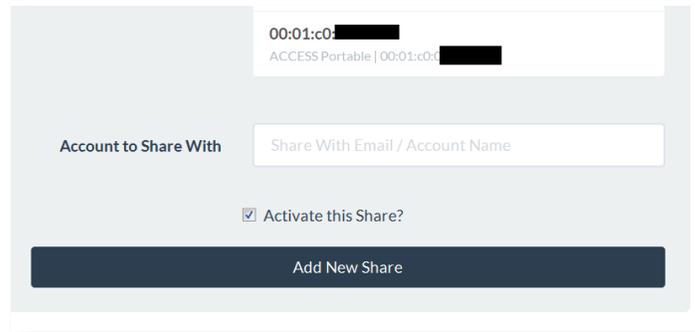
To create a Share, click the **Sharing** tab and then select **Add New Share**.



The following screen then allows you to choose which codec(s) you want to include in this Share.

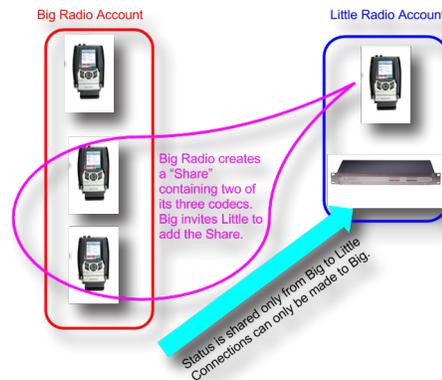


After you make your selection, you'll need to enter one of the following to identify the account you wish to Share your unit(s) with: the official name of that account as it's listed in Switchboard; or the email address for the account's administrator (which must match the email Switchboard has for that user).



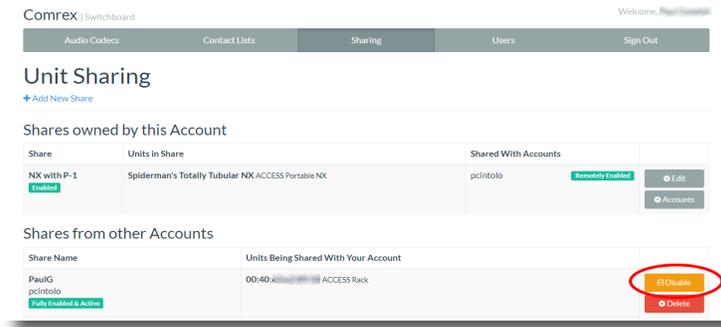
An email will then be sent from the server asking the user to confirm your Share. Once they've confirmed the Share, your Shared devices will appear as options in their contact list menu.

Please note: Shares are a one-way transaction. If you want a Share to be two-way—i.e., one where the person you're Sharing a unit with (a.k.a. the "external user") also allows you see their own unit(s)—you both must first **send** each other a Share invitation and then each **accept** the other's invitation.



Just as with normal units within a Switchboard account, an external user must then **add** a Shared unit to a Contact List in order for it to be visible to other units in their fleet. (This is true even if they're only using the single default Contact List.)

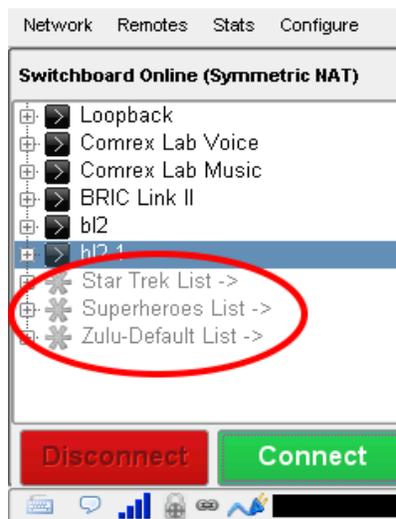
Finally, while it is possible to delete Shares, we recommend **disabling** them instead. This allows you to stop the Share but doesn't require you to do any work to recreate it if you later decide that you still want it. To disable a Share, simply click the orange **Disable** button on the bottom right of the Share edit page.



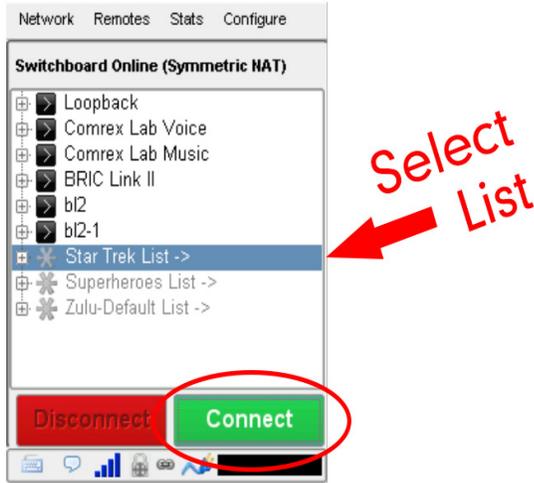
MANAGING MULTIPLE CONTACT LISTS

While most people will only use the default Contact List, it is possible in Switchboard to create and Follow multiple Contact Lists as well as to manage them from a codec's user interface.

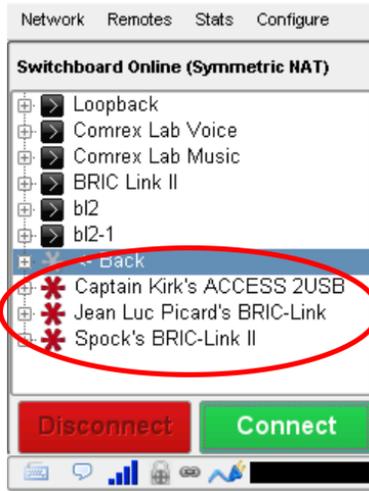
If multiple Contact Lists have been designated as "Followed" on a unit's Switchboard interface, each Contact List will appear at the bottom of the unit's Remotes tab (as shown below).



To view and/or connect to the unit(s) within a list, select the list and press "Connect" (as shown in the next figure).



When you view the units within a list, the lists themselves will temporarily disappear from the screen (as shown below).



To view the lists again, select "Back" and press "Connect" (as shown in the next figure).

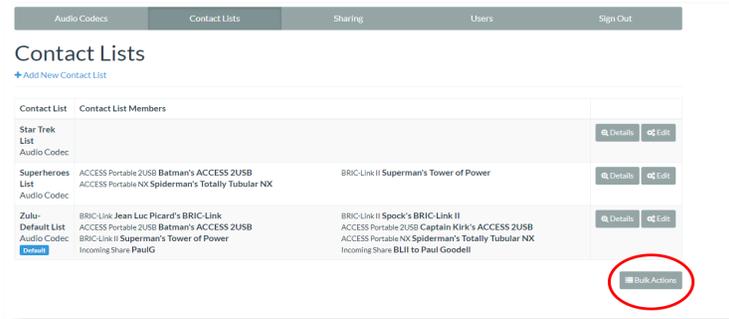


Please note: You can **only** view a Contact List on **your** codec if **your** codec is Following that list.

BULK ACTIONS FOR CONTACT LISTS

It is also possible within Switchboard to perform an action that impacts all of the codecs in a given Contact List in a single step called a **Bulk Action**.

To do this, press the **Bulk Action** button in the bottom right corner of the Contact List tab.



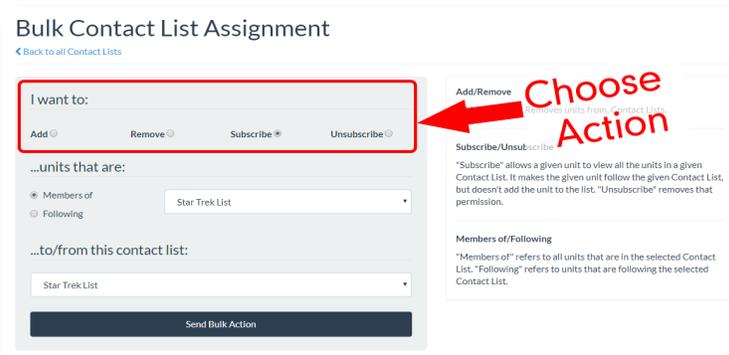
The three steps to create a Bulk Action are:

1. Choose the type of action you want to perform.
2. Select the codecs you're targeting with this change.
3. Identify the Contact List that will be impacted by the change.

Step 1: Choose the Action Type

First, you must select which of the four types of Bulk Actions you want to perform:

- ADD codecs **to** a Contact List;
- REMOVE codecs **from** a Contact List;
- SUBSCRIBE **to** a Contact List (i.e., have multiple codecs **Follow** that list);
- UNSUBSCRIBE **from** a Contact List (i.e., have multiple codecs **stop Following** that list).



Step 2: Select the Target Codecs

Next you must choose which list of codecs you're targeting with this Bulk Action.

Bulk Contact List Assignment
◀ Back to all Contact Lists

I want to:
Add ◯ Remove ◯ Subscribe * Unsubscribe ◯

...units that are:
 Members of Following

Star Trek List

...to/from this contact list:
Star Trek List

Send Bulk Action

Add/Remove
Adds units to, or Removes units from, Contact Lists.

Subscribe/Unsubscribe
"Subscribe" allows a given unit to follow all the units in a given Contact List. "Unsubscribe" removes that permission.

Members of/Following
"Members of" refers to all units that are in the selected Contact List. "Following" refers to units that are following the selected Contact List.

When you complete this step, remember to specify whether you want to target the units that are part of a Contact List or the units that are Following that list (i.e., the option in the yellow-outlined box on the middle-left of the above figure).

Note: Bulk Actions can ONLY be performed on ENTIRE Contact Lists. They CANNOT be performed on individual codecs or on a portion of a Contact List. This means that a Bulk Action **will affect ALL of the codecs** that are either part of a Contact List or are Following that list.

If you only want to change a subset of the codecs in a list, we recommend that you create a new Contact List with only those units in it and then perform the Bulk Action using that list.

Step 3: Identify the List That Will Be Changed

Lastly, you must choose the Contact List that will be affected by this Bulk Action. This will be the list that will have codecs added to it or removed from it, or which will have codecs Follow it or stop Following it.

When you are finished, press the **Send Bulk Action** button.

Bulk Contact List Assignment
◀ Back to all Contact Lists

I want to:
Add ◯ Remove ◯ Subscribe * Unsubscribe ◯

...units that are:
 Members of Following

Star Trek List

...to/from this contact list:
Star Trek List

Send Bulk Action

Add/Remove
Adds units to, or Removes units from, Contact Lists.

Subscribe/Unsubscribe
"Subscribe" allows a given unit to follow all the units in a given Contact List. "Unsubscribe" removes that permission.

Members of/Following
"Members of" refers to all units that are in the selected Contact List. "Following" refers to units that are following the selected Contact List.

SWITCHBOARD THEORY AND CONCEPTS

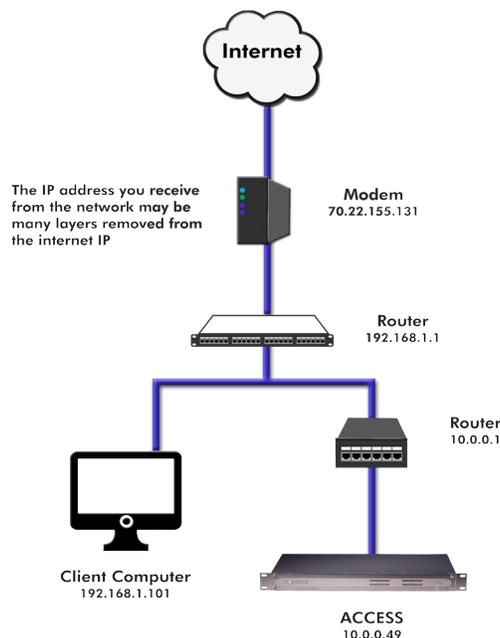
Switchboard is useful because it's not always simple to connect two devices over the internet which are essentially "peers". There are two major reasons for this. First of all, to initiate a stream to a device over the internet requires that you know its IP address. This is the number that gets applied to the destination field of the IP packet, so internet routers can determine how best to send it along its way. Every device that connects directly to the public internet must have one.

However, when web browsing or sending email, this information is usually hidden from the user. In the traditional client/server scenario, such as web browsing, a Uniform Resource Locator (URL) is used to represent the IP address of the web page (which is decoded by a DNS server). Once a computer requests a web page from a web server, the web server can automatically derive the reply address from the request and respond to it. So the traditional four segment decimal address (e.g. 70.22.155.130) is completely obscured to the user.

Even if you know your IP address, it's quite possible that address will change over time. This is because the vast majority of internet users establish their addresses via DHCP, a protocol whereby a server (maintained by the ISP) will deliver one of their available addresses to the client on initial connection. That address is "leased" from the server for a particular time period. After the "lease" expires, the server is free to change it.

The commonly used Network Address Translation (NAT) router adds to the confusion, making codecs even harder to find. Most LAN-based internet connections (as opposed to computers connected directly to ISPs) actually negotiate with a local router containing its own DHCP server. This router assigns the LAN computer or device a "private" IP address.

We'll cover more about the challenges of connecting codecs behind NAT routers shortly. For now, remember that one of the problems NAT servers add is that the private IP address delivered to the codec (and the only address of which the codec is aware) has no bearing on the public address seen from the internet. In extreme scenarios, several layers of address locality can be stacked, assuring that the IP address assigned to your device is several degrees removed from the public IP address used for connections. Also, each address in the stack is temporary and able to change at any time.



Before deployment of Switchboard, the answer to this dilemma was to assure that the codec located in the studio has a fixed, public IP address. By fixed, we mean that the address is allocated exclusively by the ISP, and that address is entered manually into the configuration of the codec and is not subject to change. This scenario works because IP “calls” are usually initiated from the field. As long as the field unit can find the fixed address of the studio unit and send a stream to it, a reverse channel can be created easily and automatically by the studio unit, using the source information contained in the incoming packets. Even in this scenario, the studio IP address must be memorized or input into each codec individually.

The first function Switchboard works around is the dynamic IP address problem; it does this by acting as a Directory Server. Codec users simply log in to the free server and are given an account name and password. Once logged in, it’s a simple process to input the details of each codec owned. On the codec itself, the user will input a familiar name by which the codec will be known within that group.

Once enabled, a codec in the group that is physically connected to the internet will sync with the server. The current public IP address of the codec will be obtained by the server and the user directory will be updated with the new IP address.

In addition, the availability status of the codec is also updated. The codec will “ping” the server if anything changes (address, status, etc.). As we’ll see, this “ping” function will prove useful in other ways.

Once the codec has updated its status with the server, it’s time to download the directory. This process happens instantly. The update includes current addresses and status info for all codecs within the group. This information forms a sort of “Buddy List” that gets integrated into the codec’s connection address book. The list may still consist of entries made manually by IP address into the codec, but those are signified by a different icon. Current status of each codec is reflected by graying out entries which are not currently connected or that haven’t been synchronized to the server.

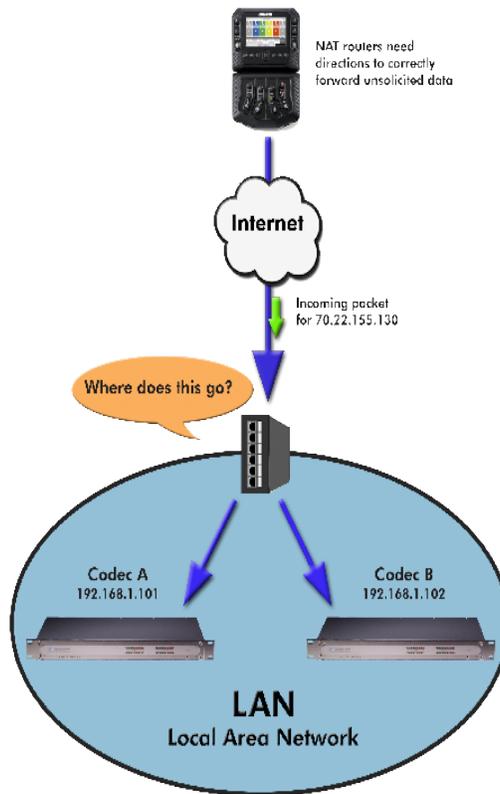
If IP addresses should change, the codec will re-sync with the server from the new address, and all will be updated automatically. Connections can be made by simply clicking on the correct name, without any updating on the part of the user.

The other roadblock provided by the use of NAT routers is the inability to accept unsolicited incoming connections from the Internet. Generally, this function acts as a rudimentary firewall and is a net positive for security, but it does cause headaches for codec users.

A router that receives a connection request doesn’t have a clue where to forward that stream unless it has specific instructions programmed into it. These instructions are known as “port forwarding”.

This can work well for fixed installations, but it’s not always an easy task to obtain that kind of security access on corporate routers. Also, forwarding functions are implemented differently on different hardware. You can easily imagine the complications of obtaining or managing port forwarding on the LAN when arriving at a new remote venue. You would likely encounter a large amount of resistance or confusion on the part of local IT staff.

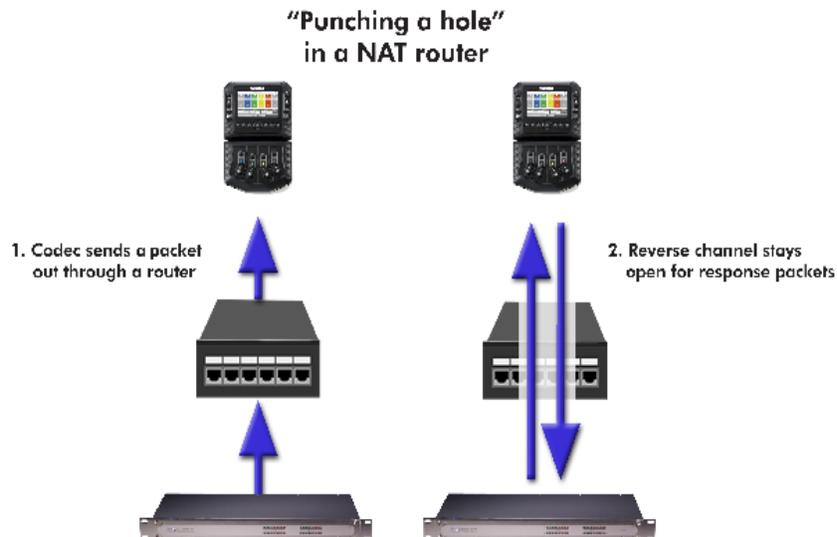
In describing NAT routing, it's important to understand the concept of ports. These are numbers, like the source and destination IP addresses that are attached to each packet. They further qualify which application on a computer (or codec) is meant to send or receive a packet.



In a typical codec application, Codec X will send a packet from Address A Port B, to Address C Port D on the Destination Codec Y. A codec that has multiple applications running (like streaming audio while simultaneously serving a configuration web page) would deliver these applications from, and to, different port numbers, but perhaps to the same IP address. Port numbers are also used by NAT routers in segmenting applications flowing through them, and they may change source port numbers at will.

Network Address Translation (NAT) refers to the ability of a router to translate requests from computers (or codecs) within its LAN onto the public internet. On its most basic level, this involves replacing the private "source" or return IP address in each packet with the true public IP and remembering where that packet was sent. This insures that any response can be forwarded back to the proper device.

A good way to think of this is that an outgoing packet "punches a hole" in the router, through which authorized reply packets may be returned to the codec for a limited time.



Switchboard aids in breaking through these different types of routers for incoming calls. Because it is in constant contact with all subscribed codecs, it can send and receive test patterns to determine whether one or more NAT routers exist on a link and what type they are. It can then choose a connection method to be used to circumvent any issues. Switchboard can:

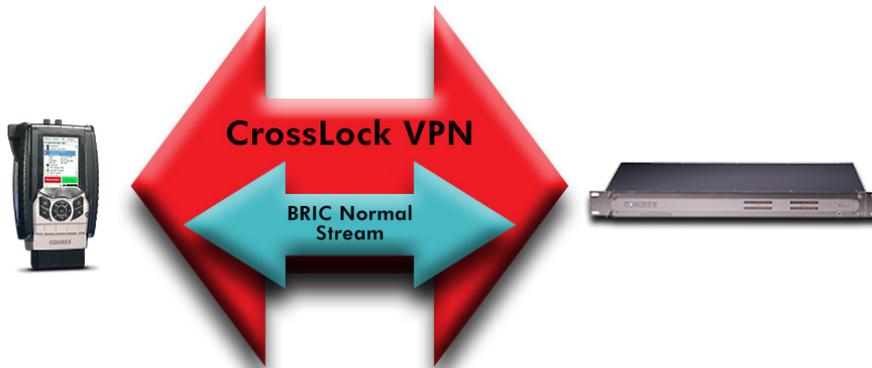
- Instruct the calling codec to make a normal connection (no NAT detected).
- Use the hole punched by connection to the Directory Server for incoming connections from other codecs.
- Instruct the called codec to make the connection in the reverse direction.

The second option, which utilizes the outgoing Directory Server “ping” described earlier, is very useful. The interval of this ping is adjustable, but defaults to about one minute, which is short enough to keep a hole punched through the majority of NAT routers.

These techniques are based loosely, with enhancements, on a generic Internet protocol called STUN (Simple Traversal of UDP through NAT). The system works well in all environments except one: when both users are sitting behind a symmetric NAT. In this situation, calls will fail even with Switchboard. The only option in that environment is to resort to port forwarding on one side of the link.

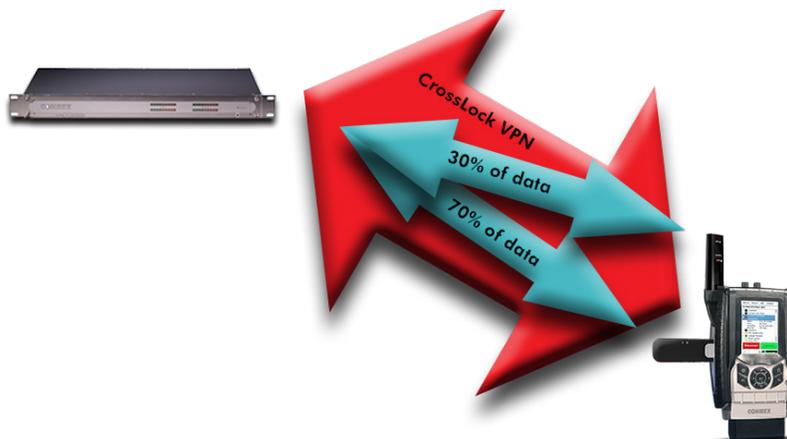
xvi. **CROSSLICK DETAILS**

As briefly described in the **Introduction to CrossLock** section, CrossLock describes a new reliability layer that gets established between Comrex devices in advance of a connection. This layer takes the form of a Virtual Private network (VPN) between the devices. The ACCESS Media stream is carried within this VPN.



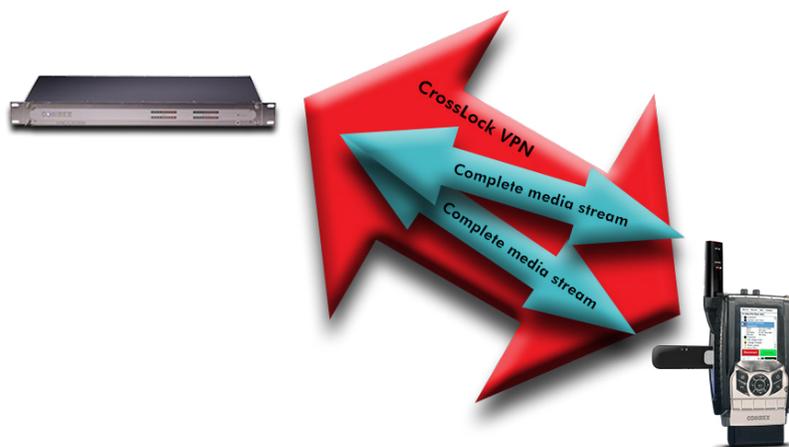
In addition to carrying the audio media, **CrossLock** allows lots of other information to be shared between the endpoints, including information about network quality and far-end delay settings. This provides for much better delay management on both ends of the link.

One or both ends of a **CrossLock** connection can utilize multiple network interfaces. This can take the form of two Ethernet connections, or any mix of wired and wireless networks. A common usage scenario would be attaching two 3G/4G modems to an ACCESS portable. In the case of one network underperforming, the majority (or all) of the data will be sent on the good network.



By default, **CrossLock** will utilize any network ACCESS senses as capable of carrying reasonable data. If a network increases in delay and packet loss, ACCESS may decide to remove media data from that network entirely. ACCESS may still use the network for background communications and error correction.

CrossLock's default configuration is "Bonding" mode, which is the best for most users. This will sum together the possible bandwidth of the available networks and send a single media stream, along with background and error correction information. An alternative mode can be employed; it is known as "Redundancy". In this mode, the entire media stream is replicated on each network (along with background and error correction info). This mode is preferred only in environments where both networks have wide network bandwidth and low delay (as in wired networks). Because Bonding mode is more adaptive and has fast recovery capability, it is preferred for wireless networks. To change **CrossLock** from the default Bonding to Redundant mode, go to **System Settings->CrossLock settings** and set the value to **On** for the **Redundant Transmission** entry.



Usage of dual networks on both ends of the link is not supported when at least one codec is ACCESS 2USB. The CPU power in ACCESS 2USB cannot support this.

CROSSLOCK AND SWITCHBOARD

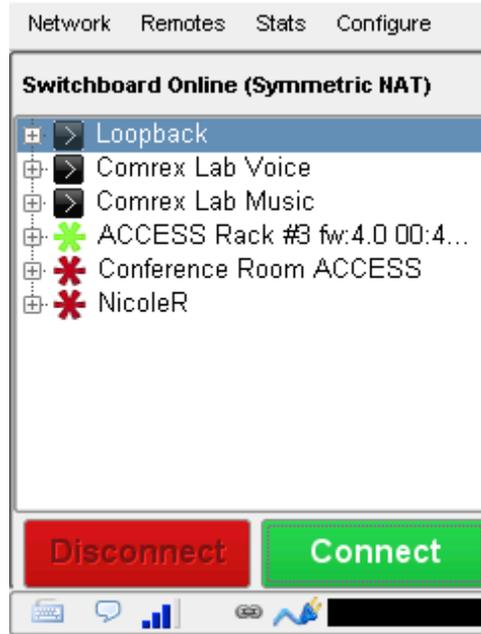
It is recommended that **CrossLock** connections be made in conjunction with the Switchboard Traversal Server. ACCESS users can get a Switchboard account for their codecs by contacting Comrex. For configuration and operation of Switchboard or ACCESS, review the previous section titled **Switchboard Traversal Server (TS)**.

Switchboard is useful, especially when using **CrossLock**, because ACCESS units need more information about their connection peers than is required in non-**CrossLock** connections. In addition to the destination IP address, **CrossLock** connections require each ACCESS to know the **Unit ID** of the other. This is required as a security function, since **CrossLock** establishes a VPN between units. The Unit ID of an ACCESS codec is the MAC address (Switchboard ID) of the codec.

When making connections via Switchboard, the IP address and the Unit ID (Switchboard ID/MAC address) is transferred between the codecs automatically, and doesn't need to be entered into the initiating codec.

Switchboard delivers a “buddy list” to each ACCESS in the fleet. This list appears on the **Remotes** menu of the 2USB.

The connections have a color coded “gear” icon to indicate the status of each other ACCESS or BRIC-Link in the fleet. Items with a green gear are ready for connection. Yellow means busy, and red means off-line.



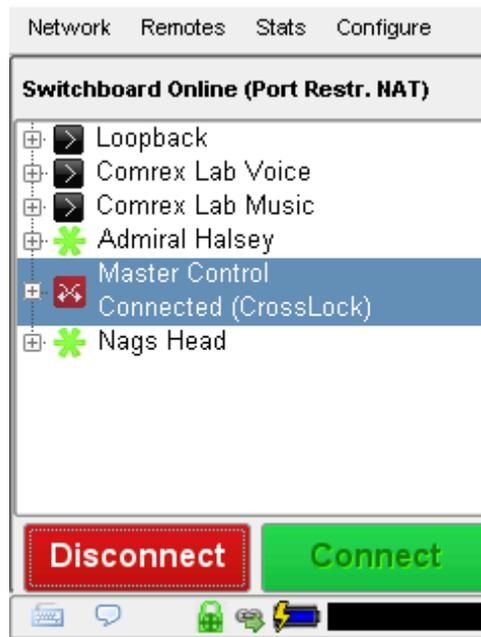
MAKING CROSSLOCK CONNECTIONS VIA SWITCHBOARD

There is no difference in making Switchboard connections via **CrossLock** and non-**CrossLock** methods. If a connection is attempted via Switchboard, and the following are true:

- 1 The ACCESS on the far end is running firmware 4.0 or higher
- 2 The **CrossLock** port (UDP **9001**) is open to the far end
- 3 Each ACCESS is aware of the other’s Unit ID (Mac address). This is handled behind the scenes in Switchboard.

Then a **CrossLock** connection will be attempted. If port **9001** is blocked, or if the far end connection has 3.x or lower firmware, the connection will proceed in the legacy “BRIC Normal” mode.

A successful **CrossLock** connection is indicated by a green “Lock” icon in the lower banner. Because **CrossLock** is established before an audio stream, and lingers for some time after, this may stay green even when an audio stream is not active.



MAKING CROSSLOCK CONNECTIONS WITHOUT SWITCHBOARD

In the case of non-Switchboard-based connections (e.g. closed networks or STLs), you will need to know the Switchboard ID (Primary Ethernet MAC address) of the unit to which you wish to connect. This is input to the “Create New Remote” pop-up in the “Switchboard ID” field.



In addition, the codec receiving the connection must have a similar entry made, with the MAC Address of the calling unit populated.

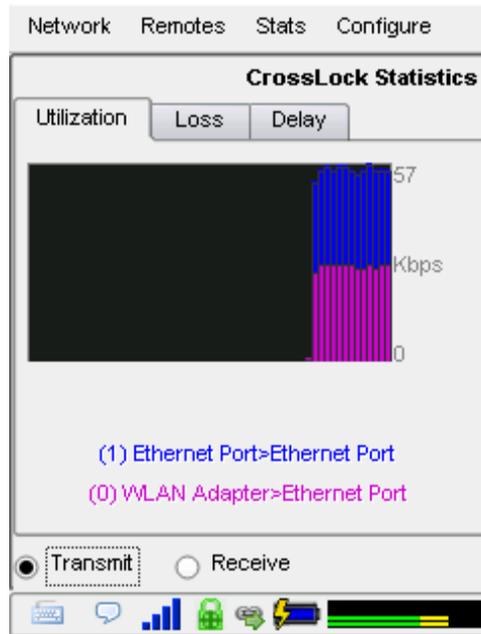
This is important. The receiving unit must have an outgoing connection programmed into its address book, containing the Switchboard ID (MAC address) of the calling unit, even if that entry is never used for outgoing calls.

Once a Switchboard ID (MAC address) is populated in the field, you will have the option of disabling or enabling **CrossLock** for this connection.

CROSSLOCK STATS

When a **CrossLock** connection becomes active, the **CrossLock** stats are activated. The stats are a very powerful tool to diagnose the quality of connections, and manage the delay settings during the connection.

UTILIZATION GRAPH



The **Utilization** tab displays a graph of the outgoing (or incoming) utilization of the network. The bars indicate the average data rate used by the system during each one-second window. It is expected that the size of these bars will vary because **CrossLock** has control over data rate through a technique called “throttling”. Based on network feedback statistics, **CrossLock** will reduce and increase the utilization dynamically.

If more than one network device is in use, the utilization graph will be color coded, indicating the relative utilization of each network device. The color code key for each network device appears under the graph.

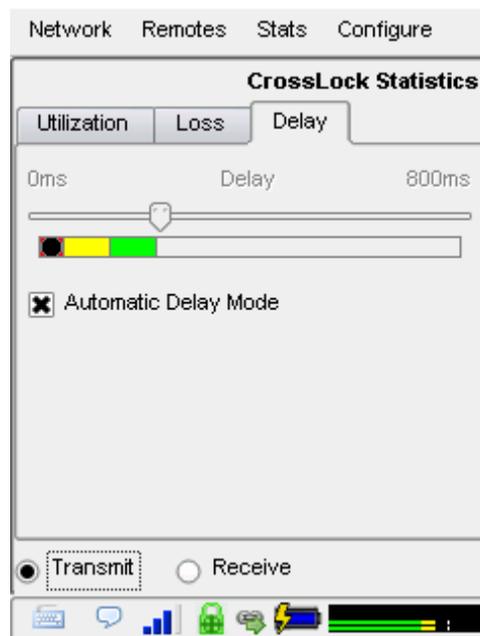
PACKET LOSS GRAPH

By selecting the **Loss** tab, you will see a graph that indicates, in percentage terms, what's gone wrong on the network during each one-second window. Three different color-coded entries appear here:

- 1 **Packet Loss (dark red)** - The system has detected that a packet has been completely dropped by the network and was never received by the decoder.
- 2 **Packet Late (bright red)** - The system received the packet, but it was too late for decoding and playout.
- 3 **Packet Recovered (green)** - The packet was either lost or late, but was recovered either by the Forward Error Correction (FEC) or Automatic Repeat Query (ARQ) error correction built into **CrossLock**.

DELAY SLIDER

The most powerful way to stabilize any streaming connection is to have the decoder add a delay buffer to the connection. This compensates for changes in the rate packets are received—known as jitter in Internet speak. **CrossLock** uses a combination of decode delay buffering and error correction to keep connections stable. When **CrossLock** is active, the activity of the delay buffer is illustrated and controlled via the delay slider on the **Delay** tab.



The slider above is in **Auto Delay** mode and the information on the slider is purely for informational purposes. Clicking off the **Auto Delay** box sets the system to **Manual Delay** mode and allows the slider to be moved via the touchscreen.

The entire slider is scalable, and the range of it from left to right will vary from one hundred milliseconds to several seconds depending on the range of delays currently being addressed. In either **Auto** or **Manual** mode, a series of color bars are overlaid on the slider, to signify delay “zones” of safety.

Furthest left is the red zone, which indicates a buffer level that is too low for stable transmission. The yellow zone indicates a delay buffer that may have stability issues, and the green zone indicates a buffer level that should provide stability. These “zones” scale, increase and decrease in size, based on the history of jitter experienced by CrossLock on the network.

In **Auto Delay** mode, two other elements are of interest. The downward arrow signifies the **Target Delay**, which is the best compromise value calculated by the system to balance stability and delay. The “bubble” indicates current delay. The Current Delay bubble will attempt to track with the **Target Delay Arrow**, but may at times fall outside it. This usually indicates that the system is actively reducing or increasing the buffer.

In **Manual Mode**, the arrow becomes a moveable cursor, and it’s up to the operator to determine how best to set the compromise between delay and stability.

Any settings made in Manual Mode will be erased after the current **CrossLock** session is terminated.

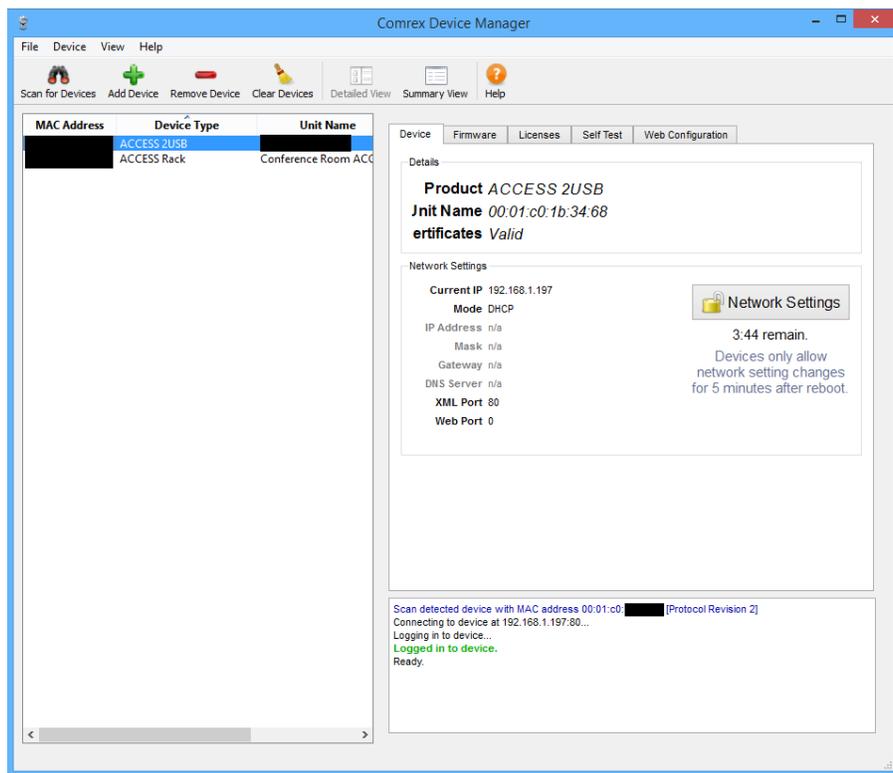
xvii. DEVICE MANAGER

Device Manager is a free program for both Windows and MAC that provides a simple and elegant interface for updating, configuring and managing your Comrex devices. With **Device Manager**, you can configure the IP Networking details, update firmware, enable license features, copy and save configuration information, and more. **Device Manager** was included on the CD sent with your Comrex equipment and can also be downloaded from our website at <http://www.comrex.com/products/device-manager/>.

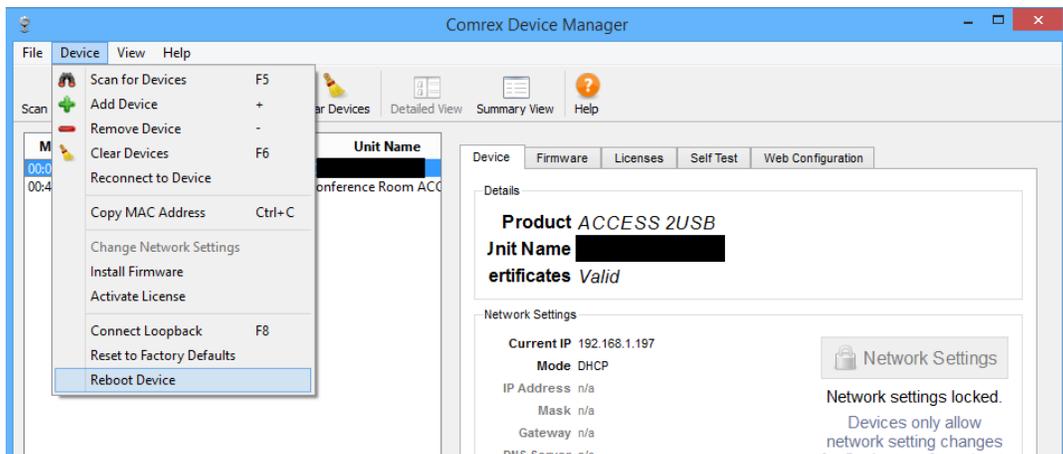
USING DEVICE MANAGER

After **Device Manager** is installed, open the program and simply click “**Scan for Devices**” to find any device that is on the same physical IP network as your computer. The list will include the unit MAC address (Switchboard ID), the device type, and the unit name. Alternatively, if you know the public IP address of a Comrex device and TCP port 80 has been forwarded to that device, you can manually add the device and perform certain functions, such as updating firmware, from outside your network.

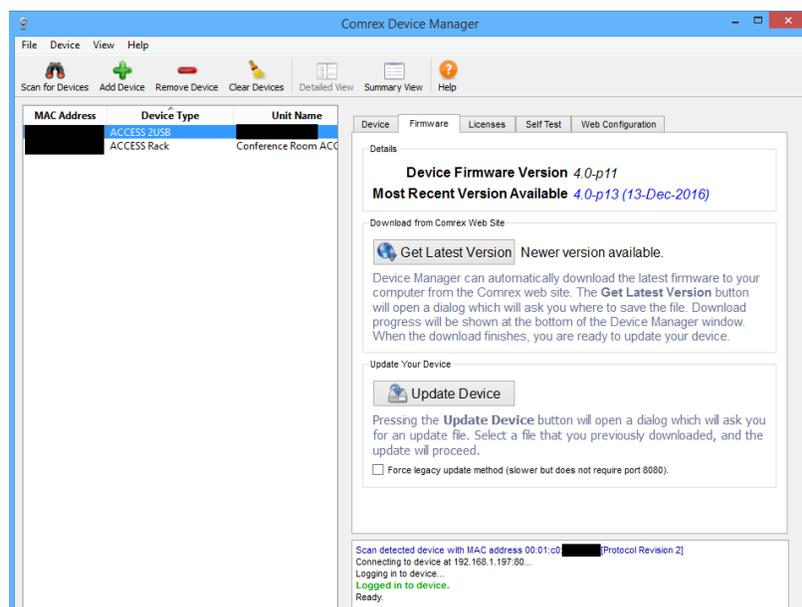
Once a unit is selected, five tabs appear on the right-hand pane.



The first tab is the **Device** tab. This tab will give you the current IP address and network settings. As a security measure, network settings may only be changed during the first 5 minutes of your Comrex product operation. If you wish to change your network settings, you will have to reboot your unit and make the changes right away.



TIP: To reboot your unit, go to the Device menu located at the top left of the window and select Reboot device.

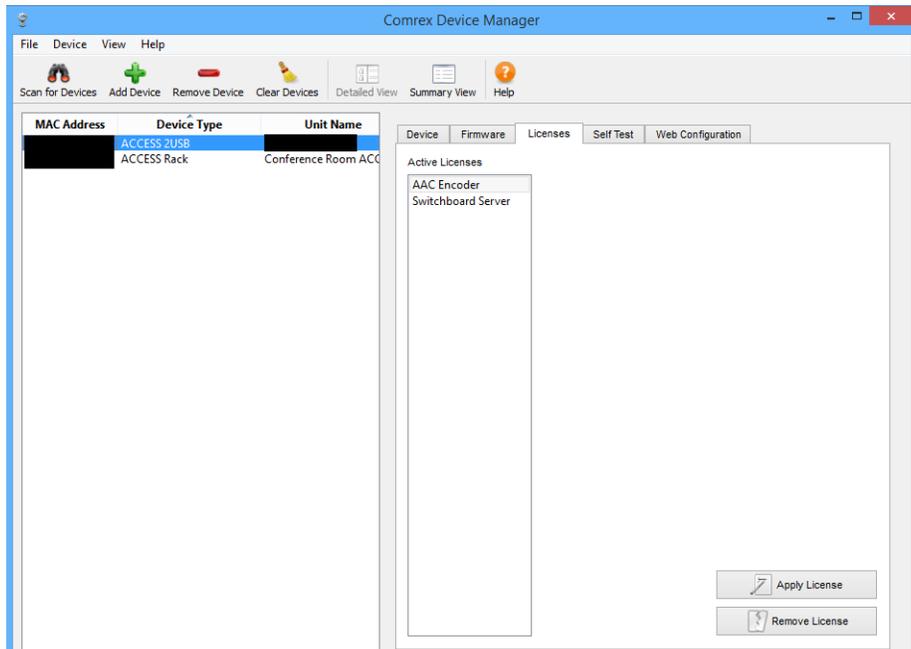


The **Firmware** tab shows you the device firmware version you currently have, as well as the most recent version available. If there is a more recent version, it will appear in blue.

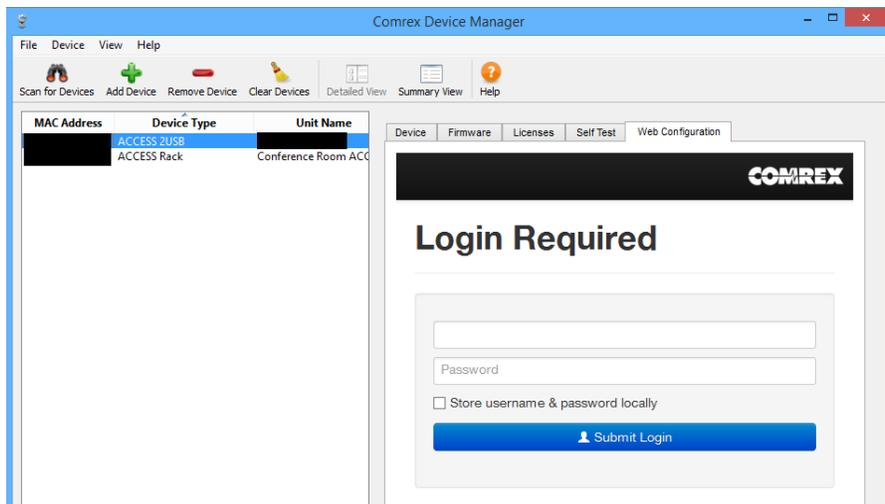
Comrex STRONGLY encourages keeping your units up to date and checking for updated firmware on a regular basis.

To update your device, select **Get Latest Version** to download the update file. Next, click **Update Device**. You will be requested to select the file to use. Navigate and select the file you just downloaded. The status of the upgrade will show in the bottom of the window. Once completed, the device will automatically reboot.

The **License** tab shows you which licenses are currently active to your unit. This is also where you can add and/or remove licenses.



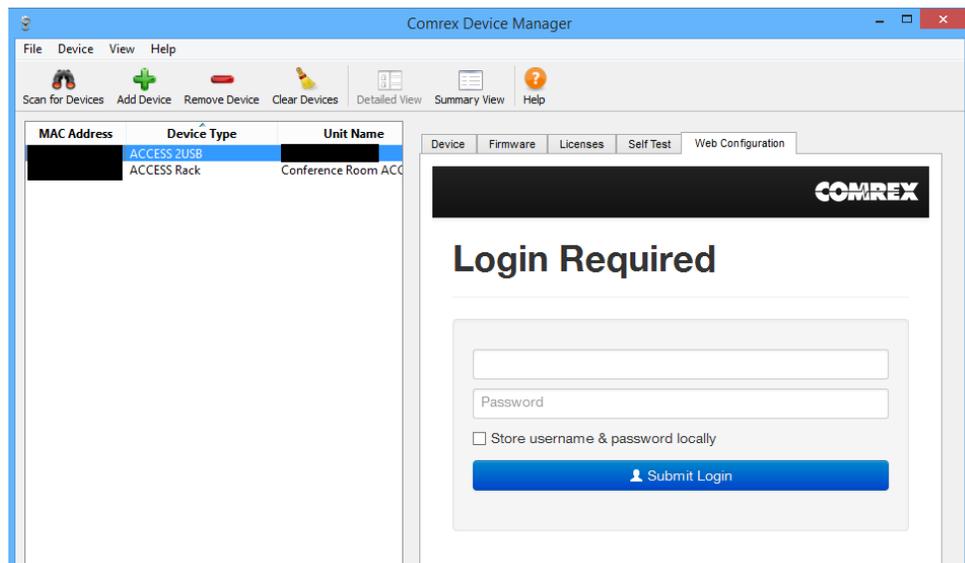
The fifth tab is labeled **Web Configuration**. This will open a simplified setup interface on ACCESS called **Toolbox**. The **Toolbox** interface allows you to configure several options including the Ethernet port. You will need to log in to **Toolbox** separately with a user name (any) and password (default = **comrex**) to enter the **Toolbox**. To learn more about Toolbox, visit the section **Toolbox on page 83**.



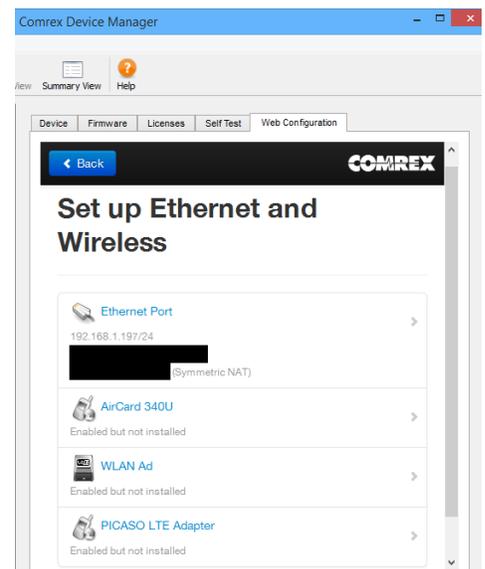
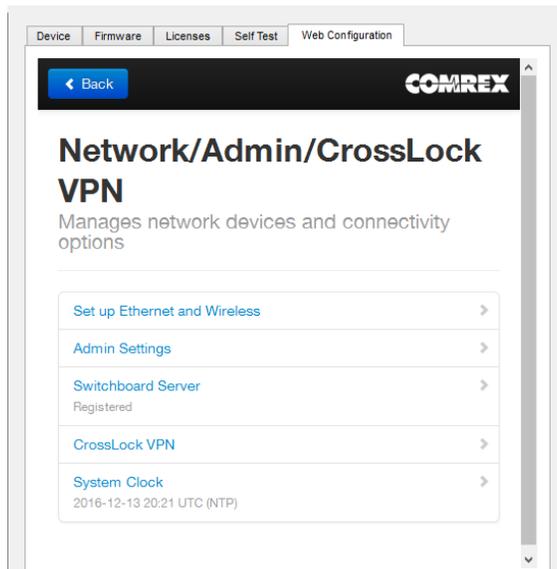
xviii. TOOLBOX

Toolbox is a network manager that allows for easy network configuration. Typically you will be using your 2USB touchscreen to perform these operations as described in the **Network Menu** section, but in some cases, such as when configuring an ACCESS Rack, it can be much easier to use **Toolbox**.

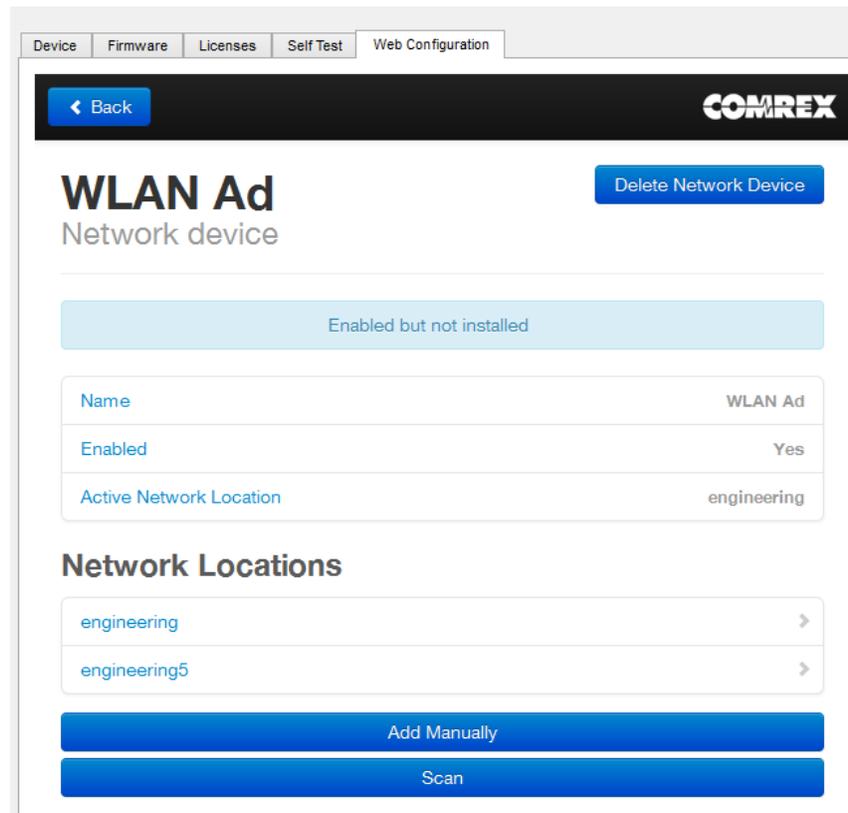
You can log into Toolbox either via **Device Manager** or through the IP address of the unit with **/cfg** appended to it (e.g. **192.168.0.34/cfg**).



Once logged into **Toolbox**, choose the **Network/Admin/CrossLock** option and then choose **Set up Ethernet and Wireless**.



From here, you can select the device you would like to configure and then adjust the parameters for that device. You can edit the **Name**, if it is enabled or not, and the **Active Network Location** (explained in the next paragraph).



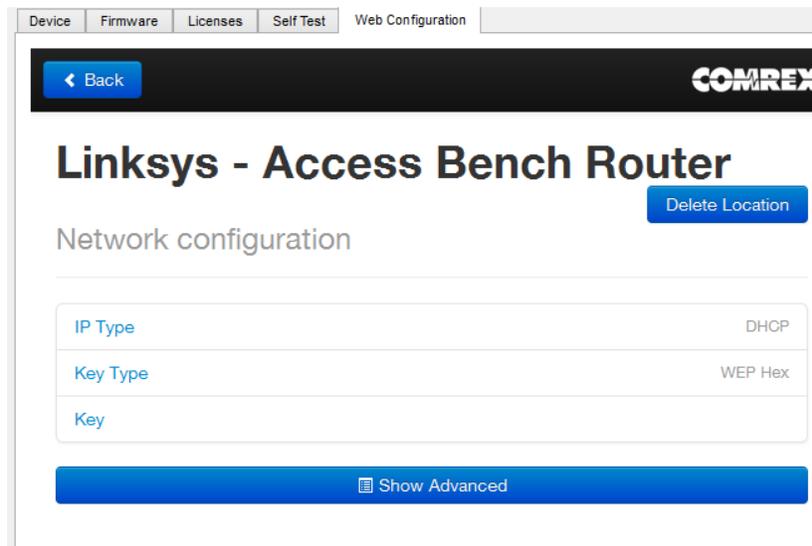
LOCATIONS

Locations are entries that are saved in your unit so that you can store network information for various environments and not need to enter it in every time. For example, if you are moving ACCESS between venues, and want to store the static IP information for each venue, you will define a new “location” (giving it a unique name). Once multiple locations are defined, you can switch between them using the **Active Network Location** option. Locations can be configured for any network device, including the Wi-Fi adapter. This can be useful in programming credentials for use in multiple Wi-Fi environments.

CONFIGURING WI-FI

When setting up a Wi-Fi connection, you can scan for all available Wi-Fi networks using the “Scan” function.

Once selected, you can enter in the details for that network, including the network key, if needed.



Once created, you can assign that network to the adapter by selecting **Active Network Location** and selecting the network from the drop-down list.

Active Network Location

The currently active network location

Default: (Automatic)

If the Wi-Fi adapter's location is set to **Automatic**, it will check all location settings when the Wi-Fi adapter is enabled, and choose the first location "match" it finds.

ADVANCED NETWORK SETTINGS IN TOOLBOX

By choosing “**Show Advanced**” under any network, the following options appear:

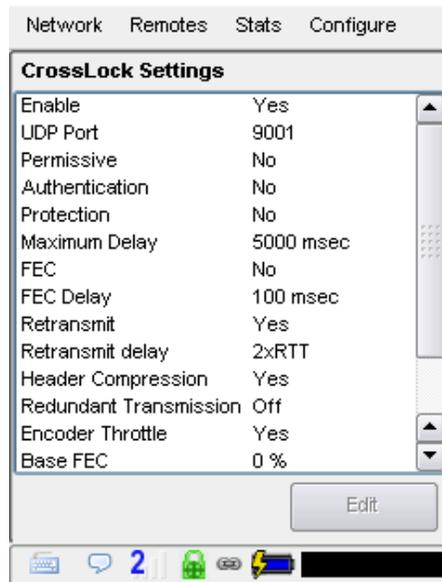
Preserve after Reset - Normally, when ACCESS is set back to factory defaults (via **Device Manager**), all the network settings (including the main Ethernet) are erased. By setting this option to “**yes**”, the settings for this network will be preserved after factory reset. Caution should be used, as it’s possible to “lock yourself out” of the ACCESS by setting the Ethernet parameters incorrectly.

Use with CrossLock - Normally enabled, this option allows you to specify that this network port will not be considered as part of a **CrossLock** connection. This may be valuable when using one port for control purposes only and a secondary port for **CrossLock** media.

Broadcast Config - Normally enabled, this option instructs ACCESS not to respond to the “**Scan**” function used by **Device Manager**. Caution: without the “scan” function, **Network Recovery Mode** is disabled.

XIX. MAKING BRIC NORMAL CONNECTIONS

If you would like to bypass **CrossLock** mode entirely, it can be disabled in the system settings menu. Under **Configure->System Settings->CrossLock VPN Settings**, choose “enable” and deselect the enable option. No outgoing or incoming **CrossLock** connections will be possible.



It is also possible to disable individual **CrossLock** connections under remote entries that appear in the Switchboard list. By choosing “**Change Remote Settings**” and deselecting the **CrossLock** option, this connection will bypass **CrossLock**.



xx. OPERATING ACCESS IN A 24/7 ENVIRONMENT

In BRIC Normal mode, the default mode of operation, ACCESS transfers all its audio data via the UDP protocol. This is in contrast to most web-based connections, such as web browsing and e-mail. These use TCP protocol. UDP, unlike TCP, is not “connection oriented”; that is, no virtual connection actually exists in this protocol layer between the devices.

In UDP, the transmitter simply launches packets into the network with the correct address, hoping the network will deliver the packets in a timely fashion. Since there is no intelligent connection built between the codecs, there isn’t actually any connection to break in the event of network failure.

If a packet is delayed or lost, no error message is sent and no packets are retransmitted. It is up to the receiver to cover up any lost data, if it can. This allows delivery of the packets with the smallest amount of overhead and delay.

Therefore, the usability of the network is the important factor, not the existence of a physical connection. Loss of the remote will usually be due to a network failure. (If the network fails and is later restored, the packets stream will be restored to the decoder.)

For most applications, such as remote broadcasting, it’s useful to simulate a connection-oriented stream, so ACCESS uses a low-bandwidth sub channel to deliver information back to the encoder about overall connection status. It does this in its “application layer”, rather than the “transport layer”, which is where UDP exists.

By default, it monitors the health of a connection. If no data is detected as received by the decoder during the preset user adjustable timeout, it “tears down” this connection and goes back to idle state. This can give an indication to the user that the network has failed and it’s time to look at the problem.

The good thing about having the connection protocol in the application layer is that its use is optional. For 24/7 operation, there’s no advantage to having the connection end if no data is received for a timeout interval.

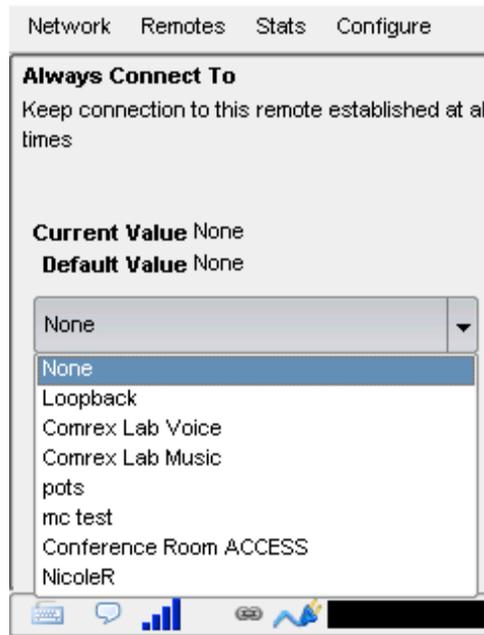
To set ACCESS for 24/7 operation, several parameters are changed:

- 1 The timeout value is set to infinity—the connection will never be torn down regardless of data.
- 2 ACCESS is configured to re-establish the connection in the event of a power re-cycling.
- 3 The local **Disconnect** control is disabled. The **Disconnect** function on the receiving side is still enabled, but will result in an immediate reconnection by the initiating side.

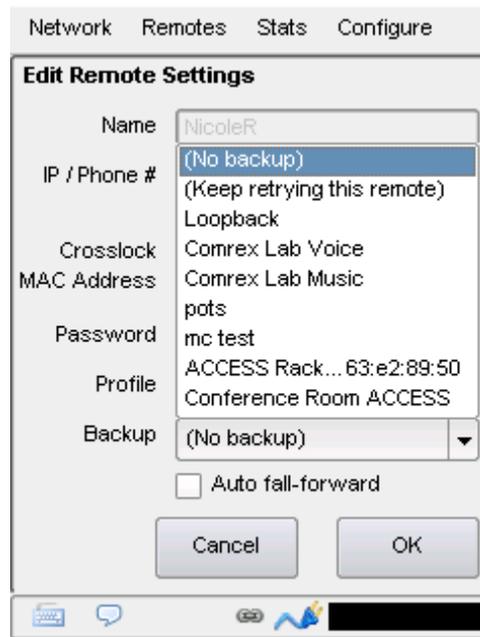
SETTING ACCESS FOR 24/7 OPERATION

On the ACCESS 2USB, go to the **Connections** section of the **System Settings** menu.

The field labeled **Always Connect To Remote** offers a pull-down menu of all available connections. Setting this value to one of your pre-defined connections results in configuring the unit for 24/7 operation to that remote. No configuration is necessary on the remote side.



ACCESS has another option for continuous connections. When building a remote entry, there is a field for backup options. One of those options is called **“Keep Retrying This Remote”**.



Using this mode will allow the unit to disregard the timeout value and keep a persistent connection. The difference is that the **Disconnect** function still works and the connection will not be reinitiated on a power re-cycle. This mode is meant for users who are making temporary connections, but do not want the system to time out and disconnect in the event of network failure.

xxi. **MAKING EBU 3326/SIP COMPATIBLE CONNECTIONS**

Comrex codecs (and many other brands) have a set of protocols that allow easy IP connections between units. In general, when connecting between Comrex hardware, it's best to use these proprietary modes to take the most advantage of the features of the product.

However, many users are concerned about getting "locked in" to a certain codec brand. Because of this, an international committee was formed by the European Broadcast Union called N/ACIP to hammer out a common protocol to interconnect codec brands. This committee resulted in the establishment of EBU 3326, a technical document which determined standards for codec compatibility.

EBU 3326 by and large establishes a set of features each codec should support, then leaves most of the heavy lifting to other, previously agreed upon standards like SIP (IETF RFC 3261). Topics not yet covered by EBU 3326 include things like carrying ancillary data and contact closures from end-to-end, codec remote control and monitoring, and complex NAT traversal, which at this point are still left to the individual manufacturer's discretion. This is why it's best to stick to a single codec vendor and their proprietary protocols.

MORE ABOUT EBU 3326

The Tech 3326 document defines several mandatory encoding algorithms, and the transport layer that could be used on them for compatibility. However, the most complex part of the standard was the decision on how to arrange Session Initialization, which is the handshake that takes place at the start of an IP codec call. The most commonly used protocol for this is called Session Initialization Protocol, or SIP. This is used extensively by VoIP phones and therefore was a logical choice. SIP carries the advantage of making ACCESS compatible with a range of other non-broadcast products, like VoIP hardware, software, and even mobile phone apps.

EBU 3326 IN ACCESS

ACCESS does not fully comply with EBU 3326, as it does not feature the mandatory MPEG Layer II codec. Aside from this, ACCESS has been tested to be compatible with several other manufacturer's devices using encoders supported by both products. When using **EBU 3326/SIP Compatible** mode (this is how the user interface describes EBU 3326), ancillary data, contact closures, Switchboard TS, Multi-streaming and Multicasting are not supported. Outgoing call profiles built with the EBU 3326/SIP channel may lack some advanced options, and can not be set for different encoders in each direction (i.e., EBU 3326/SIP calls are always symmetrical).

EBU 3326/SIP MODES

A function of placing a SIP-style call is the ability to register with a SIP server. This is a server that exists somewhere on the network, usually maintained by a service provider. Several free servers exist that can offer registration, like **Onsip.com**.

ACCESS allows EBU 3326/SIP calls to be placed or received with or without registration on a SIP server. If registration is not enabled, connections are made directly to the compatible device by dialing its IP address, just like in **BRIC Normal** mode.

UNREGISTERED MODE

Placing a call in Unregistered EBU 3326/SIP mode is simple: just build a profile, but instead of choosing **BRIC Normal** channel, choose **EBU 3326/SIP**. This will make sure the call is initiated on the proper ports and with the proper signaling. The majority of system settings relating to EBU 3326/SIP relate to **Registered** mode.

REGISTERED MODE

Registering with a SIP server in **EBU 3326/SIP** mode can have some advantages. When using a SIP server:

- The server can be used to help make connections between codecs through routers.
- The remote codec can be dialed by its SIP URI instead of IP address.
- The SIP server can be used to find codecs on dynamic IP addresses.

SIP SERVERS

A SIP server exists in a domain. This domain is represented by a web-style URL like **sipphone.com** or **iptel.org**. A SIP server or proxy generally handles IP connections within its domain.

SIP URIS

The SIP server assigns a fixed alphanumeric name to each subscribed account. For example, an Iptel user may be assigned the user name `comrex_user`. URIs consist of a SIP user name, followed by a domain, delineated with the `@` symbol, like an email address. Our Iptel user's URI would be `comrex_user@iptel.org`. Comrex devices do not use the designation "sip:" before a SIP address.

If a connection is to be made exclusively within a domain, the domain name can be left off. As an example, to make a call to this codec from another Iptel registered codec, the dialing string can simply be `comrex_user` (with the domain being assumed).

REGISTERING WITH A SERVER

At a minimum, you will need the following information when registering ACCESS with a SIP server:

- 1 The Internet address of your SIP proxy/server (e.g. `proxy01.sipphone.com`);
- 2 The username on the SIP account (this is usually the dialing address);
- 3 The password on the SIP account.

The image below shows where this information can be applied in the **System Settings** section. You will also need to enable the **Use SIP Proxy** option in that menu.



Once this information is correctly entered, a new status line appears on the portable display.



The status will reflect the progress of the registration process. When complete, this will display **Online**. If the box does not display Online after a short time, it usually means that registration attempt failed. It's best to go back and carefully check the registration info. It might also be useful to check that your registration information is valid by using it to configure a VoIP phone or softphone.

SIP registration can be very simple with some servers, and others can require more advanced settings. There are several advanced settings available for use with SIP and they are described in the section **Advanced Settings on page 130**.

MAKING SIP REGISTERED CALLS

When registered, calls made using a EBU 3326/SIP profile behave differently than normal. The address field, regardless of whether it is a SIP URI or an IP address, is forwarded to the server. No connection attempt is made until the server responds.

If the server accepts the address, the call will be attempted. If not, an error message will appear in the status line. There are many possible reasons for call rejection by a server. Some examples are:

- 1 The server does not support direct connection to IP addresses (if the address is in this format).
- 2 The server does not recognize the address.
- 3 The server does not forward calls beyond its own domain.
- 4 The server does not support the chosen codec.
- 5 The called device does not support the chosen codec.
- 6 The address is a POTS telephone number, and POTS interworking is not supported.
- 7 The address is a POTS telephone number, and no credit is available (most services charge for this).

The basic entries provided will allow support for the vast majority of EBU 3326/SIP-based applications. However, there are inevitably situations where the defaults don't work. We've provided some advanced options that can help. As always, these options are located in the **Systems Settings** and can be made visible by selecting the **Advanced** box.

IP Port - Universally, SIP connections are supposed to use UDP port **5060** to negotiate calls between devices (and between servers and devices). Note that this is only the negotiation channel—actual audio data is passed on the RTP ports. Changing this port number will change which incoming ports are used to initiate connections and to which ports connection requests are sent. Obviously, the change must be made on both devices, and this change will essentially make your codec incompatible with industry-standard VoIP devices.

RTP Port - This is one of two port numbers used for audio data transfer (the port number directly above this is used as well). Because this port number is negotiated at the beginning of a call (over the IP port), this port may be changed without breaking compatibility. Note that many SIP standard devices use port **5004** for this function. Due to the negotiation, it is not important that these numbers match on each end. Changing this port to **5004** can actually have an adverse effect, since **5004** is the default port for other services on Comrex codecs.

Public IP Override - See the next section, **SIP Troubleshooting**, for more information.

Use STUN Server - See the next section, **SIP Troubleshooting**, for more information.

SIP Proxy Keepalive - Only applies to **Registered** mode. This variable determines how often the codec “phones home” if registered with a SIP server. It’s important that the codec periodically “ping” the server, so the server can find the codec for incoming calls. It can be adjusted primarily to compensate for firewall routers that have shorter or longer binding timings, i.e., the router may have a tendency to “forget” that the codec is ready to accept incoming calls and block them.

SIP Domain - Only applies to **Registered** mode. This is the name of the network controlled by the SIP server. This parameter must be passed by the codec to the server. Under most circumstances, this is the same as the server/proxy address, and if this field is not populated, that is the default. If, for some reason, the domain is different than the server/proxy address, then this field is used.

SIP TROUBLESHOOTING

In a nutshell, SIP establishes a communication channel from the calling device to the called device (or server) on port 5060. All handshaking takes place over this channel, and a separate pair of channels is opened between the devices: one to handle the audio, and the other to handle call control. The original communication channel is terminated once the handshaking is complete. Note that firewalls must have all three ports open to allow calls to be established correctly. Also, port forwarding may be required to accept calls if your codec is behind a router.

The main area where SIP complicates matters is in how an audio channel gets established once the handshake channel is defined. In the common-sense world, the call would be initiated to the destination IP address, then the called codec would extract the source IP address from the incoming data and return a channel to that address. In fact, that’s how the default mode of Comrex codecs work, and it works well.

But SIP includes a separate “forward address” or “return address” field, and requires that a codec negotiating a call send to that address only. This is important in the case of having an intermediate server. And this works fine as long as each codec knows what its public IP address is.

OUTGOING CALL ISSUES

A unit making an outgoing call must populate the “return address” field. But any codec sitting behind a router has a private IP address, and has no idea what the public address is. So, naturally, it will put its private IP address (e.g. **192.168.x.x** style) address into that “return address” field. The called codec will dutifully attempt to connect to that address and undoubtedly fail, since that can’t be reached from the Internet at large.

INCOMING CALL ISSUES

Incoming calls to codecs behind routers are complicated by the fact that ports on the router must be forwarded to the codec. In the case of SIP, this must be three discrete ports (For Comrex codecs these are UDP 5060, 5014 and 5015) <6014 and 6015 with 3.0 firmware>. And since even the “forward address” is negotiated in SIP, the incoming unit is likely to populate the “forward address” field with its private address as well.

SOLUTIONS

Many times the “return address” field issue is fixed by the SIP server (in **Registered** mode) and no compensation measures are necessary. Often, in fact, the server insists on acting as a “proxy” and handles all the traffic itself—outgoing and incoming streams are relayed directly by the server, solving any router issues.

In point-to-point connections, this isn’t possible. All is not lost here, since we can find some hacks to make this work. The first place to look is your router, since many modern routers are aware of this issue and have taken steps to relieve the pain. If your router supports a SIP Application Layer Gateway (ALG), then enabling this option can fix the issue. Essentially, the router will get smart enough to read your SIP handshake, find the outgoing address field, and replace it with your public IP. This is a pretty slick solution, but there may be environments where you are not aware whether this option is supported on your router, or you may not have the ability to enable it. So on to solution two:

STUNNING SUCCESS

Another technique for working around the SIP-Router issue is by using a protocol called STUN. This can be enabled in Comrex codecs in the **Advanced EBU 3326/SIP** options and essentially allows for the codec to learn what its public IP address is. It does this by contacting a STUN server out on the Internet (the default one is maintained by Comrex) and simply asking. If this option is enabled, the codec itself will handle the address switching.

Be aware of the dreaded “battling workarounds” issue. In our simple description, we left out the fact that ports are being translated by the router as well as IP addresses. If the ALG-enabled router receives an unexpected result in the SIP address field (as it might if using STUN), it may not translate ports as expected, and it’s likely that the call will fail. When in doubt, the best technique is to try a SIP call with STUN turned off, and if the return channel fails, try enabling STUN.

FIX OF LAST RESORT

Finally, there’s a brute-force option available on Comrex Codecs when STUN ports are blocked by a firewall, or can’t be used for some other reason. Under **Advanced System Settings**, a field is available called **Public IP Override**. Any address put into that field will be pasted into the address SIP field. So if you know what your public IP address is (you can obtain it from many websites via a browser) you can manually paste it here. Keep in mind, this is often subject to change over time (and obviously if you use a different network), so it’s important to remember this change has been made on your codec.

XXII. MULTISTREAMING

Note: This section deals with advanced topics relating to ACCESS capabilities.

ACCESS supports the ability to run one encoder per unit, but this single encoder stream may be sent to up to nine destinations simultaneously. We call this capability “multi-streaming”, since the encoder creates a separate but identical outgoing stream to each decoder. **Note: Your Internet connection must be able to support these streams.** For example, if your encoder runs at 35 kbps network utilization, sending to two locations will require 70 kbps upload speed from your network.

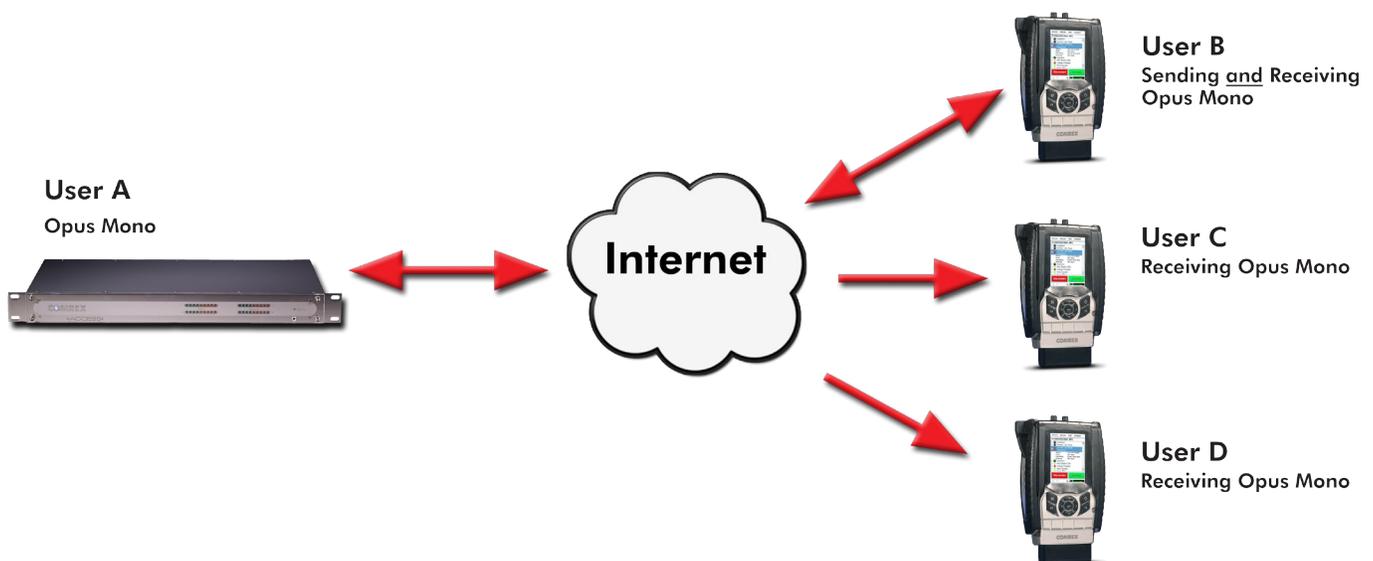
Multi-streaming should not be confused with IP Multicast, which is described in the next section.

Note: Multi-streaming is unsupported with CrossLock connections.

Each ACCESS can also run only one decoder, so it’s important that in a multi-stream environment, a maximum of one stream is sent in the reverse direction. This means that users interested in hearing a multi-stream must turn off their encoders.

This can be a bit confusing because multi-streams can be initiated from either end of the link.

Below is an ACCESS multi-stream arrangement. ACCESS A is the multi-streamer, with ACCESS B, C and D listening to the same audio. Additionally, ACCESS B is sending a stream back to ACCESS A. In order to set up a multi-stream scenario, you will need to know how to turn ACCESS encoders **Off**. This must be done by building a profile with either the **Local** or **Remote Transmitter** mode set to **Off**.



To turn the encoder off, select the profile you will be using in the **Manage Profiles** menu and select **Edit**. Under each folder, both **Local** and **Remote**, there is a **Transmit On/Off** option. By selecting this, you can then turn the transmit to off by unchecking the **On** box.



We'll give two examples of multi-streaming scenarios. The first is an environment where the ACCESS that is serving the multi-stream initiates the calls, and in the second the serving ACCESS accepts all its incoming connections.

In the "multi-streamer as caller" model, two different profiles will be built on ACCESS A. The first profile, labeled "Multi-Duplex," will be defined as a normal, full-duplex ACCESS connection. The encoder to be used will be selected in the **Local Encoder** section, and the stream desired in return will be defined in the **Remote Encoder** section.

The second profile is called "Multi-Simplex", and in this profile the **Remote Transmitter** is turned **Off**. Most other selections in this profile are irrelevant.

User A will define remote connections for ACCESS B, C, and D. He will assign the "Multi-Duplex" profile to ACCESS B, and "Multi-Simplex" profile to the others. He will then establish a connection with ACCESS B first, followed by C and D.

In model number 2, where the serving ACCESS accepts all incoming connections, all the profiles are built on the **Remote Receivers**. ACCESS B will use a simple profile by defining the encoders in each direction and assign it to ACCESS A. ACCESS C and D will each define a profile with their Local Encoders turned off. ACCESS B should connect first. When C and D connect, they will hear the same stream as B, regardless of how their remote encoders are set in their profiles.

In a multi-streaming environment, the first man wins. For example, the first connection made between units will determine the encoders used for all others. After the first full-duplex connection is made, all other attempts at full-duplex connections to either end will be rejected.

xxiii. IP MULTICAST

NOTE: This section deals with advanced topics relating to ACCESS capabilities.

IP Multicast is an efficient way of delivering ACCESS digital audio streams to multiple locations. This involves relying on the network to distribute the stream to the locations that require it, rather than creating an independent stream for each user.

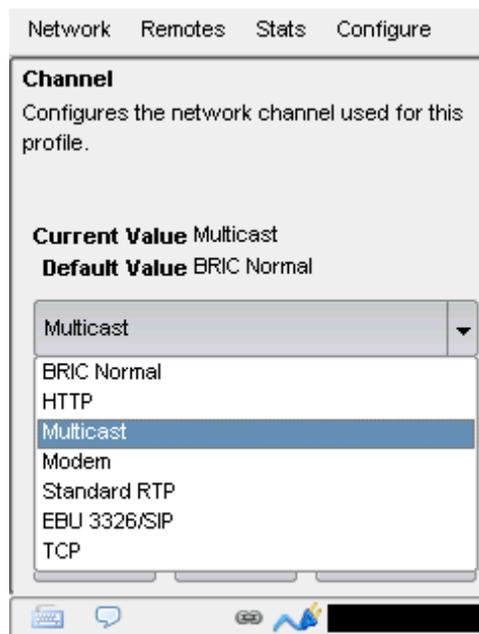
IP Multicast requires the use of an IP Multicast-capable network. The commercial Internet, with few exceptions, is not capable of supporting IP Multicast. Some private LANs and WANs are IP Multicast-capable.

IP Multicast supports only a single direction stream. An IP Multicast encoder cannot receive input streams.

In this manual, we assume that IP Multicast users will be familiar with the basic concepts of setup and operation of the network, so we will focus on how to configure ACCESS for Multicast mode.

MULTICAST PROFILES

To set any remotes to Multicast, you must first create a profile for either a Multicast Sender or a Multicast Receiver on the **Manage Profiles** tab.



When you define a new profile, you have the option to choose **Multicast** as the profile type. Multicast profiles have fewer options than other profile types, and some of the available options will have no effect.



The important settings for Multicast are:

- **Sender/Receiver** - Determines whether this particular ACCESS is designed to generate the IP Multicast stream (send) or decode one (receive).
- **Encoder Type** - Determines the type of stream to be used by the Multicast Encoder (not relevant for decoders).

In addition to the basic options for **IP Multicast** profiles, clicking the **Advanced** box will allow setting of the same **Advanced Options** available for **Normal BRIC (Unicast)** profiles.

SETTING UP A MULTICAST REMOTE

All Multicast connections are outgoing connections. A Multicast Sender must initiate an outgoing stream, and a Multicast Receiver must initiate an incoming one. These remotes are configured within a special address range known as a Multicast Block, typically 224.0.0.0 to 239.255.255.255. To establish a Multicast connection, simply define a remote as having an address within the IP Multicast Block, use an IP Multicast profile, and press **Connect**.

TIME-TO-LIVE

Time-to-Live (TTL) is a variable set by Multicast encoders to determine how long a packet is processed before it is dropped by the network. The default value of TTL in ACCESS is **0**, which limits its use to within a LAN environment. TTL may be manually changed on a Multicast Sender remote by configuring the IP address followed by a “/” (forward slash), followed by the TTL value.

As an example, a remote Multicast encoder could be set for the address **224.0.2.4/255**, which would signify an address with the Multicast Block with a TTL of **255** (which is the max value available).

CHANGING PORT NUMBERS FOR MULTICAST

The default port of UDP 9000 may also be changed on Multicast remotes. The port number is assigned in the usual way, directly after the IP address, preceded by “:”, followed by the TTL. As an example, the IP address of a Multicast Sender on port **443** with a TTL of **100** would read:

224.0.2.4:443/100

xxiv. LEGACY STATS

Prior to CrossLock's implementation, stats for connections were represented with the **Channel Stats** and **Peer Stats** menus.

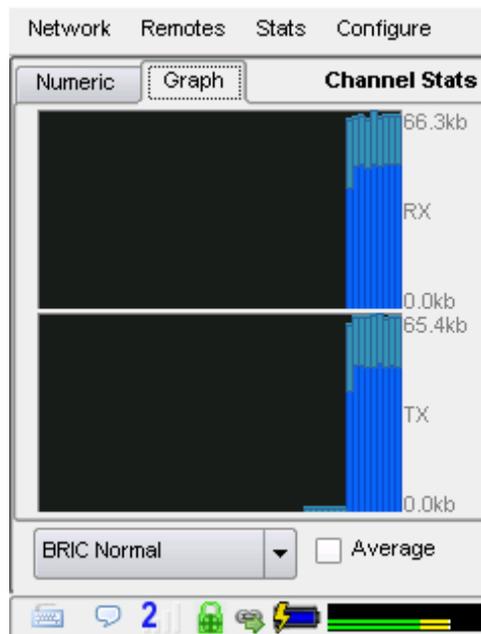
The **Peer Stats** menu and **Channel Stats** menu are considered a legacy resource to view network performance. CrossLock stats are recommended to be your source of this data.

Channel Stats provide real-time graphs of outgoing and incoming data.

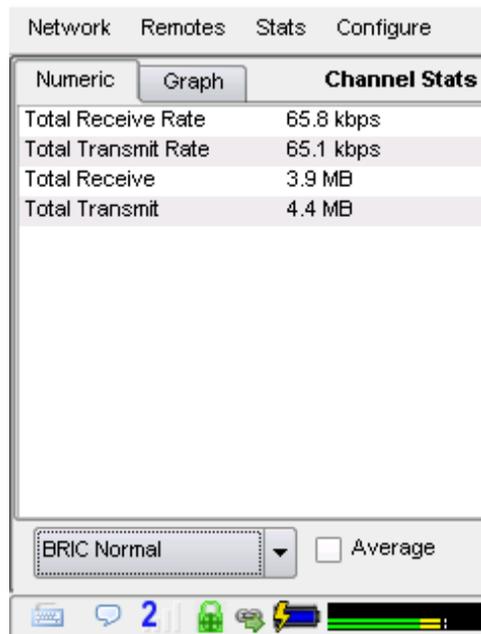
Peer Stats give detailed information regarding the decoder buffer manager's functions, such as call duration, transmit and receive delays, frame loss rates, overhead, and more.

CHANNEL STATS

The **Channel Stats Graph** tab provides real-time graphs of outgoing and incoming packets. Each column represents one second of outgoing data, segmented into audio coding data (shown in blue) and overhead, such as IP/UDP headers, RTP headers and similar data (shown in light blue).

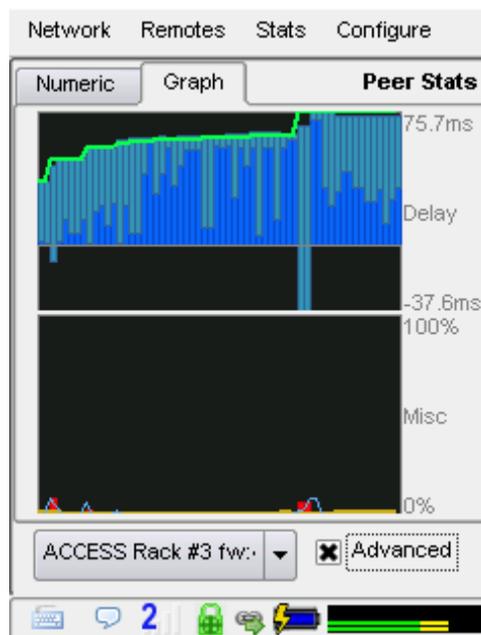


The **Numeric Channel Statistics** tab gives an indication of the same values instantaneously, as well as the total amounts of incoming and outgoing data (in bytes) for the current connection. This information can be helpful when operating on data networks with per-megabyte transfer charges. If you do not have an unlimited data plan, you may want to keep track of overall data usage and optimize your connection profile for the most efficient transfer settings. These totals reset once the connection is closed.



PEER STATS

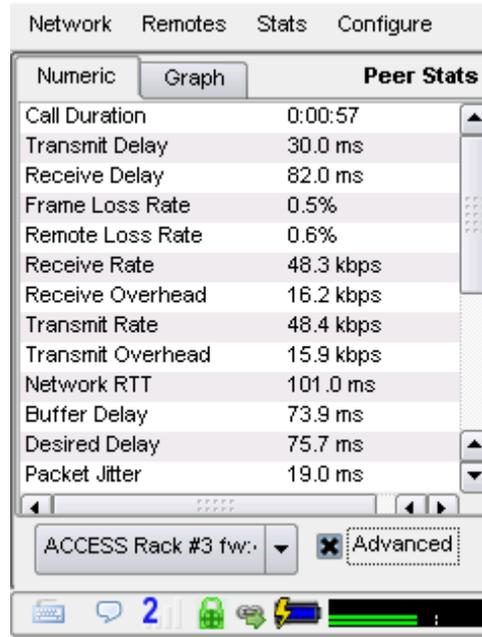
The **Peer Stats Graph** tab represents the work of the Jitter Buffer Manager. The area of most interest is the light blue area as shown below, which illustrates a spread of jitter values (referenced to the current playout pointer) over the last second. If this area covers a large span, the relative jitter is high. If the light blue section of the graph is small or invisible over a time period, there has been very little jitter present.



Based on the historical value of this jitter figure, the buffer manager will expand or contract the receive buffer (lengthening and shortening overall delay). The time interval over which this measurement is assessed is called the "jitter window", and is adjustable in the **Advanced Profile** editor.

The work of the Buffer Manager is shown by the green line, which is the target buffer delay that the system is trying to achieve, based on measurements done over the jitter window.

The lower half of the **Peer Stats** display shows a real-time and historical representation of frame loss. If the decoder does not receive packets in time, the chart will show a red line indicating percentage of lost packets over the one-second interval.



Here's a brief description of the statistics available on the **Peer Status Numeric Tab**:

- **Call Duration** - The total elapsed time of the current call.
- **Transmit / Receive Delay** - These figures are an estimation of how much delay (in milliseconds) is attributed to each end of the link. This includes coding delay and buffering, but does not include any delay caused by the network.
- **Frame Loss Rate** - The percentage of packets considered to be lost and subject to error concealment.
- **Remote Loss Rate** - The percentage packet loss reported by the decoder on the far end of the connection. This statistic is only valid when using the "BRIC normal" channel between two ACCESS units with software revision 2.3 or higher. It's updated at 5-second intervals.
- **Receive Rate** - The data rate at which frames are fed into the decoder, exclusive of protocol headers.
- **Receive Overhead** - The rate of RTP, UDP and IP protocol headers being received and stripped by the decoder.
- **Transmit Rate** - The data rate of frames being generated by the transmitter, exclusive of protocol overhead.
- **Transmit Overhead** - The rate of RTP, UDP, and IP protocol headers being added to the encoder frames.

xxv. **STREAMING SERVER FUNCTION**

ACCESS has the ability to act as a streaming server, delivering AAC and HE-AAC to compatible PC based media players. Currently tested media players include WinAmp, VLC, iTunes, Windows Media 12, and Windows Media Player with Orban/CT HE-AAC plug-in.

By default, streaming server functionality is turned off. To enable it, go to the **System Settings** tab of the user interface and choose the **HTTP Settings** option. Under the first option, set **Accept Incoming Connections** to **Enabled**.

Next you will need to choose an encoder for use by the streaming server. Only the encoder choices that are compatible with the players listed are shown in this menu. Choices span between a mono audio feed at 18 kb/s, up to a stereo feed at 128 kb/s.

Keep in mind that multiple streams will require this bandwidth along with around 25% overhead for each stream.

The **Genre**, **Info URL** and **Public** options may be set for anything, or left alone. These options, if applied, will be embedded into the stream.

DECODING A HTTP STREAM

To decode a stream, open one of the supported players and find the option to open a URL-based stream. In Winamp and VLC, input the address of the ACCESS in the following format (the address is merely made up for this example and used for demonstration only):

http://192.168.0.75:8000

(insert the real IP address, but always use port **8000**)

In Windows media, input the address like this:

http://192.168.1.75:8000/stream.asx

(using the actual IP address)

SIMULTANEOUSLY CONNECTING ACCESS AND STREAMING

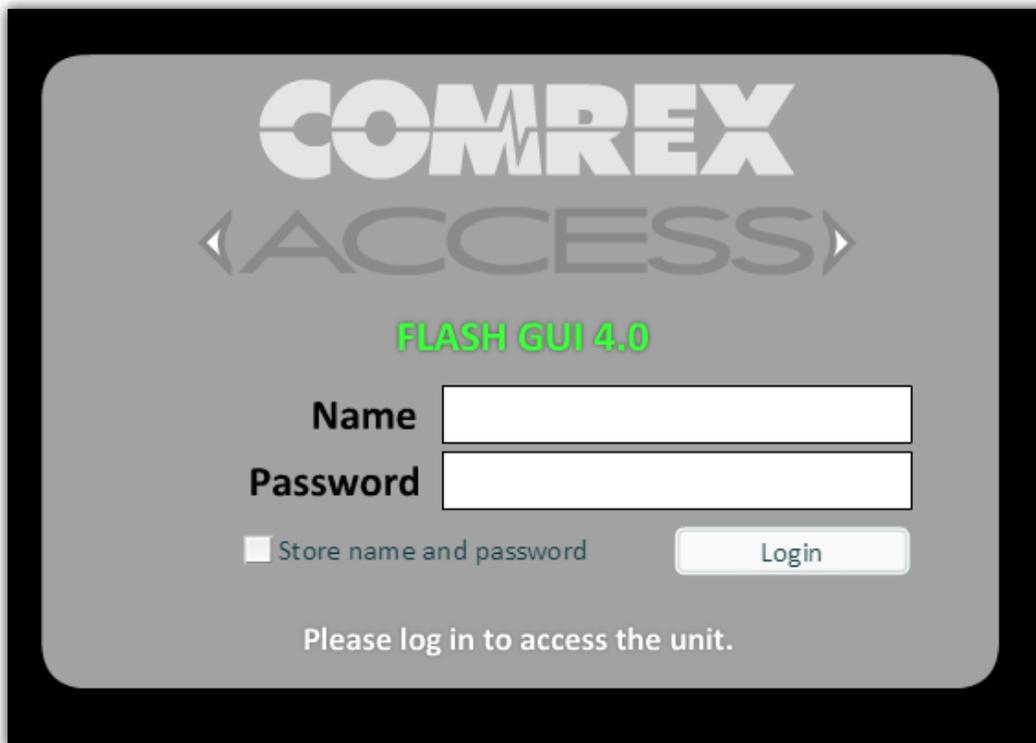
ACCESS can stream while connected to another ACCESS in normal mode. If the BRIC connection is using an AAC algorithm supported by players, when a stream is requested it will be delivered using the same encoder as the BRIC connection, regardless of the HTTP settings. If the ACCESS encoder is Linear or FLAC, the stream request will be rejected.

xxvi. WEB-BASED INTERFACE INTRODUCTION

Besides using the touchscreen, ACCESS may be configured and controlled remotely via the Web-based Interface. Once your IP settings are configured and ACCESS has cleanly booted on your LAN, you will have access to the Web-based Interface. **Note:** ACCESS 2USB does NOT support HTML5.

To use the Web-based Interface, open a Flash-enabled web browser on a computer that is on the same physical IP network (LAN) as the ACCESS unit and input the IP address of the ACCESS.

Once you are connected to ACCESS, a login screen will appear. Type in any username along with the default password, **comrex**.



COMREX
ACCESS
FLASH GUI 4.0

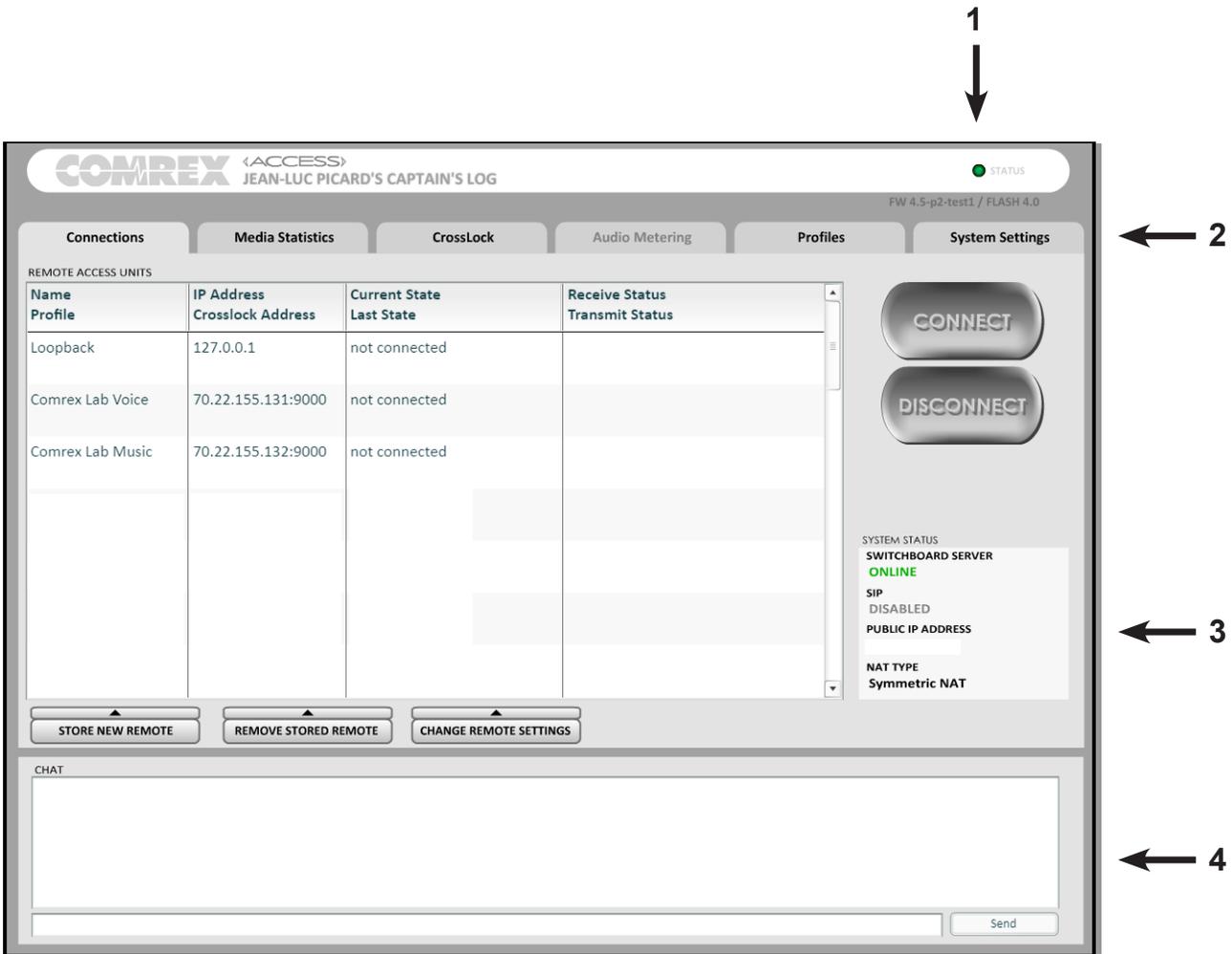
Name
Password

Store name and password

Please log in to access the unit.

Tech Tip: You can also access the Web-based Interface from a browser on a computer that is not on the same LAN when you forward port TCP 80 to the ACCESS. Consult with your IT department for assistance with that.

There are three main parts to the ACCESS Web-based Interface screen:



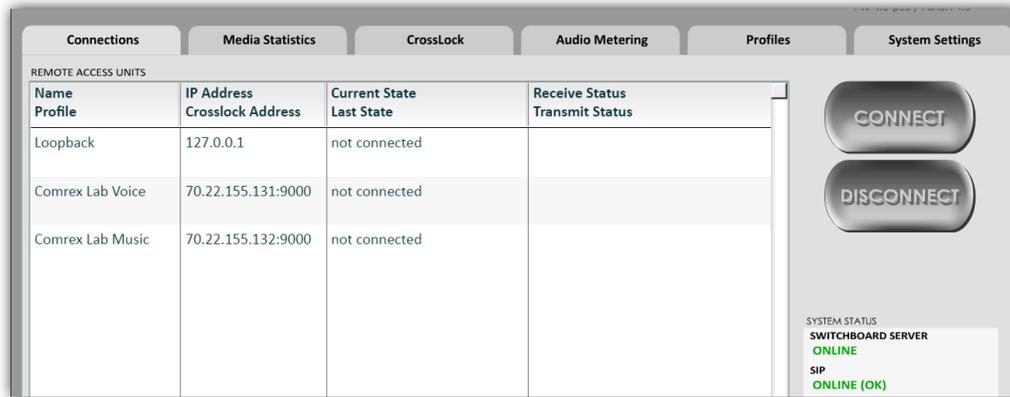
- 1 **Status Indicator** - The Status Indicator shows whether the Comrex ACCESS is actively engaged in a connection. When the unit is connected to a remote, the Status Indicator will turn bright green.
- 2 **Tabs** - Use these tabs to control and obtain status of ACCESS. They are described in detail in the next sections.
- 3 **Registration Status** - This window provides various network information and status, including Switchboard TS status (if licensed), SIP registration status, the unit's public IP address and NAT type.
- 4 **Chat Window** - Allows for a chat utility between any users who are logged into that particular ACCESS web interface. In addition, when ACCESS is connected to a remote user, chat text will appear from any users logged into the remote web interface.

Note: The **Audio Metering** tab is not supported for ACCESS 2USB, but is available when interfacing with an ACCESS Rackmount.

xxvii. WEB-BASED INTERFACE CONNECTIONS MENU

CONNECTIONS TAB

The **Connections** tab is the first screen to appear when the system is turned on. The **Connections** tab is like a “phonebook” for your ACCESS. It allows you to define and edit your outgoing connections, and also indicates when there are incoming connections.



Name Profile	IP Address Crosslock Address	Current State Last State	Receive Status Transmit Status
Loopback	127.0.0.1	not connected	
Comrex Lab Voice	70.22.155.131:9000	not connected	
Comrex Lab Music	70.22.155.132:9000	not connected	

CONNECT
DISCONNECT

SYSTEM STATUS
SWITCHBOARD SERVER
ONLINE
SIP
ONLINE (OK)

TEST REMOTE ENTRIES

By default, three remotes are already present on the **Connections** tab, and can be used immediately for testing.

Loopback is a testing mode for estimating quality and best case delay, in which a single ACCESS encodes and decodes the same audio in a loopback configuration (the send and receive portions are connected together).

Comrex Lab Voice and **Comrex Lab Music** are codecs you can connect to for testing your unit. These test lines are located at the Comrex headquarters in Devens, Massachusetts.

REMOTES LISTED FROM SWITCHBOARD

Switchboard is a free service that Comrex provides. If you do not have an account set up with us, please contact us at techies@comrex.com or 978.764.1776 / 1.800.237.1776. To learn more about Switchboard and why you should be using it, visit the section **Switchboard Traversal Server (TS) on page 59**.

Comrex highly recommends that you utilize our Switchboard server in conjunction with your audio codecs. When your audio codecs have been added to your Switchboard account and placed in a contact list, those codecs will populate automatically in the device’s Remotes list once it is powered up and registered with Switchboard. This makes connections for broadcasts quick and easy.

Name Profile	IP Address Crosslock Address	Current State Last State	Receive Status Transmit Status
Loopback	127.0.0.1	not connected	
Comrex Lab Voice	70.22.155.131:9000	not connected (Local disconnect)	
Comrex Lab Music	70.22.155.132:9000	not connected	
2usb NR	74.94.151.157:60176 00:01:c0:1b:34:68	not connected	
Conference Room ACCESS	74.94.151.157:9000 00:40:63:ef:5d:3b	not connected	

CONNECT
DISCONNECT

SYSTEM STATUS
SWITCHBOARD SERVER
ONLINE
SIP
ONLINE (OK)

Units that are added from your Switchboard contact list will show up in the Remotes list with a grey background, as shown above.

CONNECTING AND DISCONNECTING TO REMOTES

To connect and disconnect remotes, select the device in the Remotes list and select the **Connect** button to establish a connection, or the **Disconnect** button to disconnect the connection.

Incoming connections are displayed by their IP address, or, if also configured as outgoing connections, by their names. Incoming POTS connections are displayed as “incoming”.

ADD NEW REMOTE

Although using Switchboard to generate your remotes is the preferred method, you can also add remotes manually and input the information needed to make a connection.

To add a new remote, click on the **Store New Remote** button in the bottom left.

The following menu appears.

You will need to input a name for this remote (which can be anything), as well as the destination IP address (or dial-up phone number for a POTS call).

Next, you must decide if you intend to use CrossLock for the connection. Comrex recommends the use of CrossLock for most connections, because the VPN (Virtual Private Network) created by CrossLock increases connection reliability in most circumstances. Unless you know of a specific reason that your setup might not support CrossLock, we suggest enabling it.

CrossLock connections that don't use Switchboard can be complex to set up. This is because the hardware on each end must know the Switchboard ID (MAC address) of the other for security purposes.

If you want to use CrossLock, check the **Use CrossLock to Connect** box and put the Switchboard ID (MAC address) of the unit you are going to connect to. Note that the codec being connected to must have a corresponding entry with this unit's Switchboard ID (MAC address).

If you do not want to use CrossLock, you can leave the box unchecked and the Switchboard ID (**MAC address**) entry blank.

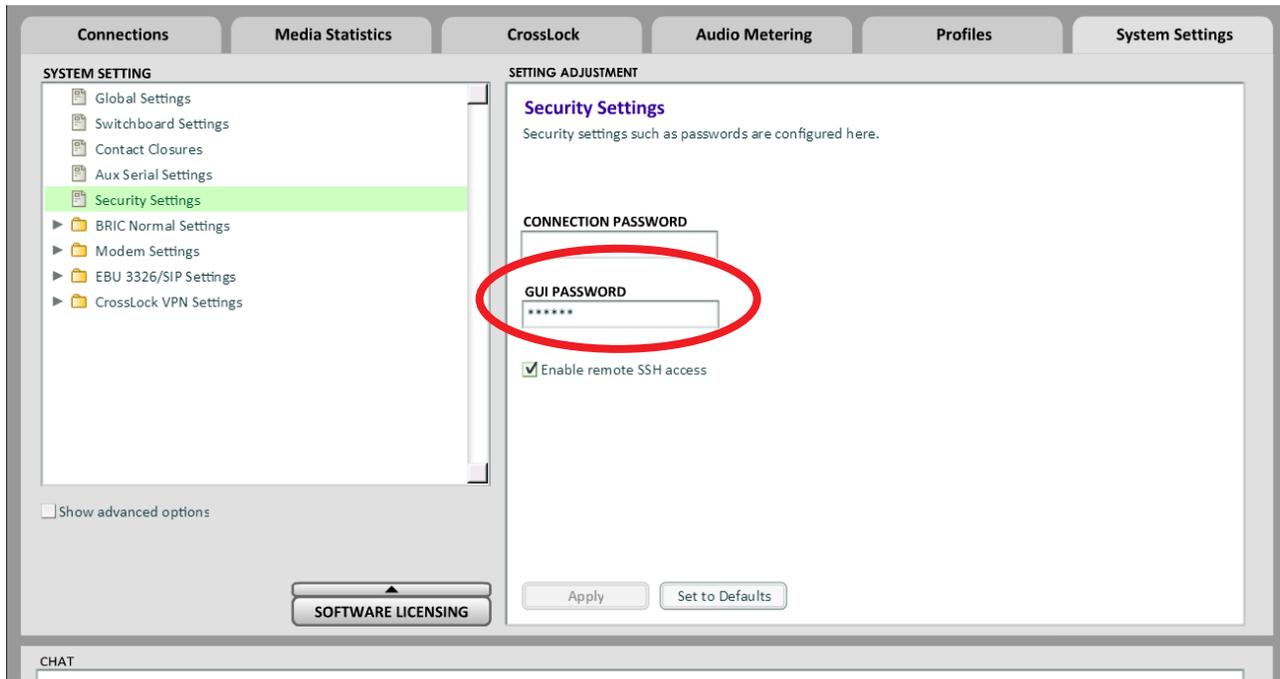
Next, you need to choose a profile to use when making these connections. ACCESS includes several default profiles to choose from, each of which enable a simple full-duplex link using one of the available algorithms.

Name	IP Address	Current
		Last
CHANGE REMOTE SETTINGS		
REMOTE NAME		
Ground Control to Major Tom		
IP ADDRESS OR PHONE NUMBER		
192.168.1.119		
<input type="checkbox"/> Use Crosslock to Connect		
SWITCHBOARD ID		
CONNECTION PASSWORD		
PROFILE		
(Default Profile)		
(Default Profile)		
3 sec timeout AAC Mono		
5 sec timeout OPUS Mono		
0 sec timeout OPUS Mono		
1 sec timeout OPUS Mono		
STORE NEW REMOTE		REMOVE STORED REMOTE

If you wish for a more complex feature set when making this connection, you will need to navigate to the **Profiles** tab and set up a specific profile using your custom parameters. To learn about creating Profiles, visit the section **Profiles Menu on page 44**.

Once defined in the **Profiles** section, the new profile will be available in the **Profile Select** window and can be assigned to a remote connection.

Optionally, you may add a password to this outgoing remote for connection authentication. In this case, the incoming ACCESS must also be programmed with the matching incoming password, which is assignable under the **System Settings** tab under **Security**.



Finally, you may specify how the unit is to behave when connection is lost to this remote.

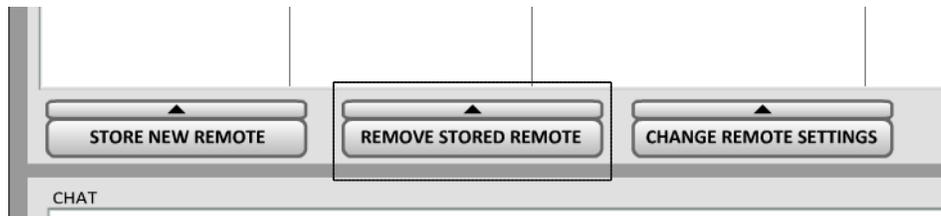
EDIT REMOTES

Existing remotes may be edited by highlighting a remote from the list and selecting **Change Remote Settings**.

Tip: CrossLock Switchboard IDs (MAC Addresses) can not be edited—the remote entry must be deleted and recreated to edit outgoing CrossLock info.

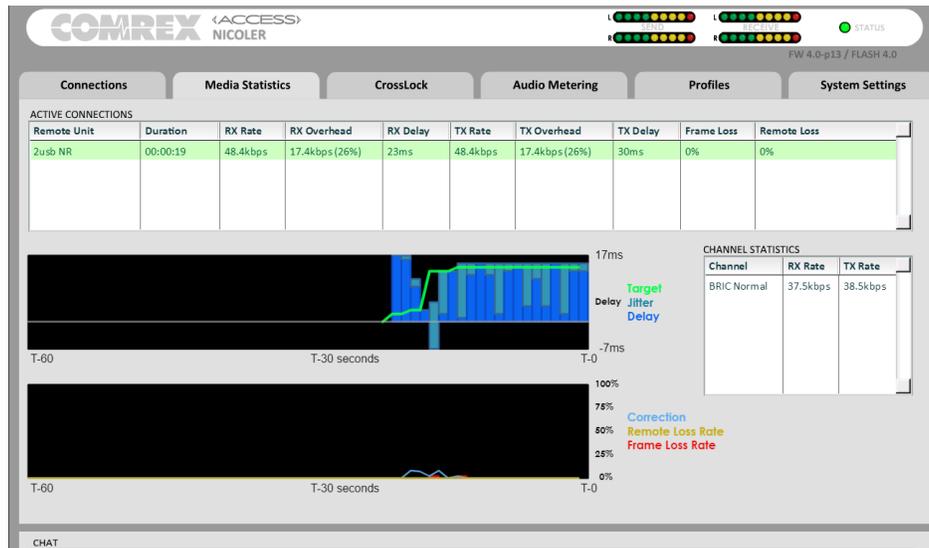
DELETE REMOTES

Remotes can be deleted by highlighting a remote from the list and selecting **Remove Stored Remote**.



XXVIII. WEB-BASED INTERFACE STATISTICS MENUS

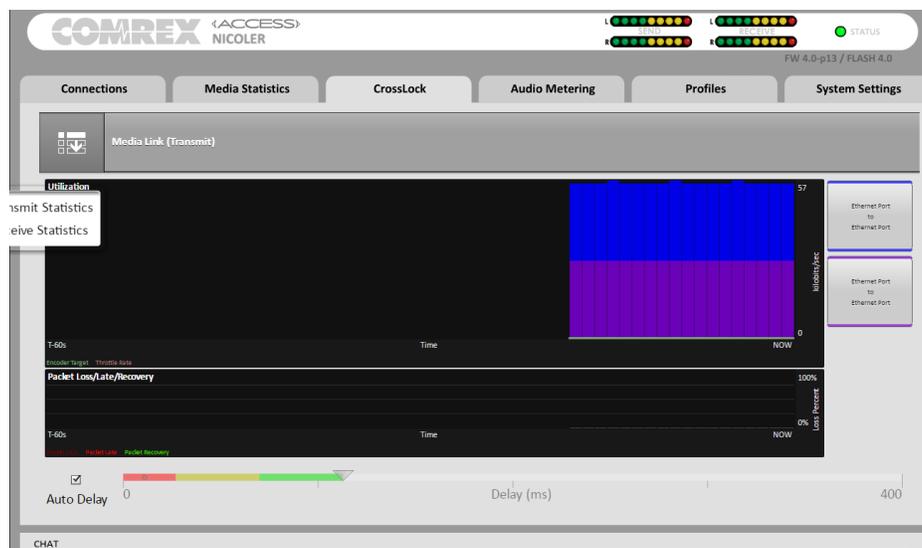
The **Media Statistics** tab will show graphical and numerical representations of the network performance for both the local and remote codecs. It also includes information regarding the decoder buffer manager's functions, such as call duration, transmit and receive delays, frame loss rates, overhead, and more.



These stats are considered a legacy resource to view network performance. The **CrossLock** statistics available on the **CrossLock** tab is recommended to be your source for this data. These stats are considered superior to the **Media Statistics**, and should be used when monitoring network performance.

CrossLock Stats allows you to see CrossLock in action. You can determine how many networks are being utilized, the delay associated with both ends of the connection, loss and recovery of packets, and more.

For details on CrossLock and the **CrossLock Stats**, visit the section **CrossLock Details** on page 73.



XXIX. WEB-BASED INTERFACE PROFILES MENU

Profiles are what define the behavior and type of connection for your codecs in both directions. Profiles are separate from remotes, which define the address to connect with.

ACCESS has many options to optimize connections based on your broadcasting needs (the number of locations you broadcast to, the diversity of connections you use, network availability, etc.). Your specific needs will dictate how simple or intricate your profile and remote settings will be. ACCESS comes with a series of profiles that are optimized for the majority of IP and POTS connections. Many users may never need to define their own profiles.

When using ACCESS, the point where the connection originates controls all available connection parameters in both directions. Keep in mind that these profiles are useful only for connections initiated from the local ACCESS. Incoming connections are defined by the ACCESS at the other end.

VIEWING PROFILE DETAILS

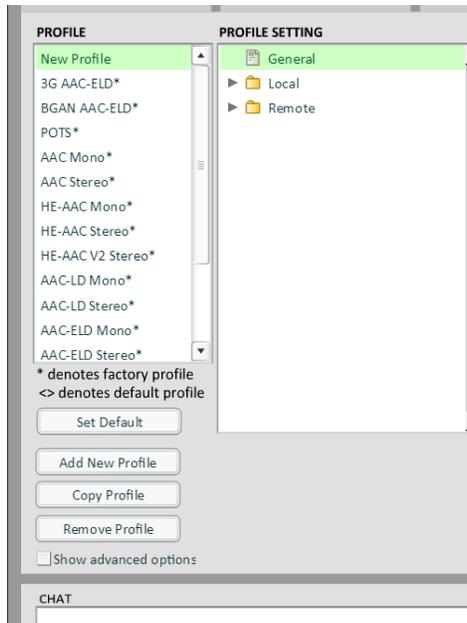
To view the parameters set for a profile, select the profile in the **PROFILE** list on the left. The main options under **PROFILE SETTING** are **General**, **Local**, and **Remote**.

The screenshot displays the web-based interface for COMREX ACCESS NICOLER. At the top, there are status indicators for SEND and RECEIVE (L and R) and a STATUS indicator. Below the header, there are tabs for Connections, Media Statistics, CrossLock, Audio Metering, Profiles, and System Settings. The main content area is divided into three sections: PROFILE, PROFILE SETTING, and SETTING ADJUSTMENT. The PROFILE list on the left includes various codec profiles such as 3G AAC-ELD*, BGAN AAC-ELD*, POTS*, AAC Mono*, AAC Stereo*, HE-AAC Mono*, HE-AAC Stereo*, HE-AAC V2 Stereo*, AAC-LD Mono*, AAC-LD Stereo*, AAC-ELD Mono*, and AAC-ELD Stereo*. The PROFILE SETTING section is currently set to General, which includes sub-options for Local and Remote. The SETTING ADJUSTMENT section shows the General Profile Settings, including fields for PROFILE NAME (New Profile) and CHANNEL (BRIC Normal). There are buttons for Set Default, Add New Profile, Copy Profile, Remove Profile, Apply, and Set to Defaults. A chat window is visible at the bottom.

General is where you can name the profile and choose the channel type. **BRIC Normal** is the standard IP-based channel connection. The other options are considered advanced and will be explained in later sections. You'll use the **Local Settings** to determine how your ACCESS behaves, and the **Remote Settings** will determine how the ACCESS on the far end behaves.

EDITING AND ADDING PROFILES

Custom profiles are easy to create on ACCESS. You can create one from scratch by selecting **Add New** on the **Profiles** tab, or copy an existing profile using the **Copy Profile** button.



TIP: You cannot edit factory profiles. Comrex recommends that when creating a new profile, you copy a factory profile that is close to what you would like the settings to be, and edit that copied profile.

Profile creation is segmented into commonly used and advanced options. In order to simplify the interface, **Advanced Options** are normally hidden from the user. Once a profile is defined, it will be available from the **Profile** drop-down menu.

To build a new profile, select **Add New** and a new profile appears on the list labelled **New Profile**.

Select it and press **Edit**, and you'll see a list of options.

IMPORTANT: Building a profile doesn't change how any remotes connect until that profile is assigned to a remote.

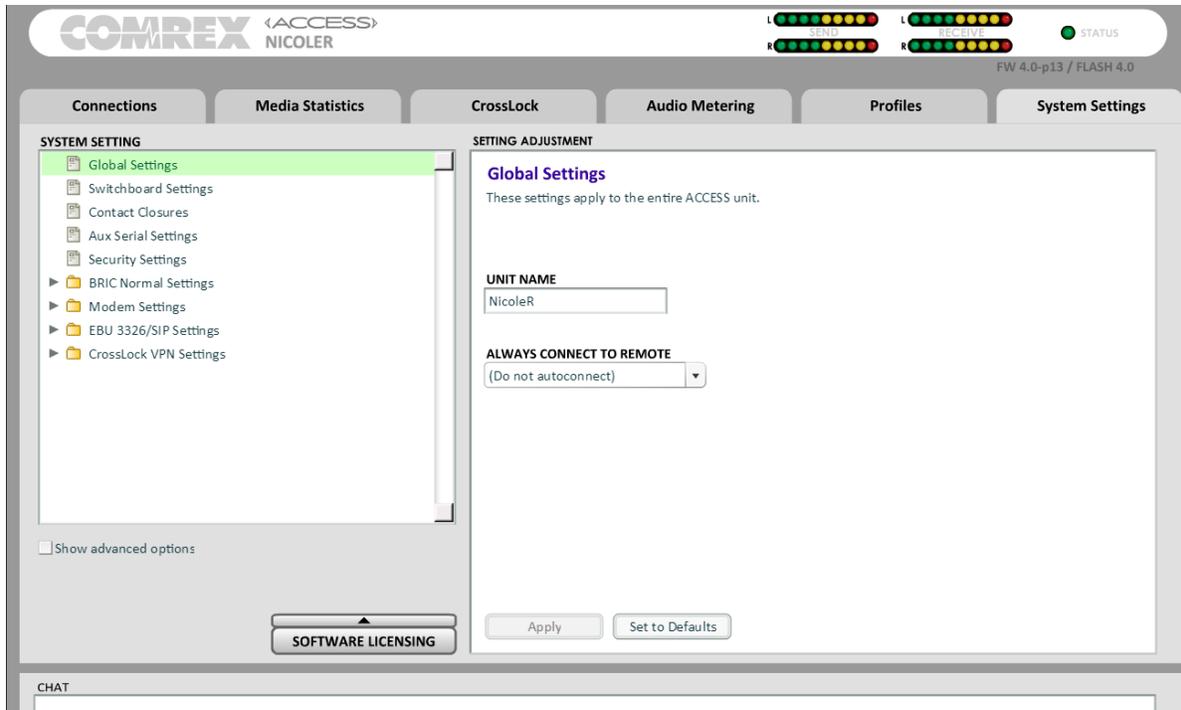
DEFAULT PROFILE

When a new remote is created, a default profile is assigned unless a different profile is selected from the drop-down menu under **Profile**. The default profile, when shipped from the factory, uses an OPUS algorithm.

TIP: You can change the default profile by navigating to **Configure->Manage Profiles**, highlighting the desired profile, and pressing the **Set Default** button. This profile will be used on all new remotes unless a different one is selected in the **Create New Remote** screen. The default profile shows an asterisk (*) next to it in the Profiles list.

System Settings define parameters that are not specific to a particular remote connection. Examples are how incoming (POTS and IP) calls are handled, global modem settings, and how the contact closures are assigned. Basic options are shown by default. Less used options are hidden until the **Advanced** box is checked. To learn more about advanced settings, visit the section **Advanced Settings on page 130**.

GLOBAL SETTINGS

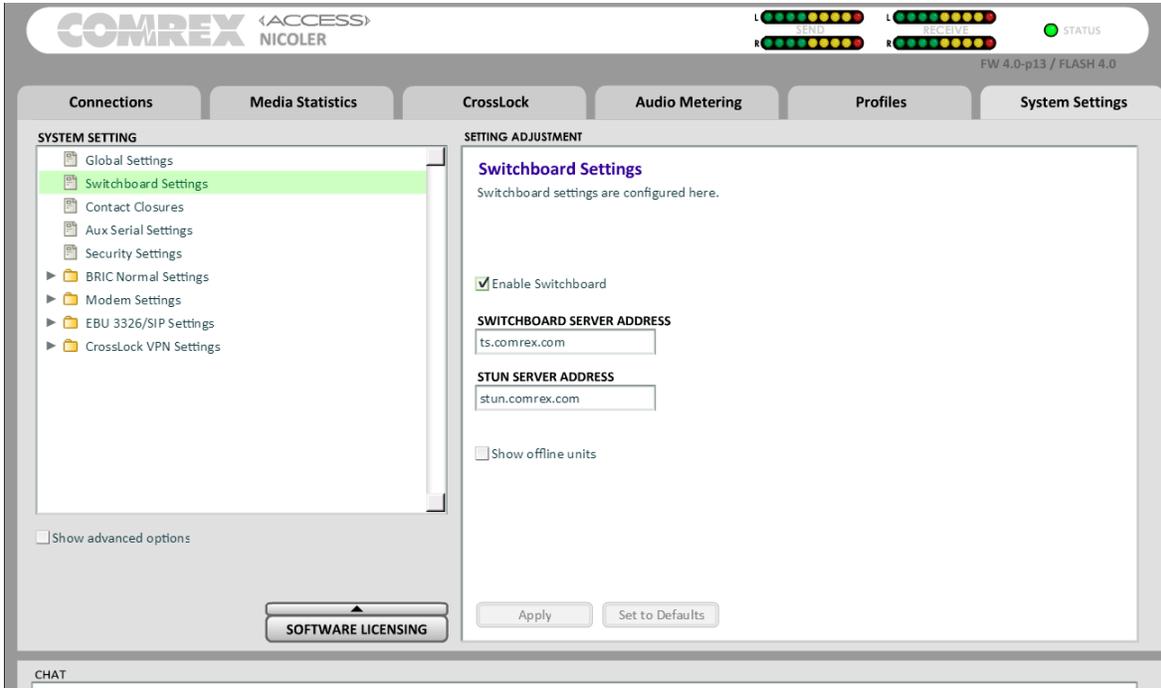


Unit Name - Users are encouraged to name their codecs here. The default name of a codec is the unique MAC address (Switchboard ID) of the Ethernet port. When this is changed to something familiar and unique (such as “Roving reporter”, “Weather guy”, etc.), the new name is reflected in several places:

- In the browser used to show the remote control page;
- In Comrex-provided utility software such as **Device Manager**;
- In Switchboard Contact Lists.

Always Connect to Remote - This setting is available to designate a remote for “always-on” operation. This is useful in environments where a signal is required to be on 24 hours a day. To assign an “always-on” remote, pull down the menu and select which remote to designate as “always-on”. A connection will be made and sustained to the chosen remote. To learn more, go to the section **Operating ACCESS IN A 24/7 Environment on page 88**.

SWITCHBOARD SERVER



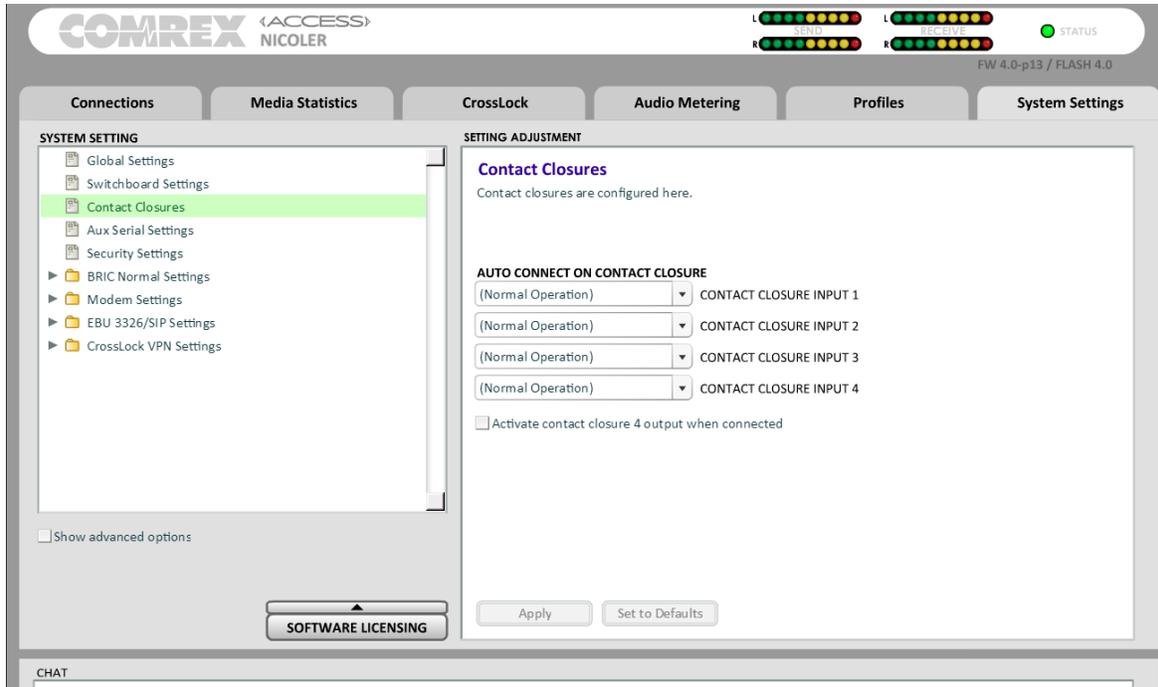
Enable Switchboard - Allows the use of the Switchboard Server to connect to remotes.

Switchboard Server Address - Shows the IP address of Switchboard.

Stun Server Address - Enables the unit to contact the STUN server maintained by Comrex to learn what its public IP address is.

Show Offline Units - When enabled, offline remotes will be shown in the **Remotes** list.

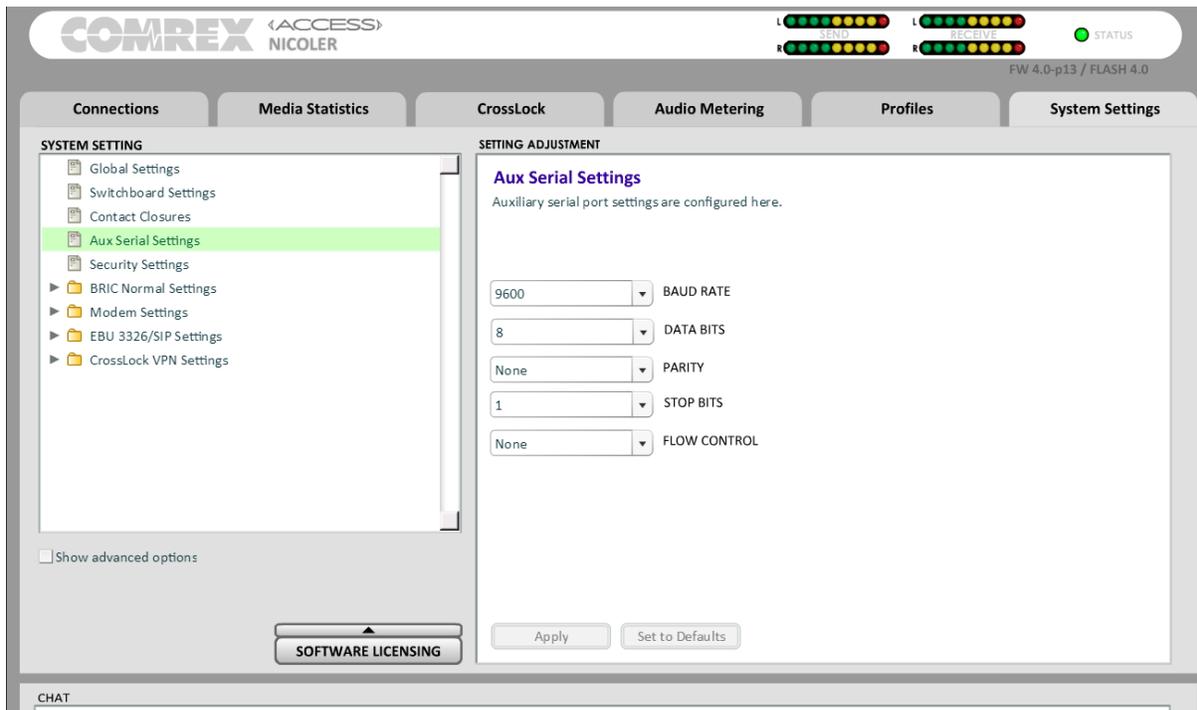
CONTACT CLOSURES SETTINGS



Connect on CC (1,2,3,4) - These choices define auto connect rules for remotes to be triggered by the four external input triggers available. NOTE: These inputs are shared with the end-to-end contact closure signals, so if a remote is designated as **Auto Connect** on a closure, that closure signal is not available for use in the direction from this ACCESS. To assign a remote connection to a contact closure, pull down the menu box next to the desired closure and select the proper remote. A connection attempt will be made whenever the contact is triggered, and will disconnect whenever the contact is released. (You can also assign the **F2** key to trigger **Contact Closure #1** at the remote codec.)

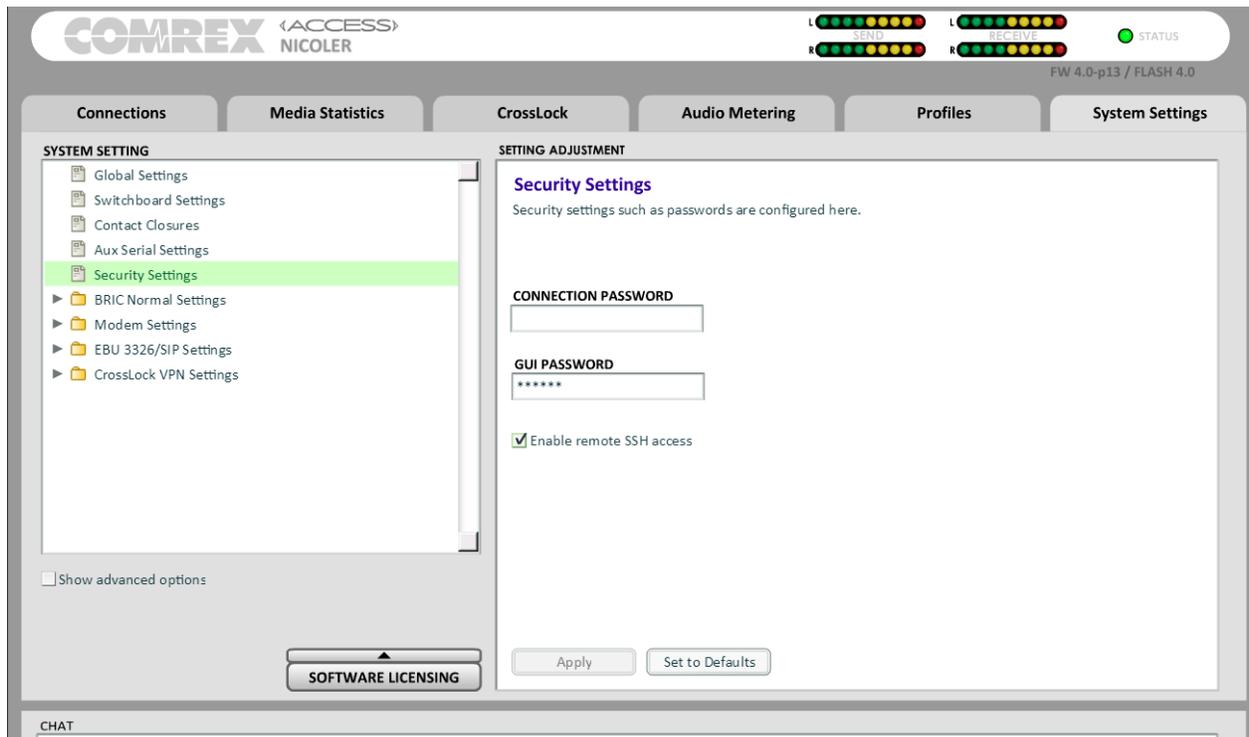
Activate contact closure 4 output when connected - Under normal circumstances, the contact will close when commanded by the other end of the connection. If this option is enabled, that function is no longer available. This contact will be closed when a valid connection is present, and open when no connection is present.

AUX SERIAL SETTINGS



This allows you to set the parameters of the auxiliary serial data port. This port is always active during an IP connection and allows serial data transfer along the same path used for the audio data. It does not remove any audio data; the serial data is added to the packets and bandwidth is increased to support the additional data. For this reason, heavy use of serial data can affect overall codec performance. Settings are available for **Baud Rate**, **Data Bits**, **Stop Bits**, **Flow Control**, and **Parity**. Most users will leave the defaults of **9600**, **8**, **1**, **No Flow Control**, and **No Parity**.

SECURITY SETTINGS



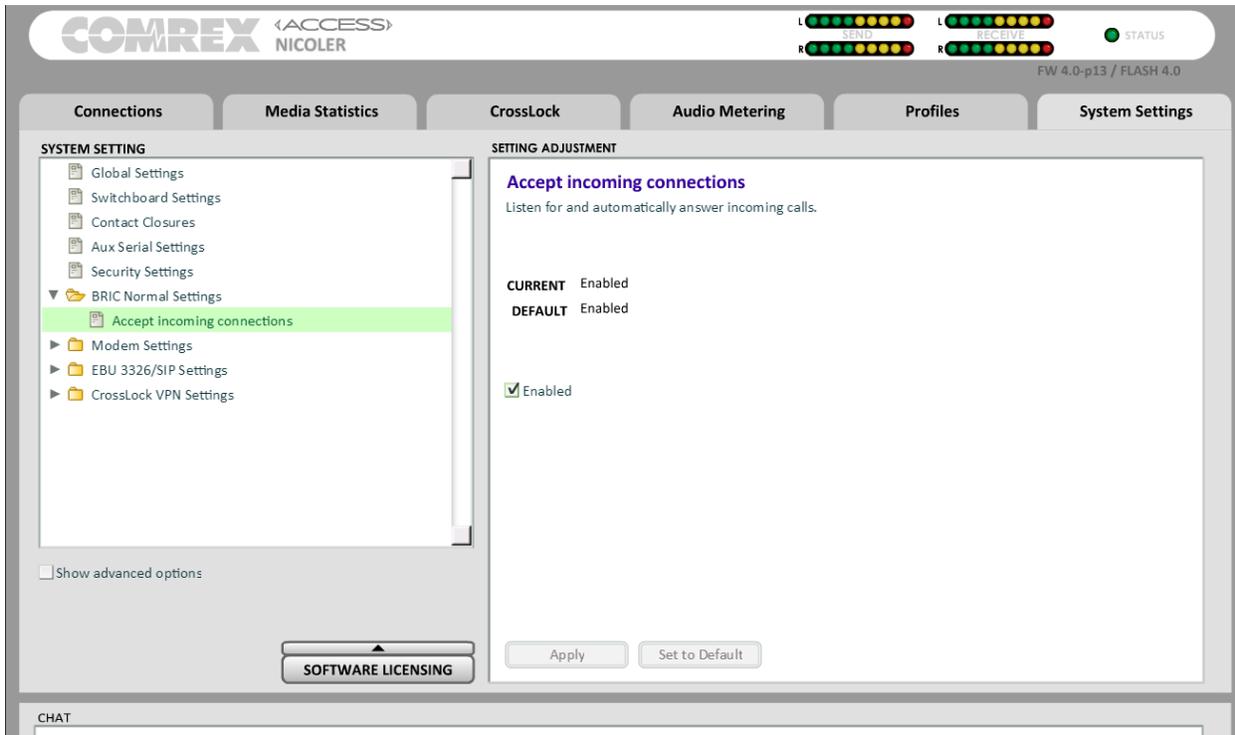
Connection Password - Allows you to define a password that must be attached to all incoming connections before they are accepted. Units contacting you must know this password and apply it to their outgoing stream, or the connection will not be completed. Leaving the field blank will disable this function.

GUI Password - Allows you to define a password for the webpage login screen and firmware updater. The default password is **comrex** (lowercase).

Enable remote SSH access - Enables Comrex support to connect to this unit using the SSH protocol for troubleshooting purposes. We recommend leaving this option enabled. Since SSH access requires a key value that is not disclosed by Comrex, generic SSH requests are rejected.

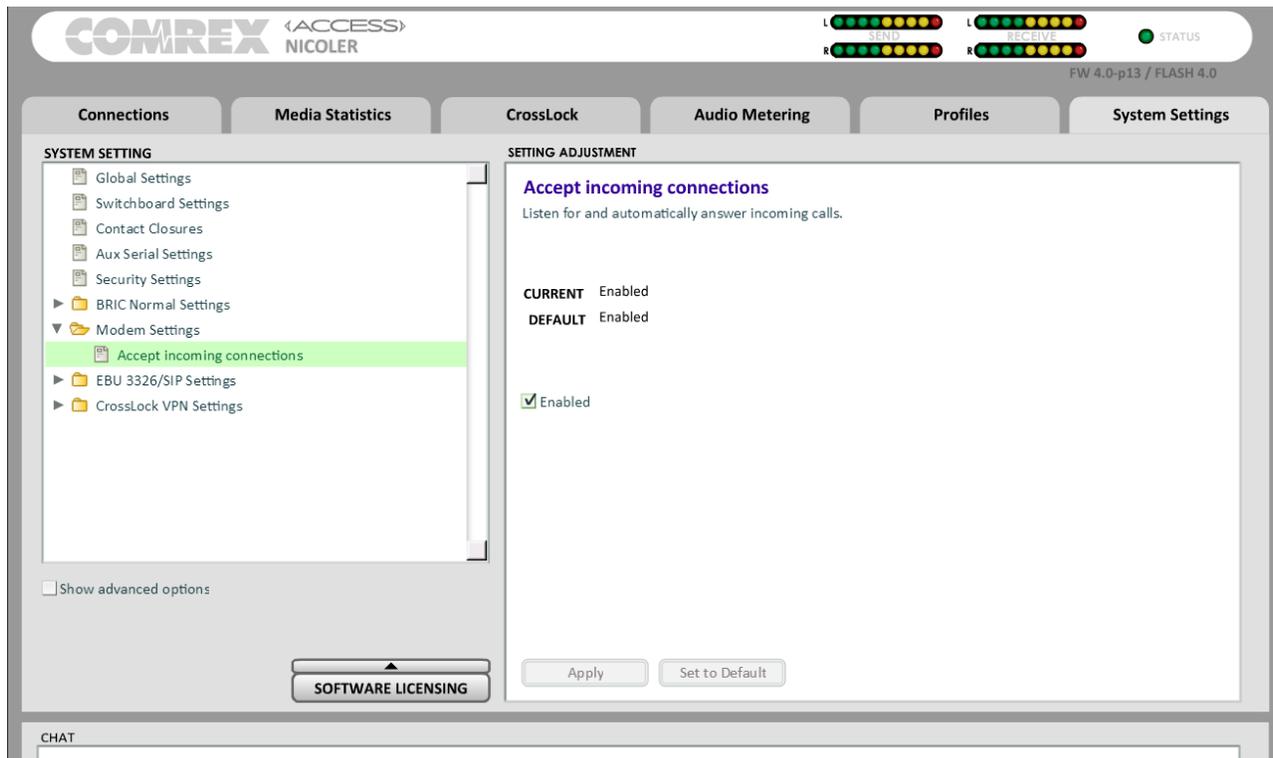
BRIC NORMAL SETTINGS

The default way ACCESS codecs connect between each other is called BRIC normal. The options in this section define if and how these connections are completed.



Accept Incoming Connections - This determines if this ACCESS is to be used for incoming normal IP connections. If this function is not enabled, ACCESS will only support outgoing calls using BRIC Normal Mode.

MODEM SETTINGS



Accept incoming connections - POTS calls must be answered automatically on ACCESS. If this option is disabled, no POTS calls will be answered and only outgoing POTS connections can be made.

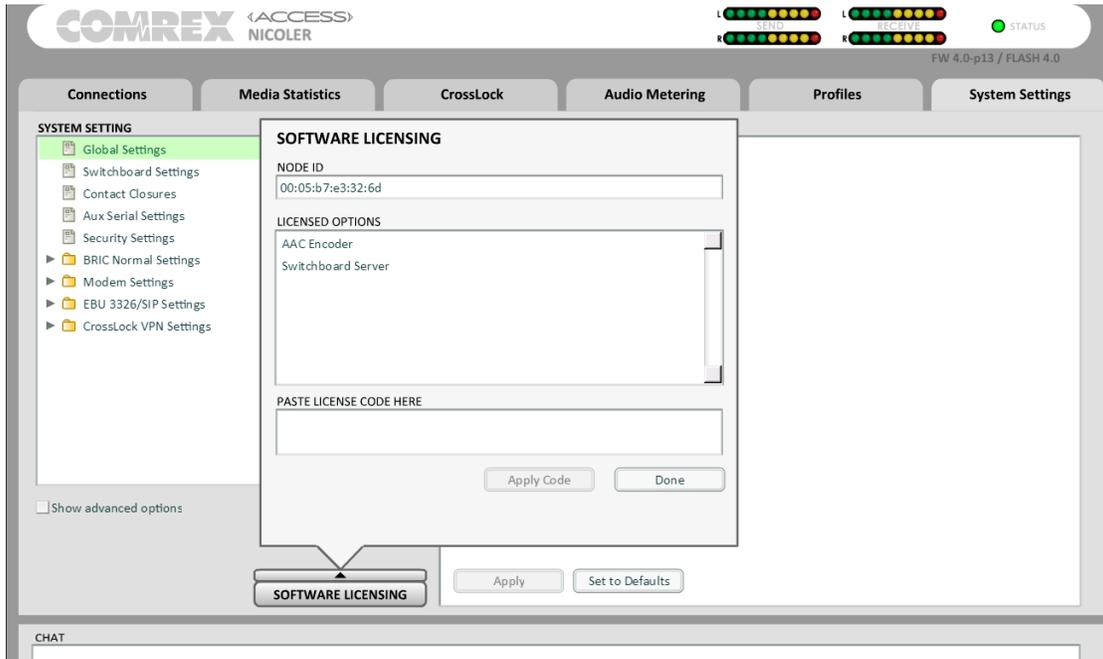
EBU 3326/SIP SETTINGS

This is an advanced topic and is covered in the section **Making EBU 3326/SIP Compatible Connections on page 91.**

CROSSLOCK VPN SETTINGS

This is an advanced topic and is covered in the section **CrossLock Details on page 73.**

SOFTWARE LICENSING



The Software Licensing button shows you which licenses are currently active to your unit. This is also where you can add licenses.

xxxI. GATEWAY OPERATION

ABOUT GATEWAY OPERATION

ACCESS includes a special operational mode that allows it to share a network connection with other devices. This can be valuable when a single wireless device is available, but email and internet access are required in addition to codec use. ACCESS will create and maintain the main network channel, then act as a router over a second network port to deliver data to an external device.

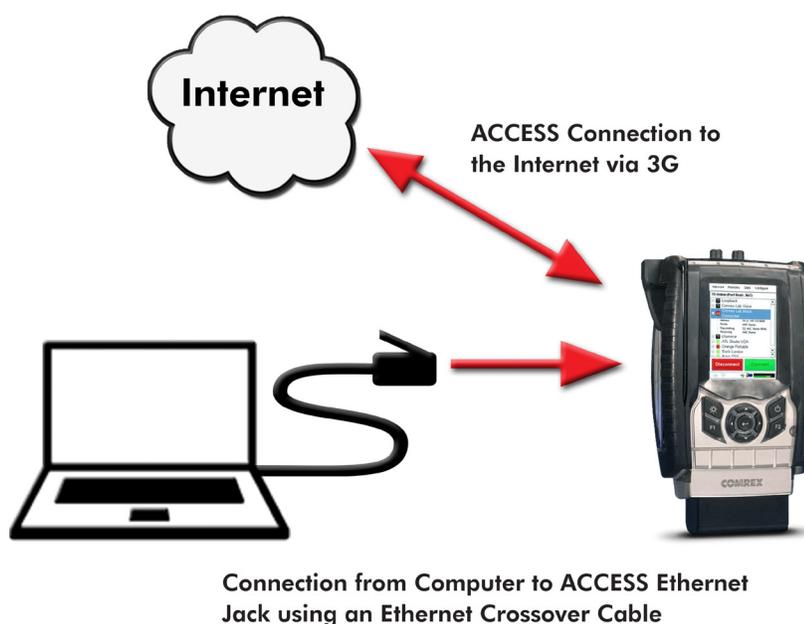
ACCESS codec packets contain real-time headers, and ACCESS will deliver these to the network ahead of other user information. In this way, ACCESS will assure that outgoing user data will not affect outgoing codec packets.

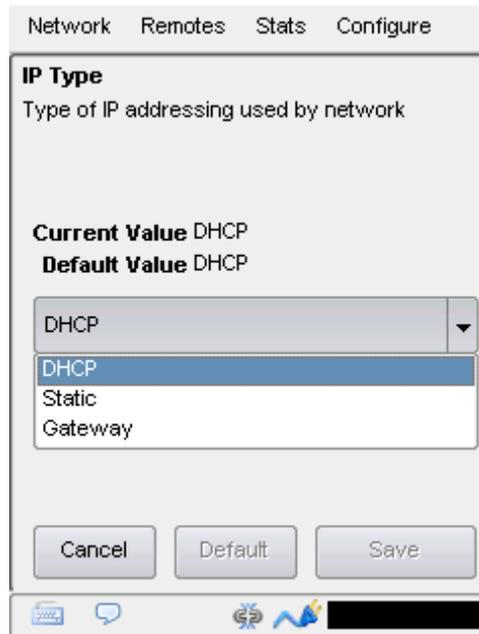
On the return channel, priority of audio codec packets vs. user packets are determined by the ISP, so heavy user data may have an effect on decoder performance.

CONNECTING AS A GATEWAY

Under most circumstances, ACCESS will be sharing a network attached to its USB jacks, and distributing data to other users via Ethernet. In this configuration, you will need an Ethernet switch between ACCESS and the computers getting the data. Alternately, if only one computer will be connected, an Ethernet crossover cable may be used between ACCESS and the computer.

As shown below, ACCESS is using a 3G adapter to connect to the internet and using its Ethernet port to share 3G data with a laptop computer via a crossover cable.





GATEWAY SETUP

Gateway Mode involves having two networks active and enabled on ACCESS: the internet side (usually a USB-based network), which is used to connect to the world at large; and the shared side (usually Ethernet), which is used to connect with other computers.

The only step to Gateway Mode is setting up your shared network side with the factory default static IP address, network mask and DHCP pool information. Navigate to **Network->Manage Networks**. Select the **Ethernet Port** from the list, select the **Configure** button and then go to the **Locations** tab. Create a new location by selecting the **Add** button, or edit the default location. Select **IP Type**, press the **Edit** button and select **Gateway** from the dropdown menu.

In Gateway Mode, ACCESS is acting as a DHCP server and router to the other devices. It will assign a dynamic address to all devices connected to it on the LAN. The static address assigned to the ACCESS ethernet port is 192.168.42.1. The pool of addresses assigned by the DHCP server is 192.168.42.128 - 192.168.42.192.

xxxii. **ADVANCED 3G/4G NETWORK SETTINGS**

3G/4G modems vary in their interface. Comrex is constantly updating drivers to work with the most popular devices. Please contact us for information about specific devices. We also keep an updated status page in the ACCESS Support section on our website.

If a device has driver support, it will appear as a WWAN Device. Select the icon for the device and click Configure.

Fields are available to fill in an outgoing phone number, a username, a password, and a modem init string. In many cases, ACCESS is programmed to extract this information from the device and fill in these blanks automatically. Otherwise, you will need to consult our website to determine which fields should be filled in for each device.

Once the proper information is entered and the device is enabled, it should deliver an IP address within 60 seconds. If no IP address is obtained, the device will not function.

When using 3G adapters based on GSM standards (non-EVDO devices), you may or may not need to apply an APN (Access Point Name) in order to establish connections and get an IP address. When using 3G adapters and USB dongles in Windows laptops, this information is usually automatically supplied by the device manager software. In the ACCESS Linux environment, this information may need to be manually entered.

The best possible way to get accurate APN information is to obtain it from the tech support at your 3G carrier. This, however, is not always possible or accurate, so ACCESS has provided the most commonly used APNs available in a pull-down list. If you select your region of the world followed by your country, a list of suggested APNs can be chosen by carrier.

This list is merely suggestions and many have not been verified. It's important, if having connection issues, to verify the accuracy of the APN with your carrier.

xxxiii. POTS (PLAIN OLD TELEPHONE SERVICE) CODEC CONNECTIONS

ACCESS is capable of connections over analog telephone lines with a modem. This mode emulates the function of Comrex POTS codecs, which have been used for years to deliver high quality audio over normal, analog dial-up telephone lines. This mode provides for a point-to-point connection between the codecs. No internet access is used, and the call is placed directly from one ACCESS (or legacy codec) to the other. A POTS Zoom modem is included with your ACCESS 2USB.

In the current firmware, ACCESS is capable of connecting over dial-up phone lines to ACCESS Codecs, Comrex Matrix Codecs, Comrex BlueBox Codecs, and Comrex Vector Codecs. **Note: Backward compatibility to Hotline codecs is not supported.**

POTS CODEC SET-UP FOR ACCESS COMPATIBILITY

The legacy codecs (Matrix, Vector or BlueBox) must be configured for operation in **Music Mode**, which will allow full-fidelity (up to 15 kHz) connections. Voice Mode is not supported by ACCESS. Contact closures and ancillary data supported by legacy codecs are not supported by ACCESS.

When defining any outgoing connection, a profile must be assigned to it. For POTS Codec-compatible connections, the factory default POTS profile should work best.

USING ACCESS WITH POTS

To use ACCESS on POTS, insert the Comrex supplied USB POTS modem into the USB jack. Connect the phone cord to a normal, analog telephone jack.

WARNING: Under no circumstances should the raw extension from a digital phone system be attached to this port—you will likely damage ACCESS, your phone system, or both. You must obtain a true telephone-company-grade line, rather than an extension from your digital phone system.

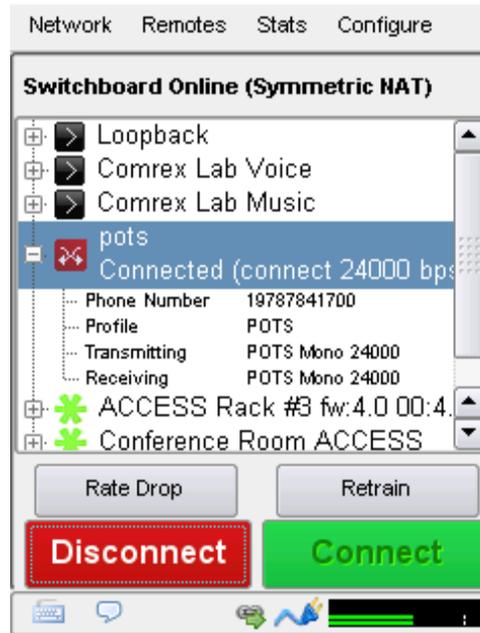
Once the POTS modem is installed, POTS Modem will appear as a new network option in the **Manage Network** tab. This network option will remain in the **Manage Networks** tab unless it is deleted by the user.

To initiate calls from ACCESS, simply create a remote connection with a telephone number as an address, rather than an IP address, in the **Remotes** tab. You must designate a POTS-based profile for this remote.

Note: Only 1 contact closure is available during a POTS connection.

RATE VS. RETRAIN

When incoming or outgoing POTS calls are active, the **Remotes** tab changes slightly. You will see two additional buttons appear on the tab, labelled **Retrain** and **Rate Drop**. These are special functions applicable only to POTS calls, so they are not visible during IP connections.



These controls are similar in function to those provided on POTS codecs. ACCESS will initially connect at the best data rate supported by the telephone line, and will display that connect rate on the **Remotes** tab next to the current state value. This value may be viewed by pressing the + next to the active connection. You can force the system to drop to the next lowest connect rate by clicking the **Rate Drop** button at any time. Audio transfer will be interrupted momentarily while the units negotiate the new connect rate. Alternately, you can force the system to initiate the entire training sequence again (the "chat" sounds heard at the beginning of a call) by clicking the **Retrain** button. You will lose audio for a longer time (approx. 7 seconds) but the modems will completely re-equalize the connection and audio will begin again once the retraining is finished.

Once ACCESS has dropped to a lower rate, either by a rate drop or retrain command from either end, there is no way to force it to connect at a higher rate. If you want ACCESS to try again for a higher connect rate, you will need to disconnect the call and dial again.

TROUBLESHOOTING POTS CONNECTION

There are dozens of factors that can affect the success or failure of a POTS codec call, some within the user's control and some not. Here's a short list of rules to follow for POTS codec connections:

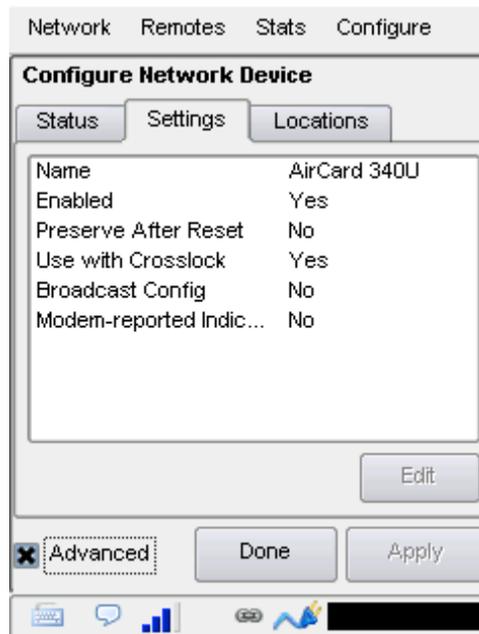
- 1 Use the POTS codec on a direct telephone company line and avoid in-house phone systems. A line used by a fax machine usually provides this direct access. (Be sure to disconnect the fax machine before connecting the codec!)
- 2 Check to see that there are no extensions or modems on the line you are using—or at least arrange that no one uses these during your broadcast.
- 3 If there is call-waiting on your line, disable it by entering “*70” in front of the number you are dialing.
- 4 If possible, try the POTS codec out at the remote site before your actual broadcast at about the same time of day that you plan to use it. This will give you a good idea of expected connect rates and possible line problems.
- 5 At minimum, connect a few minutes before airtime to assess the connection quality. Setting a MaxRate on the POTS codec, based on your findings, is highly recommended. MaxRate usually should be set at a level or two below the maximum unrestricted rate. This will provide a “guard band” of sorts against noise and corruption which may cause errors on the line.
- 6 If operation starts to degrade after a long period of connection, it may be that the phone line parameters have changed. These parameters are affected by factors such as time of day, weather and geographic location. The modems should be given the opportunity to renegotiate for these new parameters.
- 7 If you experience low connection rates or errors, try redialing. If that does not help, dial from the other end. If the call is long distance, try forcing the call to another carrier. If a good connection is found, keep that line up.

xxxiv. ADVANCED SETTINGS

The following settings are considered advanced. Most users will never need to edit these.

ADVANCED NETWORK SETTINGS

Once you check the **Advanced** checkbox under the **Settings** tab of a network, the following options appear:



Preserve after Reset - Normally, when ACCESS is set back to factory defaults (via **Device Manager**), all the network settings (including the main Ethernet) are erased. By setting this option to “**yes**”, the settings for this network will be preserved after factory reset. Caution should be used, as it’s possible to “lock yourself out” of the ACCESS by setting the Ethernet parameters incorrectly.

Use with CrossLock - Normally enabled, this option allows you to specify that this network port will not be considered as part of a **CrossLock** connection. This may be valuable when using one port for control purposes only and a secondary port for **CrossLock** media.

Broadcast Config - Normally enabled, this option instructs ACCESS not to respond to the “scan” function used by **Device Manager**. Caution: without the “Scan” function, **Network Recovery Mode** is disabled.

ADVANCED REMOTE SETTINGS

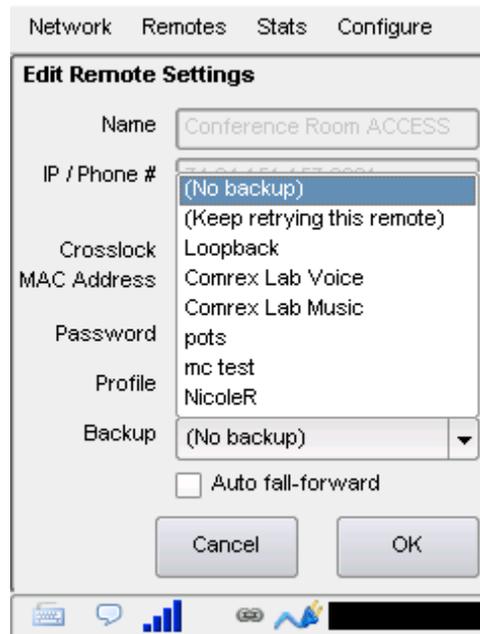
BACKING UP A CONNECTION

ACCESS features the ability to have an automatic backup to IP remote connections. The backup may be either another IP connection, or a POTS phone number.

If an IP connection fails, ACCESS will sense this and wait the amount of time designated in the **Local Timeout** parameter in the profile assigned to the primary connection. If the connection is restored in that amount of time, no backup will occur.

If the timeout period passes without restoration of the primary connection, ACCESS will automatically establish a connection (POTS or IP) to the designated backup. It will maintain that connection until it is manually disconnected.

To enable an automatic backup, both the primary and secondary remote connections must first be defined and assigned profiles. Next, select the primary remote and select **Change Remote Settings**. On this screen, choose the pull-down menu labeled **Backup Remote** and select the backup for this primary connection.



"AUTO FALL-FORWARD" FUNCTION

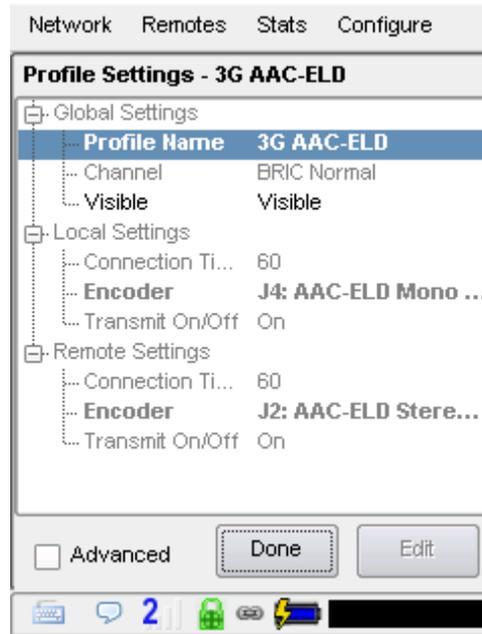
Selecting the **Auto fall-forward** function allows ACCESS to monitor the primary IP connection while the backup is active. If the primary is restored, and is detected to be valid for the timeout period, the backup will be disconnected and the unit will revert to the primary.

However, **Auto fall-forward** does not work when the POTS backup unit receiving the call is the same physical unit as the one being used as the primary IP-connected unit. This is because an ACCESS unit that is receiving an incoming POTS call cannot restore an IP connection. The backup connection must be an IP connection for an automatic restoration to take place.

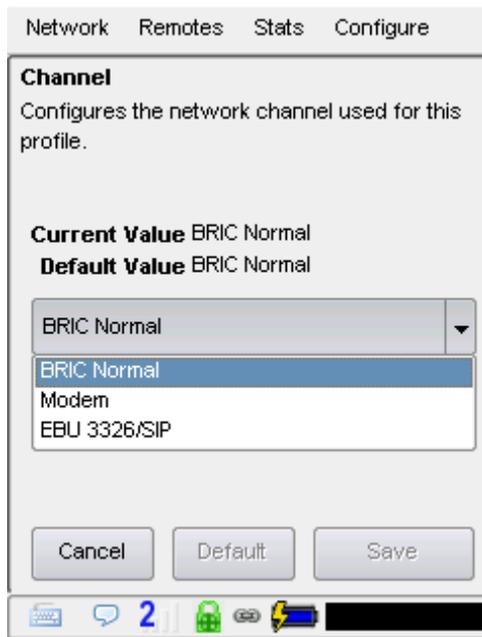
NOTE: Only IP connections can be designated as primary connections. Both IP and POTS connections can be backups.

PROFILE SETTINGS

GLOBAL PROFILE SETTINGS



Profile Name - Allows you to name the new profile. Tap the Keyboard icon in the bottom Navigation bar to bring up the keyboard.



Channel - Here you can select whether this to be used as an IP connection (BRIC Normal), a modem based connection (Modem, which uses a standard POTS phone line), or an EBU 3326/SIP connection.

If you are connecting over an IP connection to other Comrex products, we recommend you use the BRIC Normal selection.

The EBU 3326/SIP channel mode allows connections to be made in accordance with the requirements of EBU technical specification Tech3326. In this mode, ACCESS can make outgoing connections that are compatible with other manufacturer's codecs.

When using the EBU 3326/SIP channel mode to connect to other codecs, you must also choose an encoder that is included in the Tech3326 spec. These include all AAC modes, 16-bit Linear PCM, G.711 and G.722.

These compatibility modes are provided on a "best effort" basis. They are not guaranteed to be compatible with other manufacturer's implementations. ACCESS is not strictly compatible with Tech3326, because it does not support all mandatory encoders. For more information on EBU 3326/SIP, please see **Making EBU 3326/SIP Compatible Connections on page 91**.

NOTE: It's important to define the channel of a profile first. The choices in the subsequent sections will vary, depending on the Channel selection.

Make sure to press **Save** to confirm your selection.

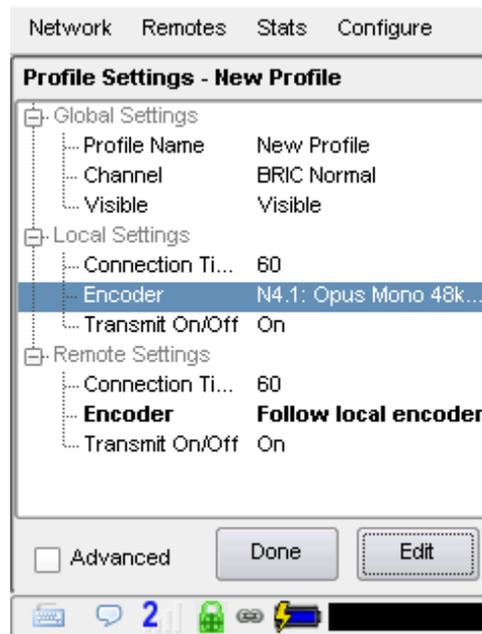
Visible - Here you can select whether this profile will be available as an option when setting up or editing Remote Settings. If you select **No**, the profile will not be visible in the Profile select pull-down in Remote Settings. This feature is useful to declutter your profiles list, to ensure that you can easily find the profiles you use most often.

TIP: You will notice that there is no **Edit** button when a factory profile is selected in **Manage Profiles**. To change the **Visible** option for these profiles, select the desired factory profile and press **View**. You can then highlight the **Visible** option and then press **Edit**. **Visible** is the only setting you can change for factory profiles.

LOCAL & REMOTE SETTINGS

If you've chosen an IP-based channel (such as **BRIC Normal**), you'll have access to two sets of options: **Local** and **Remote**. You'll use the **Local Settings** to determine how your ACCESS 2USB behaves, and the **Remote Settings** to determine how the ACCESS on the far end behaves.

Each category lists identical options, so we'll cover only the **Local Settings**:



Connection Timeout - Under normal circumstances, a connection will be terminated on one end, and the other end will drop the connection. However, if a network failure occurs, or a connection is ended abruptly for some other reason, the system will drop the connection after a pre-determined time. The default is 60 seconds, but this can be shortened or lengthened here.

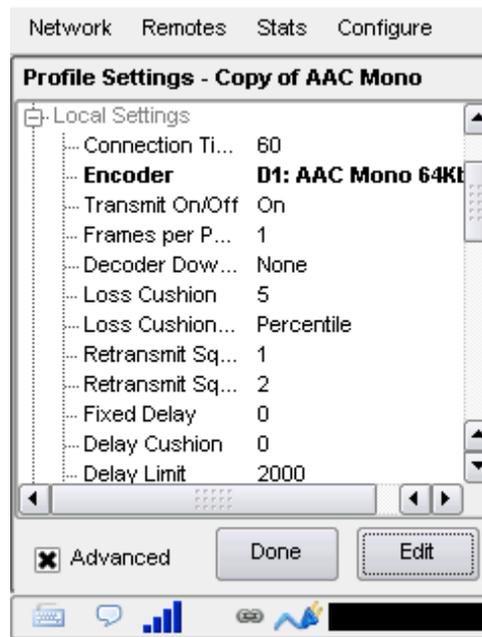
Encoder - Using this menu, you can select the encoder used to send audio from this ACCESS (local) as well as the encoder used to send audio to this ACCESS (remote). The default value of the remote encoder is to follow the local encoder; that is, it will send exactly the same codec mode it receives. The display will show **Follow local encoder** under the **Remote Settings** folder when this mode is selected.

Transmit On/Off - This option determines whether the selected encoder (local or remote) is actually sending any data. By default, all encoders are turned on, but there may be circumstances where one-way operation is desired, such as multi-streaming. Selecting **Off** under **Transmit On/Off** under the **Local Settings** folder disables outgoing audio streaming. In the same way, selecting **Off** under the **Remote Settings** folder disables the incoming audio streaming from the remote encoder.

ADVANCED PROFILE SETTINGS

The options available in the default mode should provide good performance for most users. However, in some circumstances, it may be important to fine-tune some of the more obscure parameters that make ACCESS work. In addition to the information printed below, most of these choices also have “help” information built into the selection on ACCESS to remind users of what each function does.

By clicking the **Advanced Options** box in the lower left of the **Profile Settings** screen, the following **Advanced Options** will be available:



Frames per Packet - Allows the encoder to wait for X number of frames to exist before sending a packet. This option differs from FEC because each frame is only sent once. Setting this value to a number higher than one can reduce network usage, at the expense of delay. This is because this setting reduces the frequency with which packet overhead bits like IP and UDP headers are sent.

Decoder Downmix - This allows the decoded “stereo” (two-channel) audio that arrives at the receive end to be downmixed to a mono signal. The choices are **None**, **Mono Left Only**, **Mono Right Only**, and **Mono Full**. Except for **None**, these are mainly used for sending two different mono streams to two different destinations at the same time. For more information on these choices, see the section **Appendix D - Using the Comrex ACCESS Decoder Downmix Function on page 161**.

Loss Cushion - This choice instructs the buffer manager to ignore a certain percentage of late packets in its calculation. The default value is 5%. Applications that are not at all delay sensitive may wish to reduce this value to zero, while extremely delay sensitive applications may prefer to have this closer to 25%. By eliminating packets that

arrive extremely late, delays can be reduced greatly. The decoder error concealment does a very good job of hiding any losses that may result.

Loss Cushion Mode - This mode ensures that the unit will show losses in terms of percentile of packets lost.

Retransmit Squelch Trigger and **Retransmit Squelch Max** - These options are used to determine how the buffer manager reacts to typical data dropouts, like those seen on some wireless networks. If the data protection causes retransmission of data packets during a signal fade, this can cause the network protection layer to “fight” the buffer manager, expanding the buffer and increasing the delay, with no real benefit.

The **Retransmit Squelch** capability allows the decoder to detect these events and avoid having the buffer manager react. These should normally be left where they are, but may be changed if dropouts are a problem.

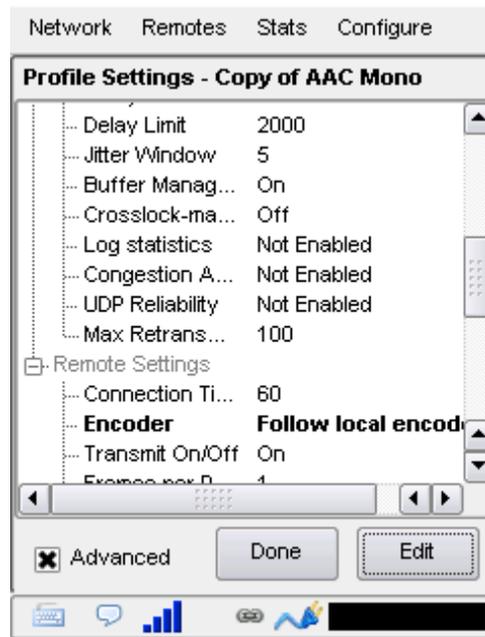
The **Retransmit Trigger** function determines the amount of time the decoder must experience 100% packet loss before the **Retransmit Squelch** function is triggered. Default is one second.

The **Retransmit Squelch Max** function determines the longest period of data loss during which the squelch function is active. The default is two seconds. During the squelch period, the buffer manager will ignore the relative jitter experienced and will not adjust buffer size to compensate.

Fixed Delay - This option simply sets the **Delay Cushion** and **Delay Limit** at a similar value, so that the delay buffer is defined to the chosen value and will not increase or decrease significantly.

Delay Cushion - The **Delay Cushion** setting instructs the jitter buffer manager to not attempt to drive the delay below a certain value. For example, if the delay cushion is set to 500 mS, that amount of fixed delay will be added to the buffer. If the jitter manager needs to increase the buffer it will do so, but will not fall below the ½ second level.

Delay Limit - The **Delay Limit** instructs the jitter buffer manager to not “wind” the buffer out beyond a certain delay value, regardless of how many packets are lost. This is useful in applications where staying below a certain delay figure is essential. However, use of the delay limit can result in very poor performance if the network jitter dramatically exceeds the set limit.



Jitter Window - This parameter defines the amount of time (in minutes) that historical network performance is analyzed. The result is used to make the rest of the calculations. As an example, if the **Jitter Window** is set to the default of five minutes, and if a dramatic network event happens that causes the buffer to react by increasing the buffer size, the event will be included in the manager's calculations for the next five minutes. If the network experiences improved performance, the manager may choose to wind the buffer back down after the five minutes has passed.

Buffer Management On/Off - This option is available only as a troubleshooting tool. Turning the buffer manager off will result in eventual failure, since the manager compensates for clock skew between the encoder and decoder.

Crosslock-managed Delay - By default, the buffer manager finds its own delay target. The **CrossLock** layer also calculates a delay target that is generally more conservative, and this option allows that target number to be used. Our testing shows best results with the default delay target.

Log Statistics - This function is used in factory diagnostics and should be left disabled unless instructed to be changed by Comrex support.

Congestion Avoidance - Enabling this option allows the encoder to dynamically change the number of frames per packet sent, thereby reducing total data requirements. In addition, in most encode modes, enabling **Congestion Avoidance** provides the system with the ability to step down to a lower encode data rate if desired. This will happen automatically and with no audio interruption. NOTE: Step down congestion avoidance is not enabled in Linear PCM modes.

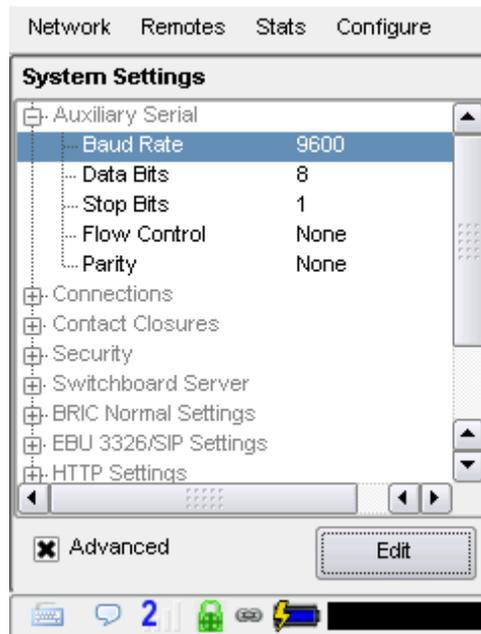
UDP Reliability - UDP, the Internet protocol used by BRIC Normal connections, does not have any inherent error correction capability. **UDP Reliability** adds an intelligent algorithm that requests packet resends only when appropriate. **UDP Reliability** can be useful on some wireless connections that have unsatisfactory performance due to packet loss.

Max Retransmission Rate - Allows setting of an upper limit on how much additional bandwidth is utilized by the BRUTE UDP reliability layer. The default setting is 100, which allows the error correction layer to use the same amount of bandwidth as the audio stream. As an example, if your audio stream is consuming 80 Kb/s of network bandwidth, and UDP Max Retransmissions is set at 50%, up to 40 Kb/s additional network bandwidth may be used for error correction.

ADVANCED SYSTEM SETTINGS

When the Advanced System Settings box is checked, a few additional options are shown. Note that some of these functions are also shown in the **System Settings** section before the **Advanced** box is checked.

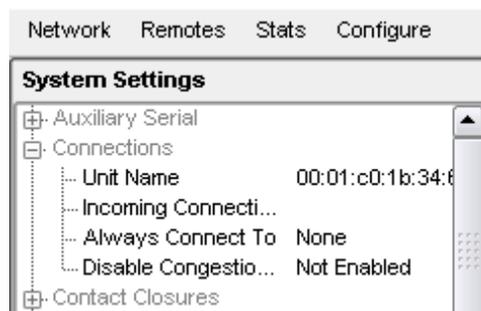
AUXILIARY SERIAL



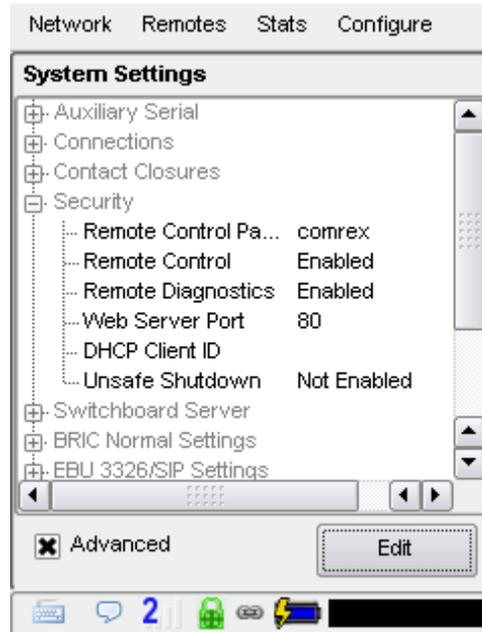
This allows you to set the parameters of the auxiliary serial data port. This port is always active during an IP connection and allows serial data transfer along the same path used for the audio data. It does not remove any audio data; the serial data is added to the packets and bandwidth is increased to support the additional data. For this reason heavy use of serial data can affect overall codec performance. Settings are available for **Baud Rate**, **Data Bits**, **Stop Bits**, **Flow Control** and **Parity**. Most users will leave the defaults of **9600**, **8**, **1**, **No Flow Control** and **No Parity**.

CONNECTIONS

Disable Congestion Avoidance - Turns “**Avoidance Congestion**” feature off.



SECURITY



Remote Diagnostics - Enables Comrex support to connect to this unit using the SSH protocol for troubleshooting purposes. We recommend leaving this option enabled. Since SSH access requires a key value that is not disclosed by Comrex, generic SSH requests are rejected.

Web Server Port - In order to deliver the remote control web page, ACCESS must “listen” on a certain Internet port number for a request from a web browser. By default, web page servers listen on port 80 for incoming requests. In some environments, you may wish to remotely control ACCESS through your router, and port 80 may already be utilized by another device. This setting gives you the ability to change the port where the system listens for and delivers web pages from. **NOTE: you will now need to enter this new port number into your browser in order to see the unit. As an example, if the Web Server Port is changed from 80 to 84, the address of the unit must be entered in a browser in the following manner: <http://192.168.1.142:84>**

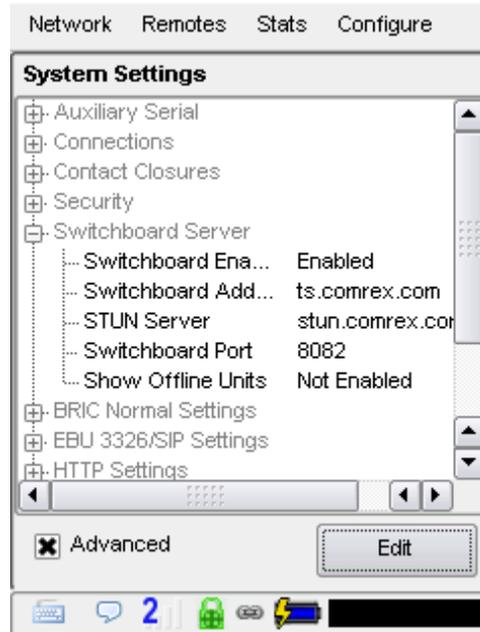
If this value is changed, there isn’t any need to change the way you get the remote web page; the change is automatically reported to the browser when the page is addressed.

The web server port is also used by the **Device Manager**, **Codec Commander** and **Remote Control** software provided by Comrex, so if you change this value you’ll want to make a note of it for the next time you update the unit’s firmware.

DHCP Client ID - Allows entry of a client ID prefix for use with DHCP address selection capability.

Unsafe Shutdown - This setting allows you to disable the Safe Shutdown feature. Ordinarily, the ACCESS will spend approximately five seconds in powering down its systems safely. For the wellbeing of your equipment, we recommend Safe Shutdown enabled, and allowing this process to complete before disconnecting all power sources.

SWITCHBOARD SERVER



Switchboard Add (Address) - Shows the domain address of Switchboard.

STUN Server - Enables the unit to contact the STUN server maintained by Comrex to learn what its public IP address is.

Switchboard Port - Allows selection of the TCP port of the Switchboard Server.

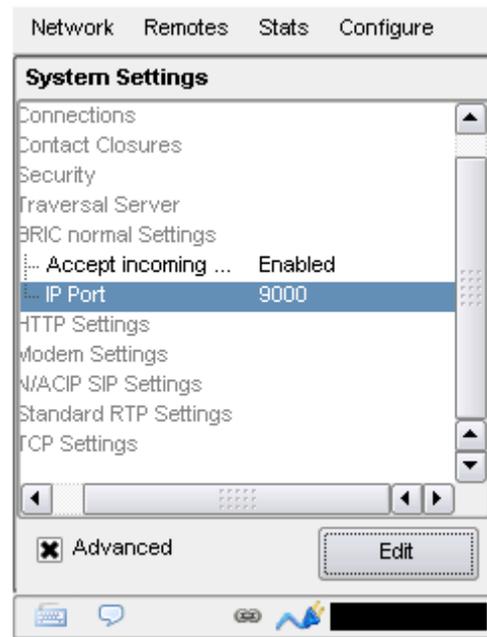
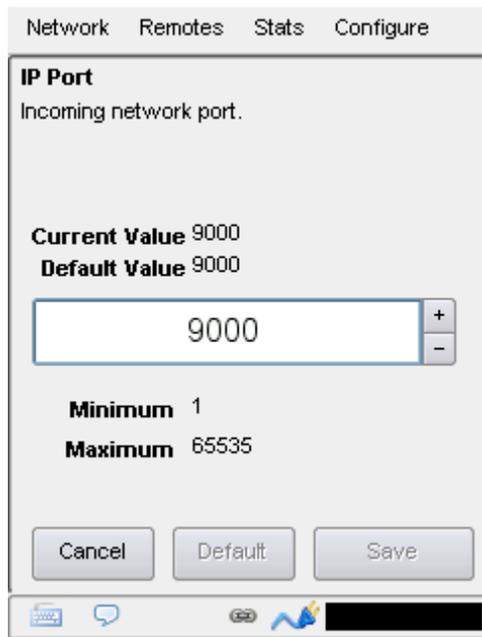
BRIC NORMAL SETTINGS

IP connections use a concept known as **ports** to differentiate between different applications on the same computer. A port can be thought of as a way to get into and/or out of your computer. Most firewalls function by only opening the network to traffic through specific ports.

Each IP connection has a source and destination port. In most cases, the source port is unimportant, but the destination port can determine whether or not the connection will be made. Certain incoming ports can be firewalled to outside traffic, and in the case of more than one ACCESS unit behind a router (sharing a single public IP address), the only way for them all to take incoming calls is to assign different incoming ports to each device.

CrossLock makes connections on UDP port 9001. Legacy Comrex audio codec connections are made on UDP port 9000. In order to accept calls from both newer and older ACCESS units, you may need to open additional ports in your router or firewall settings.

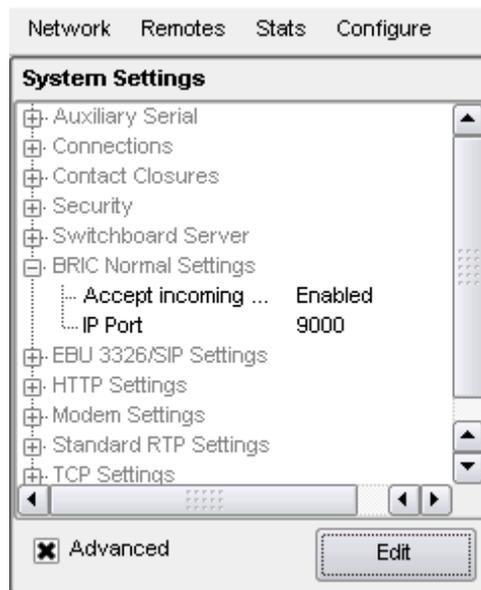
Changing the port for incoming connections is done under **System Settings**.



To change the destination port of an *outgoing* call, you must add the port number to the IP address in the correct format. For example, to initiate a connection using Comrex’s default BRIC Normal port (which is UDP 9000), enter the following into the IP address field: 70.22.155.131:9000.

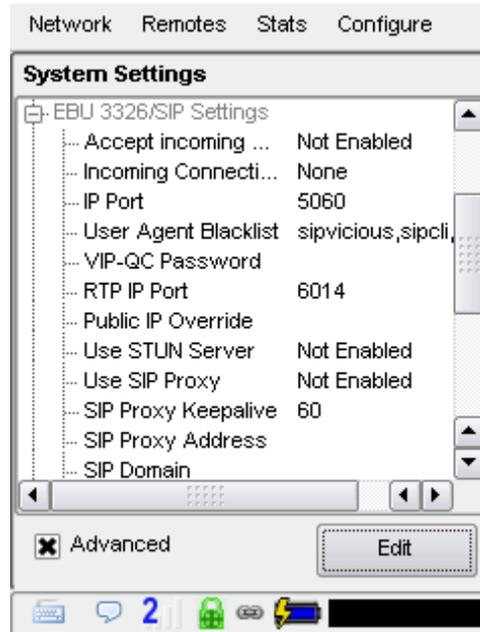
Note that the last four digits of the IP address are the numbers corresponding to the port at the receive point. Be aware that the call will fail unless the ACCESS on the far end is set to receive data on that port.

IP Port - This option allows you to define the incoming UDP port for incoming IP connections. This is explained in detail in the previous section.



NOTE: Always remember the “X+1” rule for setting the CrossLock port whenever you use a non-standard BRIC Normal port to manually establish an *incoming* connection. (For more information, see the advanced CrossLock settings on **page 149**.)

EBU 3326/SIP SETTINGS



Accept incoming connections - EBU 3326/SIP calls must be answered automatically on NX. If this option is disabled, no EBU 3326/SIP calls will be answered and only outgoing EBU 3326/SIP connections can be made.

Incoming Connection Profile - In some unusual circumstances, it's necessary to define the profile used on incoming SIP/3326 connections to be something different than what is being received. This option allows that to be changed.

IP Port - Universally, SIP connections are supposed to use UDP port 5060 to negotiate calls between devices (and between servers and devices). Changing this port number will change which incoming port is used to initiate connections, and to which port connection requests are sent. The change must be made on both devices. **NOTE: Using a port other than 5060 will essentially make your codec incompatible with industry-standard VoIP devices.**

User Agent Blacklist - Allows entry of list of SIP user agents that will not be allowed to communicate with this ACCESS unit. Must be entered with names separated by commas.

VIP-QC Password - Allows entry of password for VIP-QC connections.

RTP IP Port - Allows setting of RTP network port.

Public IP Override - Allows entry of override for Public IP port.

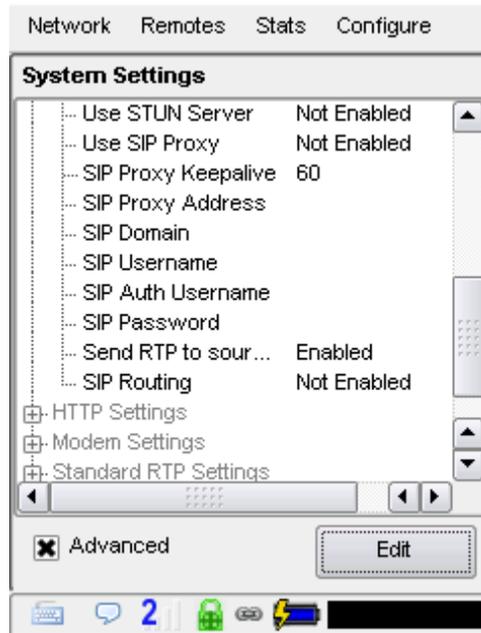
Use STUN Server - Enables/disables use of the STUN server.

Use SIP Proxy - Enables/disables registration with the SIP proxy to use for inbound and outbound calls.

SIP proxy Keepalive - Sets "keepalive" interval time for SIP connections.

SIP Proxy Address - Allows choosing proxy/registrar server to use for SIP calls.

SIP Domain - Used to authenticate SIP calls. If not set, the SIP proxy name will be used.



SIP Username - Allows entry of SIP username.

SIP Auth Username - Allows entry of SIP username for authentication.

SIP Password - Allows entry of password for authentication.

Send RTP to source port - Enables/disables the ability to send RTP data to the remote port matching the source of the received RTP packets rather than the negotiated port.

SIP Routing - Enables routing of SIP messages. **NOTE: May adversely affect the ability to traverse NAT firewalls.**

HTTP SETTINGS



Accept incoming connections - Enables/disables the HTTP streaming function.

IP Port - Sets incoming network port.

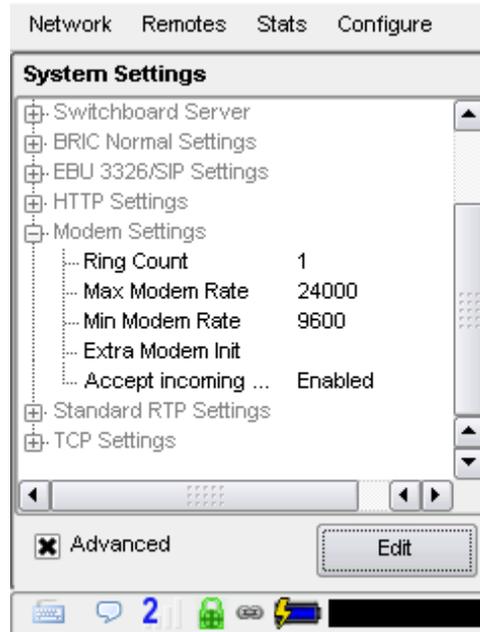
Encoder - Sets the encoder used for streaming. Must be compatible with the media player.

Genre - Sets "genre" for HTTP streaming. Default is "Live".

Info URL - Sets informational value of the URL associated with the stream.

Public - Enables/disables setting of the public stream.

MODEM SETTINGS



Ring Count - If auto-answer is enabled for incoming calls, sets the number of rings before line is answered.

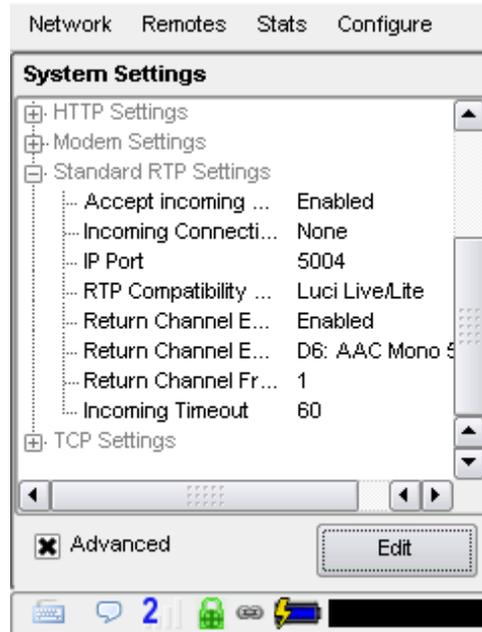
Max Modem Rate - Maximum allowed baud rate for connections. Default is 2400.

Min Modem Rate - Sets the minimum allowed baud rate. Default is 9600.

Extra Modem Init - Allows entry of a modem initialization string.

Accept incoming connections - POTS calls must be answered automatically on ACCESS. If this option is disabled, no POTS calls will be answered and only outgoing POTS connections can be made.

STANDARD RTP SETTINGS



Accept incoming connections - RTP calls must be answered automatically on ACCESS. If this option is disabled, no RTP calls will be answered and only outgoing RTP connections can be made.

IP Port - Sets incoming IP port. Default is port 5004.

RTP Compatibility mode - This option allows you to choose between several sub-options to be compatible with various equipment. The choices are:

Standard - The encoder will send simple RTP packets without regard to handshaking or status of the network. Useful mostly for experimenting against unknown gear.

Luci Live/Lite (default) - The encoder will adapt the RTP stream to be more compatible with the Luci brand smartphone app.

Zephyr Xstream - The encoder will adapt the RTP stream to be compatible with the Zephyr Xstream ISDN codec in IP mode.

Standard RTP modes other than Luci are “experimental” and are not subject to support by Comrex support staff.

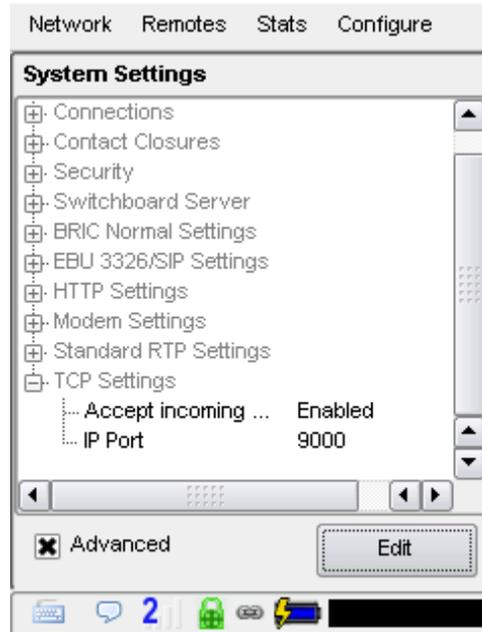
Return Channel Enabled - Enables a return channel to be sent back to the other unit.

Return Channel Encoder - Specifies the codec to be used for the return channel.

Return Channel Frames per Packet - Sets the number of audio frames that are included within each packet. **NOTE: Delay will increase if a value over “1” is entered.**

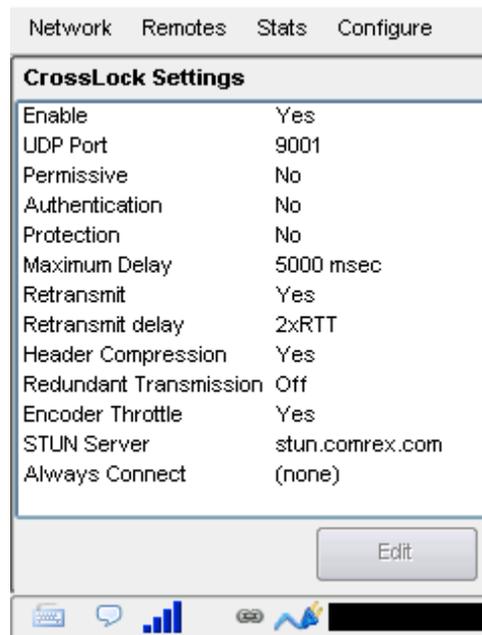
Incoming Timeout - Set the time that incoming call connections will timeout.

TCP SETTINGS



IP Port - Allows entry of incoming network port. Default is port 9000.

CROSSLICK SETTINGS



Enable - Enables the use of **CrossLock**.

UDP Port - By default, **CrossLock** uses UDP port **9001** for connections. For best results, this port should be open for incoming data on at least one of the codecs in the link. This means that unless the **ACCESS** is on an “open” Internet connection (no firewalls or routers used) the port will need to be forwarded to it. In instances where more than one codec will be attached to the same public IP address, you may need to change the default incoming port. It can be changed here. If this port is changed and **Switchboard** (which, by default, uses UDP port **9000**) is used to establish connections, no further changes are required. In the case of connections without **Switchboard**, the port change will need to be noted in the outgoing address on the calling unit.

Manually Establishing Incoming Connections - When establishing incoming connections manually (i.e., without using **Switchboard** to connect), the **CrossLock** port must ALWAYS be set one spot up numerically from the **BRIC Normal** port. This principle—**If the BRIC Normal port is X, the CrossLock port MUST be X+1**—is known as the “X+1” rule and it’s important to remember with incoming **CrossLock** connections.

If you’re using the default port settings for **BRIC Normal** (UDP 9000) and **CrossLock** (UDP 9001), this shouldn’t be a problem. If you need to use an *alternate* **BRIC Normal** port like UDP 9050, however, you **MUST** use UDP 9051 as your **CrossLock** port to establish an incoming **CrossLock** connection.

Permissive - Enabling **Permissive** mode removes the unit ID filter entirely. **CrossLock** connections can be made without regard to unit ID. Note the far end unit must know this codec’s unit ID, or must also have permissive mode available. Recommended for closed networks without security concerns.

Authentication - **ACCESS** firmware 4.0 and higher uses security certificates assigned to the codec hardware to authenticate it as a Comrex product. This option determines whether connections will be made to codecs without these certificates. Certificates are assigned to codecs by the **Switchboard** server after an upgrade to firmware 4.0 or higher (**Switchboard** upgrade not necessary). Because some codecs may be firewalled and not receive certificates after upgrades, this option is defaulted off.

Protection - **ACCESS** has the ability to prevent interception of streams (Encryption) and alteration of streams (Protection). The CPU requirements of these modes are large, and therefore it is not recommended to apply these options to streams when not required. They are set to off by default to conserve CPU.

Maximum Delay - **CrossLock** operates by choosing a “**Target Delay**” figure based on jitter performance of its various networks over a time window. To prevent excessive delay in the case of one extremely laggy network, it has a maximum delay setting here. In the case of multiple networks with very high jitter figures, this setting can be increased from the default five seconds by the user.

Retransmit - In addition to FEC, **CrossLock** utilizes an ARQ style algorithm to allow retransmission of lost packets when time permits. This mode is recommended but can be disabled here.

Retransmit Delay - **CrossLock** automatically provides an extra “Retransmit Cushion” that provides some time to make ARQ error correction effective. The default amount of time is twice the measured round trip delay of the network (2xRTT). This has been shown to be most effective on most networks, but can be altered lower (1xRTT, none) or higher (3xRTT) using this menu.

Header Compression - The nature of Internet packets sometimes results in IP overhead (RTP headers and other info) actually using nearly as much bandwidth as the payload. **CrossLock**, by default, compresses some of these headers to conserve network bandwidth. In instances where the network rejects this, or packet inspection is required, this compression can be disabled.

Redundant Transmission - When using multiple networks, **CrossLock** defaults to “Bonding” mode, adding the capability (with dynamic allocation) across the networks. Loss of any network results in a very fast adaptation to the existing networks, but can result in short audio disruptions. In scenarios where all networks are unmetered and of known good quality, changing to redundant mode can result in less disruption during a network loss. All data is delivered on all networks simultaneously. This is an outgoing parameter only—in order to provide two-way redundancy, this setting must be changed on both ends.

Encoder Throttle - Some encoders, like Opus, provide the ability to reduce outgoing data rate in the presence of network congestion. The default is to allow the **CrossLock** Manager license to throttle the encoder. This can be defeated by setting this value to “No”.

Stun Server - **CrossLock** uses its own Cloud Server (STUN) to determine the NAT status of each codec before connection. This can be set to a different value than the main STUN server used to provide status to the **Remote Connections** page. Default is always the Comrex server at stun.comrex.com.

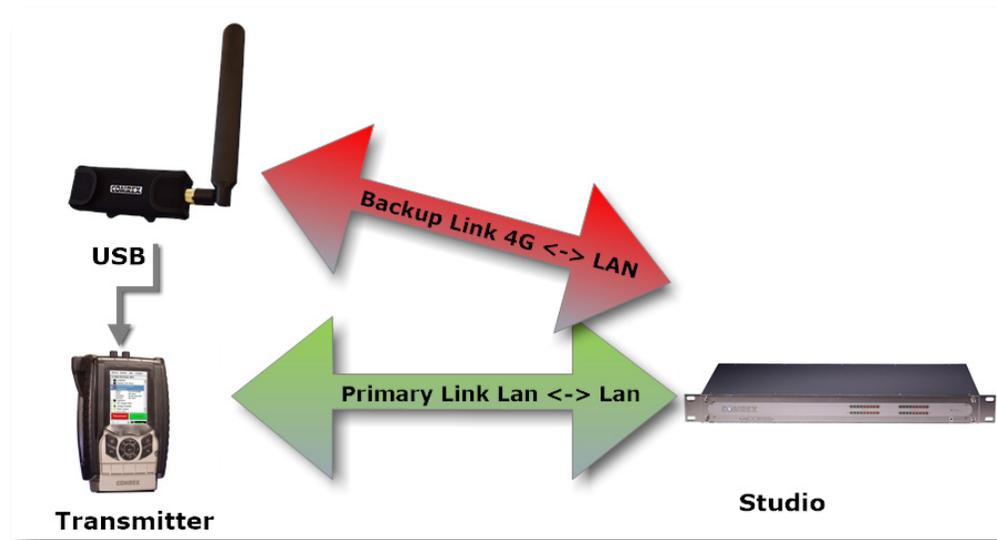
Always Connect - This option provides for **CrossLock** to be always connected to a destination. By its nature, **CrossLock** uses very little data so the network utilization of this mode (when idle) is very small. If you only connect to one destination, having **CrossLock** always connected makes media connections faster, and provides an indication of network status between the devices (“ready” light or **CrossLock** status). Most users should leave this setting off.

Note that this option is different than “**Always Connect To**” under **System Settings**. That option maintains an audio connection, not just a **CrossLock** session.

HOTSWAP

ACCESS 2USB units operating 4.3-level firmware or higher are able to utilize HotSwap, which allows customers using CrossLock in “Dual Network” mode to designate one network as primary and the other network as secondary. The secondary network (e.g. wireless 4G) then backs up the primary network in case of failure.

A typical usage scenario would be a codec that is attached 24/7 providing an STL link. Because it’s often impractical (and expensive) to run audio over a 4G wireless network full time, HotSwap ensures that the CrossLock connection primarily uses another network (e.g. an ethernet connection) and only falls over to the 4G wireless network as a backup when it needs to. When the primary network is restored, Hotswap will switch back to it and continue to hold the secondary network in a backup state, waiting for the next time it’s needed.



Please note: Codecs on both ends of the link must be running at least 4.3-level firmware in order to operate HotSwap.

Any any supported network (e.g. Ethernet, Wi-Fi, 4G wireless) can be designated as the primary or the backup network.

Because Hotswap is an alternate mode of the Comrex CrossLock reliability layer, connections between codecs must be established via CrossLock in order to use it.

DATA USAGE

It’s important to note that even when a network is in a backup state, a small amount of data is sent and received on it. (For 24/7 operation, this data will total less than 0.5 GB for a typical month of usage, assuming no Hotswap activity occurs. Of course, more data will be used if the Hotswap function engages.) **Regardless of how Hotswap is used or set up, Comrex assumes no liability for data overage charges, even in the event of software bugs or any other failure of hardware or software. It is entirely the responsibility of the user to monitor any metered data usage.**

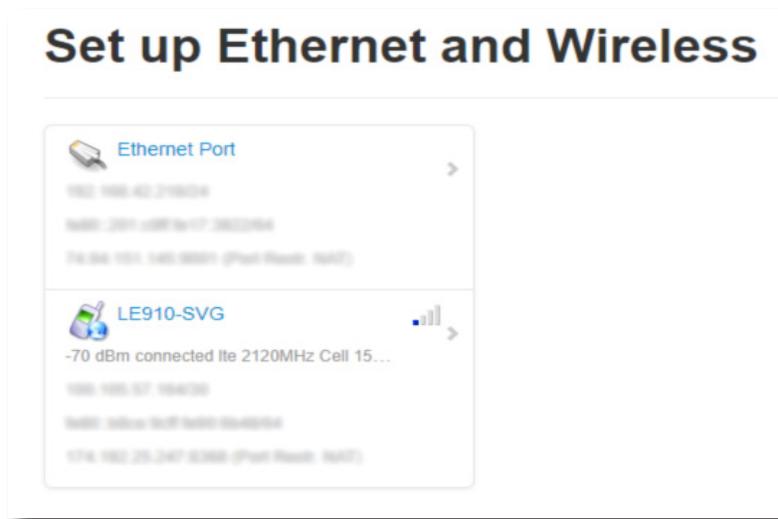
SET UP

Setup for HotSwap is done entirely on the end of the link that has the dual networks connected. Because HotSwap setup is not yet supported in the “console” (KVM) interface available on the ACCESS 2USB, setup is handled via the Toolbox configuration page, accessible from the codec via a web browser at the address: <codec_ip_address>/cfg.

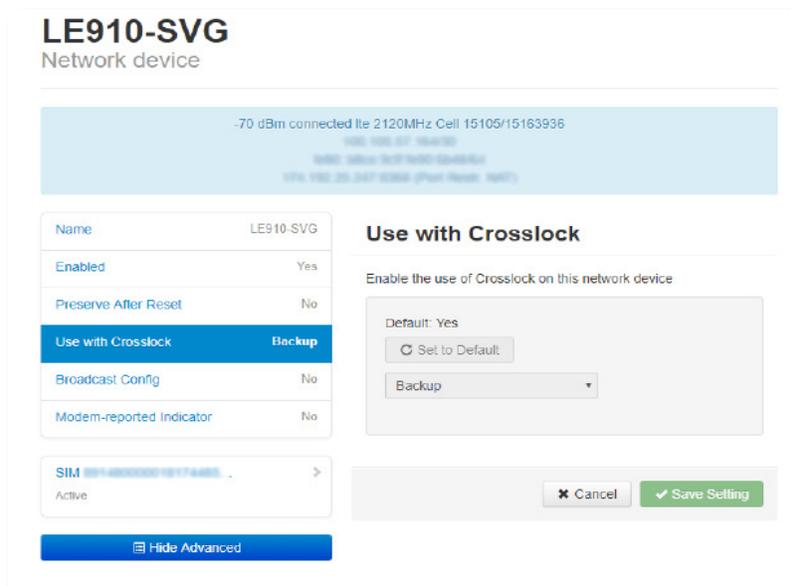
The default behavior for CrossLock is to use all networks available, and apportion data as it sees fit based on capacity and delay calculations. You will need to change this behavior in the Toolbox menu.

Before entering the setup menu, the secondary network should be attached to the codec via USB or Ethernet.

In Toolbox, navigate to the Network/Admin/CrossLock menu and select “Set up Ethernet and Wireless”. You’ll see a list of all networks attached to the codec and their status, as shown below.



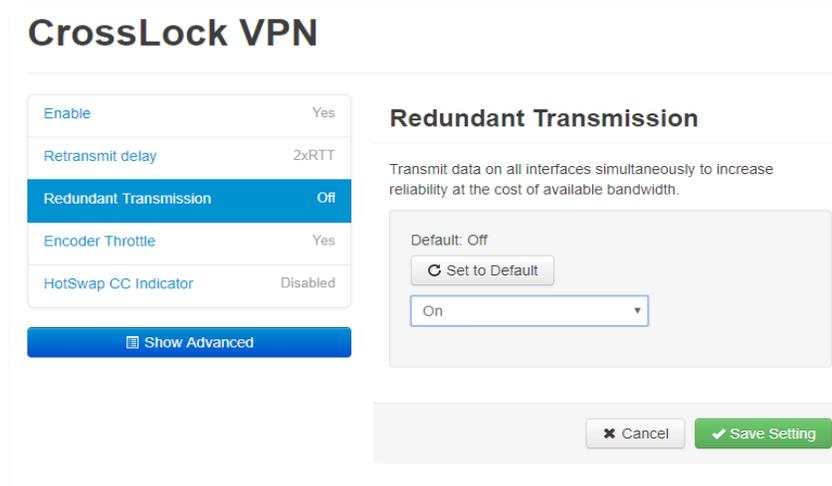
Here you will choose the backup network and expand its options using the “Show Advanced” button:



Find the option labeled “Use with CrossLock” and change the default from “yes” to “backup”.

Click “Save Settings”, then click “Back” until you get to the main “Network/Admin/CrossLock” menu.

Next choose “CrossLock VPN” and locate the entry labeled “Redundant Transmission” as shown below.



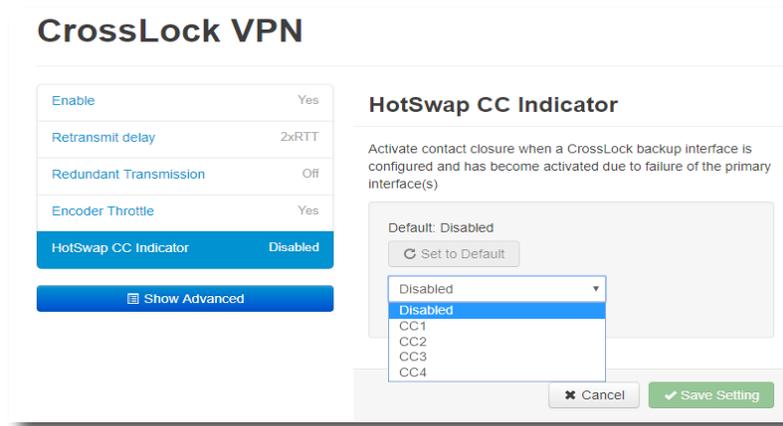
Change this from the default “Off” to “On”. Choose “Save Setting”.

Finally, you’ll want to set one of the contact closures to alarm you when the HotSwap function is engaged.

Still in the CrossLock settings, choose “HotSwap CC Unit”. First choose whether you want the contact closure output to trigger on the local, remote, or both codecs. Select “Save Setting”, and then click “Back”.



Next choose “HotSwap CC Indicator” and select which contact closure to trigger. This will override any previous settings you’ve made in the main configuration web page regarding contact closures.



Choose “Save Setting” and exit the Toolbox page.

MAKING & BREAKING CONNECTIONS

Connections are made and broken via the web-based user interface. This is accessed via a web browser at the IP address of the codec. Connections can be made manually, with or without Switchboard, and can be set to “always connect” in the case of 24/7 operation. We recommend making manual connections for 24/7 operation, and not relying on Switchboard, as it unnecessarily introduces another point of possible failure.

As long as an incoming CrossLock call is possible on the primary network attached to a codec, the call can be initiated from the other end. As an example, at a transmitter site the primary network is a DSL line and port 9001 UDP is open from the public Internet. The backup network is a 4G modem, which on its own would not accept an incoming connect request. Even without using Switchboard, the connection can be initiated from the studio side, and the 4G modem will be automatically added to the CrossLock channel.

Q: CAN I GET A REMOTE INDICATION THAT ACCESS IS CONNECTED TO SOMEONE?

A: Yes. Using the **Configure Tab/Additional Configuration**, you can re-assign **Contact Closure Output #4** to trigger whenever the ACCESS makes a valid connection. The function of **Contact Closure #4** will be changed in the following ways:

- a **Contact Closure #4** will no longer be available as an end-to-end signal.
- b Whenever ACCESS detects a valid incoming stream, it will trigger **CC #4** and maintain it until all valid connections stop.

Q: WHAT STEPS SHOULD I TAKE WHEN I'M HAVING CONNECTION PROBLEMS WITH ACCESS?

A: The first step is to determine whether the problem is occurring in one direction or both. If in only one direction, take a look at network usage patterns on the local end of each ACCESS. If someone else on your LAN is downloading large files on the decoder side (or uploading large files on the encoder side) this may cause some performance issues. You may need to ask them to temporarily cease activity, or investigate a network router solution that will offer ACCESS priority over other traffic.

Next, take a look at the **Stats** tab on the ACCESS that is decoding the faulty audio. Check the jitter figure for your incoming connection. If this number is varying dramatically (good networks keep this figure below 50 mS), then you may need to increase the **Local Delay Cushion** setting within the profile used to connect to that remote. Although it will increase your audio time delay, you may find increasing the cushion by 100-300 mS or more will result in more stable connections, since the jitter buffer manager will no longer attempt to reduce delay by making the buffer smaller than the cushion.

Q: HOW CAN I OPTIMIZE SETTINGS FOR EVDO, UMTS, OR OTHER WIRELESS ACCESS?

A: Since there is typically already a substantial delay in these networks, it's often not a priority to keep ACCESS delay to the absolute minimum. Using the profile that you set up for the EVDO connection, enter the **Advanced Options**. Raise the **Frames/Packet** setting to 4 in both **Local** and **Remote Encoders**. This will reduce overall bandwidth and enhance reliability on many networks. You may also need to increase **Delay Cushion** on the non-wireless decode side as described in the previous answer.

Q: MY IT GUY HAS APPARENTLY HAD WAY TOO MUCH COFFEE BECAUSE HIS FACE IS ALL RED AND HE'S RUNNING AROUND YELLING SOMETHING ABOUT SARBANES/OXLEY AND CRASHING THE CORPORATE NETWORK. IS THERE SOMETHING I CAN GIVE HIM TO MAKE HIM FEEL BETTER ABOUT THE SECURITY OF THE NETWORK AND HIS LIFE IN GENERAL?

A: Why, yes! We've created a special document called "**Information for IT Managers**" which was written specifically to help keep the blood pressure and stress levels of IT managers within normal tolerance. It can be found in the **APPENDIX B** on **page 159** of this manual or in the support section of our website at www.comrex.com.

Q: MY IT GUY IS CONCERNED ABOUT SECURITY AND WANTS TO KNOW WHAT SERVICES ARE OPEN ON THIS BOX.

A: As mentioned, we're serving an HTML/XML page on the well known server port, 80. Our streaming application is UDP/RTP on port 9000 (9001 for CrossLock connections). SSH is enabled by default but requires a passkey. You can disable it completely in the **Security** section of the **System Settings** menu by setting the **Remote Diagnostics** option to **Not Enabled**. Leaving **Remote Diagnostics** (SSH) enabled will help if Comrex support needs to interface with your ACCESS.

Q: I NOTICE IN THE ADVANCED OPTIONS THAT I CAN CHANGE MY STREAMING FROM UDP TO TCP. SHOULD I?

A: Not if you want the best overall performance. ACCESS is optimized in terms of data rate, stability and delay to use UDP. TCP mode increases overhead and delay, and is included only for environments where UDP is hopelessly blocked by a firewall. ACCESS decoders do listen to both TCP and UDP ports and choose whichever arrives first. If an ACCESS gets an incoming TCP connection, it will establish TCP in the other direction automatically. One other note for use with TCP: most of the information presented on the **Stats** tab is generated by the UDP functionality, so you won't see much here using TCP.

xxxvi. APPENDIX A - IP COMPATIBILITY

The ACCESS is capable of encoding and decoding a choice of three different types of non-ACCESS streams: Standard RTP, Luci Live and Zephyr Xstream. The choice is exclusive, i.e., you must set the ACCESS specifically for the type of stream you wish to be compatible with. The unit will remain incompatible with the other two types until you change it.

- 1 **Luci Live** - This PDA/PC-based software allows real-time streaming over IP links. As of version 1.2, Luci Live includes AAC and HE-AAC in addition to the default MP2 algorithm. ACCESS can communicate with Luci Live only in Luci's AAC modes. Note: The free demo available from Luci does not incorporate the AAC functions; you must have a licensed and registered copy to use AAC.

To communicate with a Luci Live device:

- a **Initial Setup** - This will define all Standard RTP connections to be Luci Compatible.
 - ACCESS Rack - On the **System Settings Tab**, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, choose **Luci Live**.
 - ACCESS 2USB Portable - Choose **Configure** then **System Settings** on the display. Under **Standard RTP Settings** select **RTP Compatibility Mode** and choose **Luci Live**.
 - b **Incoming Connections** - Luci Live sends either an AAC or HE-AAC stream to the ACCESS on UDP port 5004. These streams will be automatically decoded. By default, a return channel of AAC 56 kb/s mono is returned to the Luci Live product. The return channel may be altered to any Luci-compatible mode in the **Systems Setting** section. ACCESS that do not have the AAC upgrade applied will not create a return channel.
 - c **Outgoing Connections** - Build a profile using the **Profile Manager** on either the ACCESS Rack or Portable and select a Channel Mode of **Standard RTP**. Then choose a Luci-compatible encoder for the outgoing call. The Luci software will control what type of stream, if any, is returned to the ACCESS.
- 2 **Zephyr Xstream** - Xstream Firmware version 3.2.0 and higher supports an "RTP Push" function that is compatible with ACCESS in some modes. ACCESS is not currently compatible with the Xstream's HTTP and SIP streaming functions. There are several limitations imposed by the Xstream when using the RTP Push function:
 - ⊕ On the Xstream, only AAC and MP3 coding are available in this mode, and ACCESS is only compatible with the AAC mode.
 - ⊕ The Xstream uses downsampling in modes below 96 kb/s, which is not supported by ACCESS.
 - ⊕ In order for an Xstream to decode an ACCESS stream, the default decoder setting must be changed from <Auto> to <AAC> in the codec menu of the Xstream.

To communicate with a Zephyr Xstream:

- a **Initial Setup** - This will define all Standard RTP connections to be Xstream Compatible.
 - **ACCESS Rack** - On the **System Settings Tab**, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, select **Zephyr Xstream**.
 - **ACCESS 2USB Portable** - Choose **Configure** then **System Settings** on the display. Under **Standard RTP Settings** select **RTP Compatibility Mode** and choose **Zephyr Xstream**.

 - b **Incoming Connections** - Zephyr Xstream sends an AAC stream to the ACCESS on UDP port 9150. These streams will be automatically decoded. By default, a return channel of AAC 96 kb/s mono is returned to the Xstream. The return channel may be altered to any Xstream-compatible mode in the **Systems Setting** section. ACCESS that do not have the AAC upgrade applied will not create a return channel.

 - c **Outgoing Connections** (ACCESS AAC Option required) - Build a profile using the **Profile Manager** on either the ACCESS Rack or Portable and select a Channel Mode of **Standard RTP**. Then choose an Xstream-compatible encoder for the outgoing call. The Xstream will control what type of stream, if any, is returned to the ACCESS.
- 3 **Standard RTP** - This mode is set to receive a basic, unformatted AAC stream within a standard RTP/UDP structure. At present, this mode does not offer compatibility with other industry devices.

xxxvii. APPENDIX B - INFORMATION FOR IT MANAGERS

The purpose of this appendix is to describe all open ports and services available on the Comrex ACCESS 2USB.

The Comrex ACCESS 2USB is a device designed to move real-time, wideband audio over IP networks. The main network interface is 1000BaseT-Ethernet. The device contains an optimized version of Linux kernel. The IP parameters are set by a computer on the local LAN using a proprietary broadcast UDP protocol.

Comrex provides a Windows or MAC application (**Device Manager**) on the included CD, or available on our website at www.comrex.com, to perform this function on the local computer. Once the unit is powered on your ACCESS 2USB, you have five minutes before this function is disabled.

IP parameters can also be changed online using the password protected **Toolbox** interface at `<ip-address>/cfg`. Updates to the system are provided by a custom online updater utility. This update process is password protected and requires access to **TCP 80** and **TCP 8081**. In addition to the password protection, the update data itself must have a valid cryptographic signature from Comrex, or else it is rejected.

INCOMING SERVICES

Port	Service	Default
TCP 22	SSH*	Off (On for products shipped before 1 July 2017)
TCP 80	HTTP control	On
TCP 443	TLS protected HTTP control	On
TCP 8081	Firmware upload	Open only during upgrade process
UDP 9000	BRIC Normal Media	On
UDP 9001	CrossLock Media	On
UDP 5060, 6014, 6015	SIP	Off
UDP 5004, 5005	Standard RTP	Off (On for products shipped before 1 July 2017)
TCP 9000	BRIC Normal/TCP	Off
TCP 8000	HTTP Media	Off

*Only SSH clients with an authorized DSA key can access SSH services on the device. Other forms of authentication are disabled. This key is kept confidentially by Comrex for factory diagnostics only. SSH services may be disabled completely via the user interface.

OUTGOING SERVICES

Service	Destination
NTP	o.comrex.pool.ntp.org:123 (UDP)
Switchboard	switchboard.comrex.com:8090, switchboard.comrex.com:8081 (secondary) (TCP)
STUN	stun.comrex.com:3478 (UDP)
DNS Lookup	DNS Server:53 (TCP and UDP)

Under most circumstances, ACCESS requires an IP path in both directions for successful connections, even when audio is only being sent one-way. For networks that provide data only in one direction, it is possible to use Standard RTP mode to establish and maintain these links. This section describes how to set that up.

The following setting applies to both codecs in the link (encoder and decoder):

The codec has several compatibility modes under the Standard RTP channel mode. The units default to a mode that is compatible with the Luci Live PC-based encoder. This must be changed on both codecs.

- 1 On the ACCESS Rack, enter the Web-based User Interface and choose the **System Settings** tab. On the ACCESS 2USB Portable choose **Configure->System Settings**.
- 2 Find the **Advanced** tick-box and check it.
- 3 Find **Standard RTP Settings** and choose to edit the **RTP Compatibility mode**.
- 4 Change this setting to **Standard** and click **Apply** (or **Save** on ACCESS 2USB Portable).

DECODE SIDE SETTINGS ONLY

Also under **Advanced Standard RTP Settings**, find the **Return Channel Enable** entry. Disable the return channel and click **Apply** (or **Save** on ACCESS 2USB Portable). This will make sure that no channel will be set up in the direction to the encoder.

ENCODE SIDE SETTINGS ONLY

Obviously, connections of this type must be established from the encoding side of the link. So you'll need to build a new Profile that uses the **Standard RTP** channel mode under the Profile Editor. Choose your outgoing encoder along with any other special attributes in the profile editor. Name the Profile something descriptive like "Simplex".

Next, create your outgoing remote entry in the address book. Apply the new profile to that entry. Any connection made with that entry will connect in a unidirectional fashion.

FULL-TIME OR TRIGGERED CONNECTIONS

A remote entry using a unidirectional profile can still utilize the tools required for automatic connection.

To set up a connection to be "always active" (i.e., reconnect in the case of power outage or network failure), choose that connection on the **System Settings Tab** as the **Always Connect To** location.

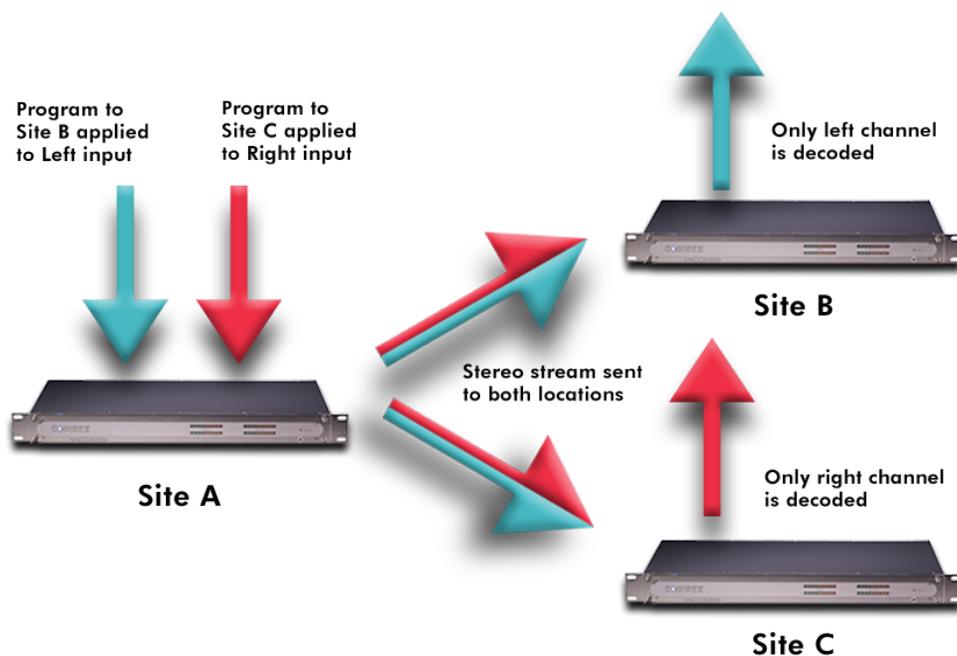
To trigger the connection when an external contact is closed, choose the connection under one of the **Contact Closure** settings on the **System Settings** tab.

xxxix. APPENDIX D - USING THE COMREX ACCESS DECODER DOWNMIX FUNCTION

ACCESS allows a stereo connection profile to instruct the ACCESS decoder to decode only one side of a stereo channel. This is useful in a scenario where two mono connections need to be sent to two different destinations simultaneously.

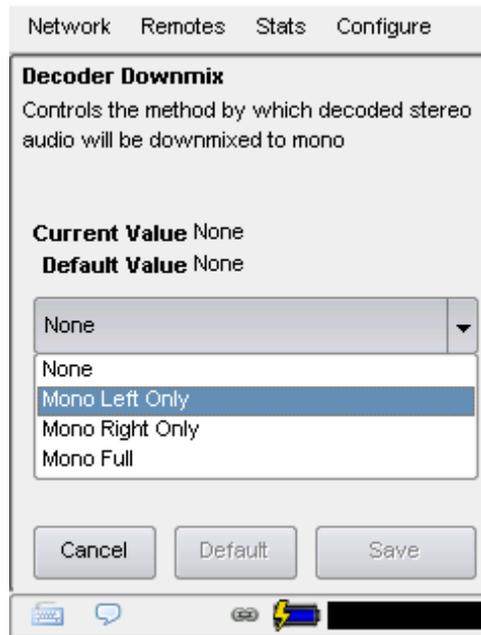
ACCESS has the ability to run a single instance of an audio encoder. But the user can create multiple profiles using that encoder to change behavior of either end of the link. The new option instructs the decoder to selectively output only Left or Right channel of an incoming stereo feed. By applying at least two different profiles to the outgoing connections, the system can effectively send only Left channel audio to one destination, and only Right channel to another.

Use of the decoder downmix function has two drawbacks: As with all multi-streams in ACCESS, full duplex operation is only supported to one destination. Also, both channels of the stream are actually delivered to both destinations over the network, utilizing more incoming network bandwidth to the decoder than necessary.



The figure above shows a typical connection using the Decoder Downmix function from the encode site (A) to two decode sites (B and C). For clarity, no return audio channel is shown from either B or C (although one could exist from either but not both).

The user at site A builds two separate connection profiles, each using the same local stereo encode option. They will turn off the remote encoder on both profiles. On the profile labeled “**Downmix L**”, under advanced options, they will go to the remote connection side and select “**Downmix**”. Here they will instruct the remote decoder to output only “**Mono Left Only**” through both Left and Right audio outputs.



The user will build corresponding “**Downmix R**” profile, selecting the “**Mono Right Only**” option in the same location.

On the **Remotes** list, the user at site A will apply the “**Downmix L**” profile to the remote connection targeted to receive the Left audio channel (site B), and the “**Downmix R**” profile to the other (site C).

Using this scenario, two independent channels can be sent to two independent locations using a single ACCESS codec on the transmitting end. This function can also be used in a “round-robin” contribution application, where multiple remote reporters are all interested in adding to a conversation, and still be able to hear each other. This scenario is a bit more complex, but is aided greatly by use of the Vortex Hotswitch application. This is described in more detail in a separate appnote, Round-Robin Remotes with Comrex ACCESS.

XL. APPENDIX E-SPECIFICATIONS

CONNECTIONS

- Power: 5-pin DIN female, pins 3+5 +15V, pins 2+4 ground
- Mono In: 3-pin XLR female, pin 1 ground, pin 2 +, pin 3 –
- Stereo Line In: 1/8" (3.5 mm) female, tip=left, ring=right, sleeve=gnd
- Line Out: 1/8" (3.5 mm) female, tip=left, ring=right, sleeve=gnd
- Headphone Out: 1/8" (3.5 mm) female, tip=left, ring=right, sleeve=gnd
- Mobile In/Out: 1/8" (3.5 mm) female, tip=send, ring=receive, sleeve=gnd
- Serial: 8-pin DIN female, pinout in Section 2
- Contact Closures: 9-pin DIN female, pinout in Section 2
- USB: USB Type A
- Ethernet: 8-pin modular, 100baseT wiring

AUDIO SPECIFICATIONS

Mono Input

Type: Balanced

Impedance: Mic: 20k Ohms (pins 2-3)

Line: 200k Ohms (pins 2-3)

Level: Mic: -60 dBu nominal, -15 dBu max

Line: 0 dBu nominal, +20 dBu max

Stereo Line Input

Type: Unbalanced

Impedance: 9k Ohms (tip to sleeve, or ring to sleeve)

Level: -10 dBu nominal, +10 dBu max

Line Output

Type: Unbalanced

Impedance: 0 Ohms (tip to sleeve, or ring to sleeve)

Level: -10 dBu nominal

Mobile In/Out

Type: Unbalanced

Level: Send: -45 dBu, Receive: -20 dBu

Frequency Response: Varies with algorithms, see descriptions

POWER

Voltage: AC: 100-240 VAC, 50-60 Hz

DC: See Section 3.

Power: 24 Watts with all peripherals

PHYSICAL

Dimensions (w/ battery): 4.75" W (12.1 cm), 8.25" D (21 cm), 2.5" H (6.35 cm)

Weight: Unit alone with battery: 2.2 lb (1.0 kg)

Shipping: 6 lb (2.7 kg) with all peripherals and packing

APPENDIX E - CONNECTIONS TO MULTIRACK

The purpose of this appendix is to describe how to make connections to Comrex ACCESS MultiRack.

BRIC NORMAL CONNECTIONS

The Comrex ACCESS MultiRack allows users to make up to 5 separate AES67 connections. This feature allows additional setup including the assignment of separate UDP ports for each MultiRack Instance. UDP 9000 is the default port for BRIC Normal connections. Instance #1 on MultiRack will use the UDP 9000 port by default. Comrex generally recommends End Users with MultiRack then use UDP 9002-9005 for instances #2-5 respectively, leaving UDP 9001 open for Crosslock.

When making Remote Entries for MultiRack, each instance needs to be its own separate entry. For BRIC Normal connections, this is done by entering the Public IP Address the MultiRack is behind followed by “:9000” for instance #1, and “:9002”, “:9003”, “:9004, and “:9005” for instances #2-5 respectively. For example, Creating a BRIC Normal entry for instance #3 on a MultiRack would read: “<IP ADDRESS>:9003”.

MANUAL CROSSLOCK CONNECTIONS

Manual CrossLock connections require special configuration options on both sides of the link. This primarily involves programming the Switchboard ID for each unit (or primary Ethernet MAC Address) into the outgoing settings on the codec on opposite side of the link. This process for outgoing calls is described above. What isn't mentioned is also important: the MAC/Switchboard ID of the outgoing unit must also be programmed into the unit receiving the call.

Note that MultiRack instances #2-5 have special Switchboard IDs consisting of the primary Ethernet MAC followed by a suffix (e.g., 00:01:0c:c0:78:19-4 for instance #4).

This is done by creating an outgoing connection describing the far-end unit, even if it is never actually used for outgoing calls. In the case of this “dummy” entry, it's not actually important for the IP address field of the far-end unit to be correct. The entry must be enabled for CrossLock operation and it must have the correct Switchboard ID/ MAC address of the far-end unit.

In the special circumstance where the default CrossLock port of UDP 9001 can not be used (e.g. several MultiRack codecs sharing a single IP address), then manual CrossLock connections get extra complex. For more information on these settings, refer to the Technote “Making CrossLock connections on non-standard Ports”.

Note: *Comrex devices must be running at least Firmware version 4.5 to designate MAC Address suffixes when making Manual Crosslock Remote Entries.*

MAKING CONNECTIONS WITH SWITCHBOARD

In order to use Switchboard, users must first have an account with the server. This account can be obtained by contacting Comrex at 978-784-1776 / 800-237-1776, or by emailing techies@comrex.com / info@comrex.com. Only one account is required for each group of codecs. Once a user name and password are provided, navigate to switchboard.comrex.com in a web browser. When first accessing Switchboard, there will be a notice stating that no units have been added to the account. By clicking on **Add New Unit**, a dialogue box will ask for the Ethernet MAC address of the MultiRack.

When adding MultiRack to your Switchboard Account, each instance must be added individually as a separate device. The primary Ethernet MAC address is used here only for MultiRack instance #1. Each instance must be added to Switchboard individually. Instances 2-5 use the same MAC address (Switchboard ID) with a suffix (e.g. -2, -3, -4, and -5) added to designate the instance.

As an example, if the primary Ethernet MAC Address is 00:01:40:c0:0d:15, that's the ID input for MultiRack instance #1. Instance #2 is added as 00:01:40:c0:0d:15-2, instance #3 uses -3, etc.

ACCESS MultiRack Audio Codec	Control Room Instance 3 [REDACTED]-3	Idle
ACCESS MultiRack Audio Codec	Control Room Instance 4 [REDACTED]-4	Idle
ACCESS MultiRack Audio Codec	Control Room Instance 2 [REDACTED]-2	Idle
ACCESS MultiRack Audio Codec	Control Room Instance 5 [REDACTED]-5	Idle

FIGURE 75 MULTIRACK INSTANCE ENTRIES IN SWITCHBOARD

XLI. COMREX SWITCHBOARD TRAVERSAL SERVER USE

You have purchased a product from Comrex that uses the **Switchboard TS** (Traversal Server) to provide the ability to locate Comrex hardware via the Internet and to aid in the making of connections when certain types of NAT routers are involved in the link. **Switchboard TS** consists of two distinct elements: the firmware that functions within the codec hardware to enable use of the function; and a server deployed on the Internet which provides the services to the codec hardware.

The purchase you have made entitles you only to the firmware elements within your codec that utilize these functions. The functions of **Switchboard TS**, as implemented in your codec, are warranted to work as described (according to standard Comrex warranty terms found in your User Manual) when used with a properly functioning Traversal Server deployed on the Internet.

Comrex has deployed and provided you account details for a **Switchboard TS** account on our server, located at [**http://switchboard.comrex.com**](http://switchboard.comrex.com).

Comrex provides this service, free of charge and at will. As such, Comrex offers no warranty as to availability of this server or of its function. Comrex reserves the right to discontinue availability of this service at any time. Comrex also reserves the right to remove any account from the server at [**http://switchboard.comrex.com**](http://switchboard.comrex.com) at any time for any reason. In no way shall Comrex be liable for this server's malfunction, lack of availability, or any resultant loss therein.

The software that runs the Comrex **Switchboard TS** on the Internet is available from Comrex in an executable format, free of charge, with basic instructions on how to set it up. The address of the server used for these functions is configurable in the codec firmware. If you wish to deploy your own **Traversal Server**, contact Comrex for details on obtaining this software.

Comrex is not liable for training or support in setting up a TS server, and the software is available without warrantee or guarantee of suitability of any kind.

XLII. LICENSE AND WARRANTY DISCLOSURES

FOR COMREX ACCESS

LICENSES

MPEG-4 audio coding technology licensed by Fraunhofer IIS

<http://www.iis.fraunhofer.de/amm/>



Fraunhofer
Institut
Integrierte Schaltungen

ACCESS uses proprietary and open-source software programs. Some of the open-source programs are licensed under the Gnu Public License (GPL). For more information on GPL see <http://www.gnu.org>.

As per the GPL, source code for this software is available on request from Comrex on CD-ROM or other electronic format. To obtain this software please contact our support department at +1 978 784 1776. We retain the right to charge a small handling fee for distribution of this software.

ACCESS makes use of open-source and/or free software with the following copyright restrictions:

ncurses

Copyright © 1998, 1999, 2000, 2001 Free Software Foundation, Inc.

See further Copyright notice below

dropbear

Copyright © 2002-2004 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

See further Copyright notice below

libxml2

Copyright © 1998-2003 Daniel Veillard. All Rights Reserved.

See Further Copyright notice below

Import code in **keyimport.c** is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Further copyright notice for ncurses, dropbear PuTTY and libxml2

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights

to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Libpcap
tcpdump

Copyright © 1988, 1989, 1991, 1994, 1995, 1996, 1997

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

WARRANTY

All Equipment manufactured by Comrex Corporation is warranted by Comrex against defects in material and workmanship for one year from the date of original purchase, as verified by the return of the warranty registration card. During the warranty period, we will repair or, at our option, replace at no charge a product that proves to be defective, provided you obtain a return authorization from Comrex and return the product, shipping prepaid to Comrex Corporation, 19 Pine Rd, Devens MA 01434 USA. For return authorization, contact Comrex at 800-237-1776 or 978-784-1776 or email techies@comrex.com.

This warranty does not apply if the product has been damaged by accident or misuse or as a result of service or modification performed by anyone other than Comrex Corporation.

The next two paragraphs apply to all software contained in this product:

WITH THE EXCEPTION OF THE WARRANTIES SET FORTH ABOVE, THE PRODUCT (MEANS COLLECTIVELY THE HARDWARE AND SOFTWARE COMPONENTS) IS PROVIDED STRICTLY "AS-IS." COMREX CORPORATION AND ITS SUPPLIERS MAKE NO WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR WARRANTY AGAINST LATENT DEFECTS. COMREX CORPORATION AND ITS SUPPLIERS DO NOT WARRANT THAT THE PRODUCT IS ERROR-FREE, THAT ALL ERRORS MAY BE DETECTED OR CORRECTED, OR THAT THE USE OF THE PRODUCT WILL BE UNINTERRUPTED. IN NO EVENT WILL COMREX CORPORATION AND ITS SUPPLIERS BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE RESULTING FROM THE USE OF THE PRODUCT INCLUDING LOSS OF PROFITS, LOSS OF SAVINGS, LOSS OF USE OR INTERRUPTION OF BUSINESS EVEN IF COMREX CORPORATION OR ANY OF ITS SUPPLIERS HAS BEEN ADVISED OF THE POSSIBILITY OF SAME. IN NO EVENT SHALL COMREX CORPORATION AND/OR ITS SUPPLIERS' TOTAL LIABILITY TO YOU REGARDLESS OF THE FORM OF ACTION EXCEED THE AMOUNT YOU PAID AS PART OF THE PURCHASE PRICE OF THIS PRODUCT. COMREX CORPORATION AND ITS SUPPLIERS MAKE NO WARRANTY, EITHER EXPRESSED OR IMPLIED, THAT ANY USE OF THE PRODUCT WILL BE FREE FROM INFRINGEMENT OF PATENTS, COPYRIGHTS, OR ANY OTHER THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

THE SOFTWARE OWNED BY COMREX CORPORATION OR BY ITS SUPPLIERS RESIDING IN OR OTHERWISE ASSOCIATED WITH THIS PRODUCT ARE PROTECTED UNDER COPYRIGHT LAW AND INTERNATIONAL TREATIES. UNAUTHORIZED REVERSE ENGINEERING, REPRODUCTION AND/OR DISTRIBUTION OF THE PRODUCT OR ANY PORTION THEREOF, IS STRICTLY PROHIBITED AND MAY RESULT IN CIVIL AND CRIMINAL SANCTIONS, AND WILL BE PROSECUTED TO THE FULL EXTENT OF THE LAW. COMREX CORPORATION AND ITS SUPPLIERS OWNS AND SHALL RETAIN ALL RIGHT, TITLE AND INTEREST IN AND TO ANY SOFTWARE SUPPLIED TO YOU IN AND AS PART OF THE PRODUCT AND ALL INTELLECTUAL PROPERTY RIGHTS RELATED THERETO. THE SALE OF THE PRODUCT SHALL NOT BE CONSTRUED IN ANY MANNER AS TRANSFERRING ANY RIGHT OF OWNERSHIP IN ANY SUCH SOFTWARE.

XLIII. CONFORMITY INFORMATION

SUPPLIERS U.S. DECLARATION OF CONFORMITY

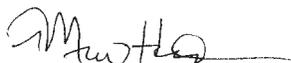
Place of Issue: Devens, Massachusetts

Date of Issue: April 4, 2007

Equipment: Comrex ACCESS 2USB Portable

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

Individual plug-in devices for wired and wireless connectivity will have their own certifications from their manufacturers. Information is available on each device's label.



Thomas O. Hartnett, Technical Director, Comrex Corporation

EC DECLARATION OF CONFORMITY FOR R&TTE DIRECTIVE

We:

Manufacturer's Name: Comrex Corporation

Manufacturer's Address: 19 Pine Road
Devens, MA 01434
U.S.A.

hereby declare on our sole responsibility that the product:

**Comrex ACCESS 2USB Portable
Digital Audio Codec**

to which this declaration relates is in conformity with the essential requirements and other relevant requirements of the R&TTE Directive (1999/5/EC). This product is compliant with the following standards and other normative documents:

European EMC Directive (89/336/EEC)

EN 55022:1998/A1:2000, Class A Conducted and Radiated Emissions

EN55024: 1998/A1:2001/A2:2003 (Immunity, ITE Equipment)

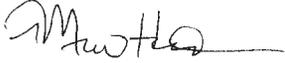
Low Voltage Directive (2006/95/EEC)

EN 60950-1: 2001

Individual plug-in devices for wired and wireless connectivity will have their own certifications from their manufacturers. Information is available on each device's label.

Information regarding configuration of this equipment for operation on the telephone networks of the EC countries may be found in the Comrex ACCESS 2USB Portable product manual.

Contact person: Thomas O. Hartnett, Technical Director

Signed:  _____

Date: 04 April 2007