BRIC-Link

Product Manual

COMREX

BRIC-Link Manual

ABOUT COMREX

Comrex has been building reliable, high quality broadcast equipment since 1961. Our products are used daily in every part of the world by networks, stations and program producers.

Every product we manufacture has been carefully designed to function flawlessly, under the harshest conditions, over many years of use. Each unit we ship has been individually and thoroughly tested.

Comrex stands behind its products. We promise that if you call us for technical assistance, you will talk directly with someone who knows about the equipment and will do everything possible to help you.

You can contact Comrex by phone at 978-784-1776. Our toll free number in North America is 1-800-237-1776. Product information along with engineering notes and user reports are available on our website www.comrex.com. Our email address is info@comrex.com.

WARRANTY AND DISCLAIMER

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 return authorization from Comrex and return the product, shipping prepaid, to Comrex Corporation, 19 Pine Road, Devens, MA 01434 USA. For return authorization, contact Comrex at 978-784-1776 or fax 978-784-1717.

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

With the exception of the warranties set forth above, Comrex Corporation makes no other warranties, expressed or implied or statutory, including but not limited to warranties of merchantability and fitness for a particular purpose, which are hereby expressly disclaimed. In no event shall Comrex Corporation have any liability for indirect, consequential or punitive damages resulting from the use of this product.

I. INTRODUCTION

The Comrex BRIC-Link is a low-cost, high-performance solution for audio-to-IP conversion. Leveraging many of the core technical aspects of Comrex's successful remote broadcast BRIC-Link product line, the BRIC-Link provides for an elegant way of moving Linear or compressed audio with very low delay. BRIC-Link may be used over a range of IP links, is very simple to use, and doesn't require the expense of more full-featured codecs. While it carries an entry-level cost, BRIC-Link maintains superb audio specifications and hardware reliability, making the system suitable for STLs and other mission-critical functions.

BRIC-Link is contained in a small desktop package. Two BRIC-Links may be installed to occupy 1RU of rack space.

APPLICATIONS

The BRIC-Link is uniquely suited to point-to-point "nailed up" high-quality audio links over a variety of data networks, like ISM band IP radios, T1s, satellite channels, WANs, and LANs. The robustness of the BRIC Normal technology (Broadcast Reliable Internet Codec) used in the box allows the system to perform well on the public Internet as well (using AAC or Opus compression modes).

AUDIO CODING

For users concerned about delay and coding artifacts, the BRIC-Link offers a robust stereo or mono Linear mode that does not compress audio. In addition, unique to real-time audio codecs, BRIC-Link offers FLAC lossless compression, reducing network throughput by 30-40% with absolutely transparent coding and no tandem coding concerns. For situations where further reduced bandwidth is desired, BRIC-Link offers AAC/HE-AAC modes as standard, allowing superb audio quality at dramatically reduced data rates. For compatibility with mobile phone and web applications, BRIC-Link also implements Opus audio compression, along with VoIP standard G.722.

TRANSMISSION MODES AND DELAY

The BRIC-Link is a true codec, offering a full-duplex stereo encoder and decoder in each unit. When two-way transmission is not required, the reverse channel may be disabled. The BRIC Normal technology incorporated includes a jitter buffer manager that automatically balances delay and stability, dynamically increasing and decreasing delay based on network performance. For networks where QoS is known, these parameters may be set to maintain a consistent level of jitter buffer.

End-to-end coding delay in Linear modes is less than 25 ms. Delays when using FLAC and Opus modes are less than 30 ms. AAC modes incorporate around 100 ms total end-to-end delay while HE-AAC modes deliver around 220 ms.

In addition to coding delay, network propagation and jitter buffers will add delay to any IP link and are network dependent.

SWITCHBOARD SERVER

Switchboard is a standard feature with BRIC-Link that allows the codec to "sync" with Comrex's cloud-based traversal server. **Switchboard** facilitates connections between codecs without any knowledge of IP addresses on either end of a link. Switchboard traversal server allows for monitoring presence and status information for all Comrex codecs in a user's fleet, and assists with connections through routers and firewalls that might be difficult otherwise. **Note:** BRIC-Link requires the one-time purchase of a Switchboard Traversal Server License for use with Switchboard.

CROSSLOCK

BRIC-Link comes with a reliability feature called CrossLock VPN. Comrex codecs running 4.x-level firmware and higher are compatible with CrossLock. This is a transport layer that adds the following features:

- Error Correction (ARQ and FEC);
- Dual Network support (Bonding and Redundancy modes);
- Enhanced statistics and diagnostics.

Use of **CrossLock** is optional, and requires a Comrex codec running 4.x-level firmware on each end of the link. **CrossLock** connections can be made via the Comrex **Switchboard** function (see previous section) or manually. For manual connections, **CrossLock** requires extra settings to assure connections are only made within your known group of codecs. 4.3-level firmware and higher also supports **CrossLock** when using very data-intensive algorithms like Linear PCM and FLAC.

Users running 4.3-level firmware or higher are also able to utilize **HotSwap**, which is a feature of **CrossLock** that allows users to designate one network in a **CrossLock** connection as *primary* and the other network as *secondary* in order to increase flexibility and avoid potentially expensive data overage charges.

ADDITIONAL FEATURES

HTML5

Previous firmware versions for Comrex codecs provided a web-based control page powered by Adobe Flash. As Flash has lessened in popularity and impedes operation on many mobile browsers, BRIC-Link (and older Comrex products with new firmware) now delivers web-based control using the modern HTML5 standard.

II. BRIC-LINK DIAGRAMS AND INSTALLATION

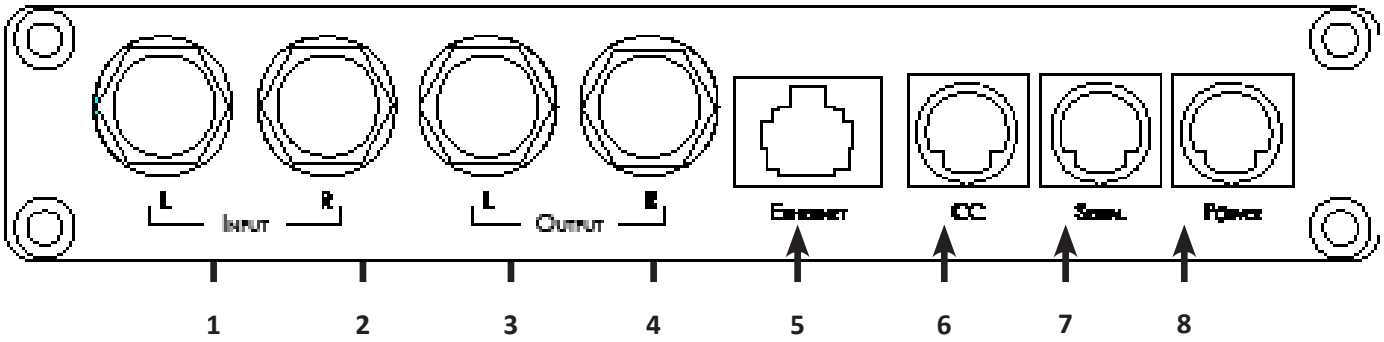

FIGURE 1 **REAR**

PANEL DIAGRAM AND DESCRIPTIONS

1 **Left Audio/AES3 Input** - Accepts professional level, balanced analog audio, or if configured, AES3 stereo digital audio for input.

2 **Right Audio Input** - Accepts professional level, balanced analog audio.

3 **Left Audio/AES3 Output** - Delivers professional level, balanced analog audio, or if configured, AES3 stereo digital audio for output.

4 **Right Audio Output** - Delivers professional level, balanced analog audio.

5 **Ethernet 10/100baseT** - Connection for network connections.

6 **Contact Closures** - Provides for 4 contact closure triggers, and 4 open-drain style contact closure outputs.

7 **RS-232** - Provides serial data I/O across the IP link. Data rate is configurable.

8 **Power** - 4-Pin connector for attachment of Comrex approved DC power adapter. Requires 24 V DC @ 1 A.

FIGURE 2 **PANEL DIAGRAM AND DESCRIPTIONS**

9 **DIP Switches -** 8 individual DIP switches allow selection of certain operational parameters (see **DIP Switch Settings** on **Page 16**).

10 **Left/Mono I/O Level Indicator -** Tri-color LED shows left channel input or output level.

11 **Right I/O Level Indicator -** Tri-color LED shows right channel input or output level.

12 **Ready/Status LED -** Bi-color LED shows Ethernet carrier loss (Red) or valid connection state (Green).

13 **Reset Button -** Issues a hardware reset to the system when pressed momentarily.

PINOUTS - BALANCED AUDIO

Stereo professional level connections are available on the rear panel via ¼" TRS-style connectors for left and right input and output. Adapters are provided to convert these connections to XLR. For analog connections, the jacks are wired as follows:

1 Sleeve - Ground

2 Tip - Balanced Audio +

3 Ring - Balanced Audio -

These connectors have a fixed level where a full scale signal represents +20 dBu (22 Vpp). A nominal input level of 0 dBu (2.2 Vpp) is recommended.

PINOUTS - AES3

A nominal input level of 0 dBu (2.2 Vpp) is recommended. When configured via the DIP switches, the left input and output become AES3 digital ports. The jacks connectors are wired as follows:

1 Ground

2 AES3 +

3 AES3 -

To use AES3, the front panel DIP switches must be set appropriately. AES3 input connections can be at 32, 44.1 or 48 kHz. The front panel DIP switches must be set appropriately. On the BRIC-Link, the output audio sample rate automatically locks to the input sampling rate. If analog input is used, (or AES3 input configured and unconnected), AES3 output is always 48 kHz.

Because BRIC-Link 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

In mono encode modes, BRIC-Link uses the left channel of the stereo input for delivery to the mono encoder.

OUTPUTS

In stereo decoder modes, left and right channels are delivered to the output connectors separately. In mono decoder modes, mono audio is delivered to both left and right output connectors.

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.

Pin #	Function	Direction
1		
2		
3	TX Data	From BRIC-Link
4	Ground	
5	RX Data	To BRIC-Link
6		
7		
8	Ground	

PINOUTS - CONTACT CLOSURES

Contact closures are available via the 9-pin mini-DIN connector on the rear panel of the BRIC-Link. 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.

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

DIP SWITCH SETTINGS

BRIC-Link has a set of eight DIP switches used for audio and indicator configuration.

DIP Switch #	Function	Default (Down)
1	Analog/AES3 Input Select	Analog
2	Analog/AES3 Output Select	Analog
3	Audio Loopback*	Disabled
4	Level LEDs TX/RX Select	TX
5	Headphone out select TX/RX	TX
6-7	Future Use	
8	Factory Reset	

RESET TO FACTORY DEFAULT USING DIP SWITCHES

To factory reset your device using DIP switches, follow these steps:

1. Put DIP switch 8 up.
2. Press the RESET button once, then wait until the Left, Right, and Power LED flash red and green (can take up to 40 seconds).
3. Put DIP switch 8 down.
4. Press the RESET button once.

III. QUICK START-MAKING CONNECTIONS WITH BRIC-LINK

This section skips over many of the details concerning the configuration of remote connections with BRIC-Link, and focuses instead on the minimum information needed to establish a connection. BRIC-Link connections with the use of the Switchboard server will be covered.

MORE ABOUT PROFILES

Refer to **Page 31** for more information about creating profiles on BRIC-Link. Profiles, once created, can be assigned to any remote connection on the Connections page. BRIC-Link ships with several popular profiles pre-programmed by default, and has the ability to create custom profiles. For the purposes of this Quick Start, use the system default profile, which won't require changes to the factory default settings. This factory-default profile uses the Opus mono encoder in both directions of the link.

LOGGING IN

After determining the IP Address of the BRIC-Link, open any computer's web browser on the same network as BRIC-Link. Type the IP address in the browser URL to navigate to the BRIC-Link's web interface. Log in to BRIC-Link with any user name and, if it has not been changed, the default password "comrex" (lowercase).

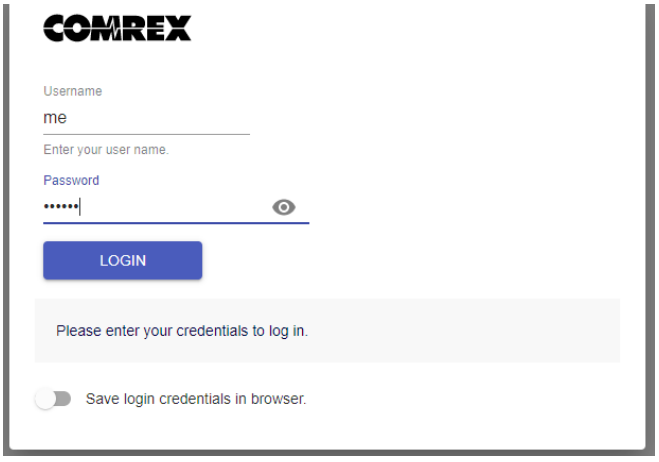

FIGURE 3 **WEB INTERFACE LOGIN**

MAKING SWITCHBOARD CONNECTIONS

On the Web Interface, select the "Connections" Tab. This Tab will populate with a list of available remote codecs to call. When the BRIC-Link is "synced" with Switchboard, connections to other codecs in a user's Switchboard account are simple. Go to the listings on the bottom that appear with a "Gear" icon on the left side. Any units with a Green

Gear icon are available for Switchboard connections. Highlight them and select the “Connect” button on the right side of the screen to initiate a connection.

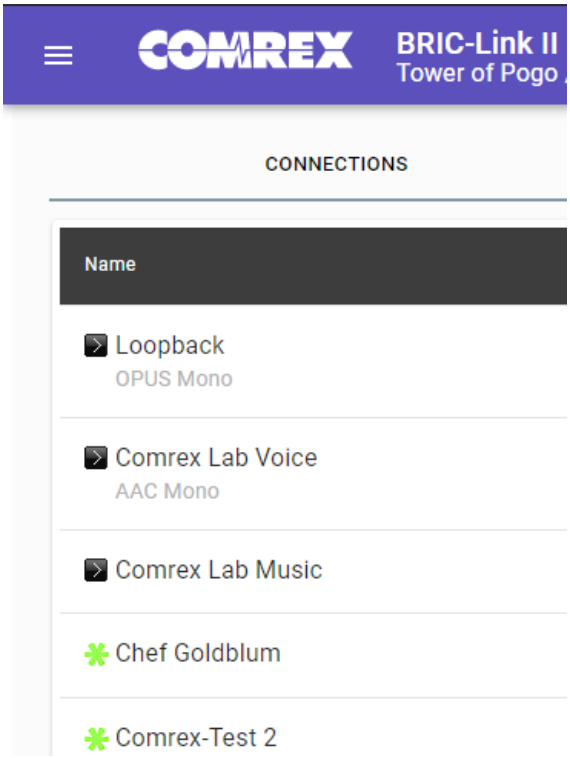

FIGURE 4 **SWITCHBOARD CONNECTIONS ICONS**

RECEIVING INCOMING CONNECTIONS

By default, BRIC-Link is set to automatically answer incoming calls, whether or not Switchboard is used to make them. Incoming calls will appear in your connections list while they are active. They can be disconnected locally by highlighting them and clicking “Disconnect”.

FIGURE 5 **ACTIVE SWITCHBOARD CONNECTION**

IV. USING THE DEVICE MANAGER PROGRAM

Firmware updates for the BRIC-Link should be handled using Comrex **Device Manager**, a Windows- and MAC OS-executable program that can be downloaded from the Comrex website. **Device Manager** can also be used for license installation and IP configuration.

Please note: In order to configure a BRIC-Link unit for the first time (without knowing the unit's IP address), **Device Manager** must be run on a computer located on the same network (e.g. physical LAN connection) as the unit itself. If this is not possible, an Ethernet crossover connection between the BRIC-Link and a computer should be used for configuration.

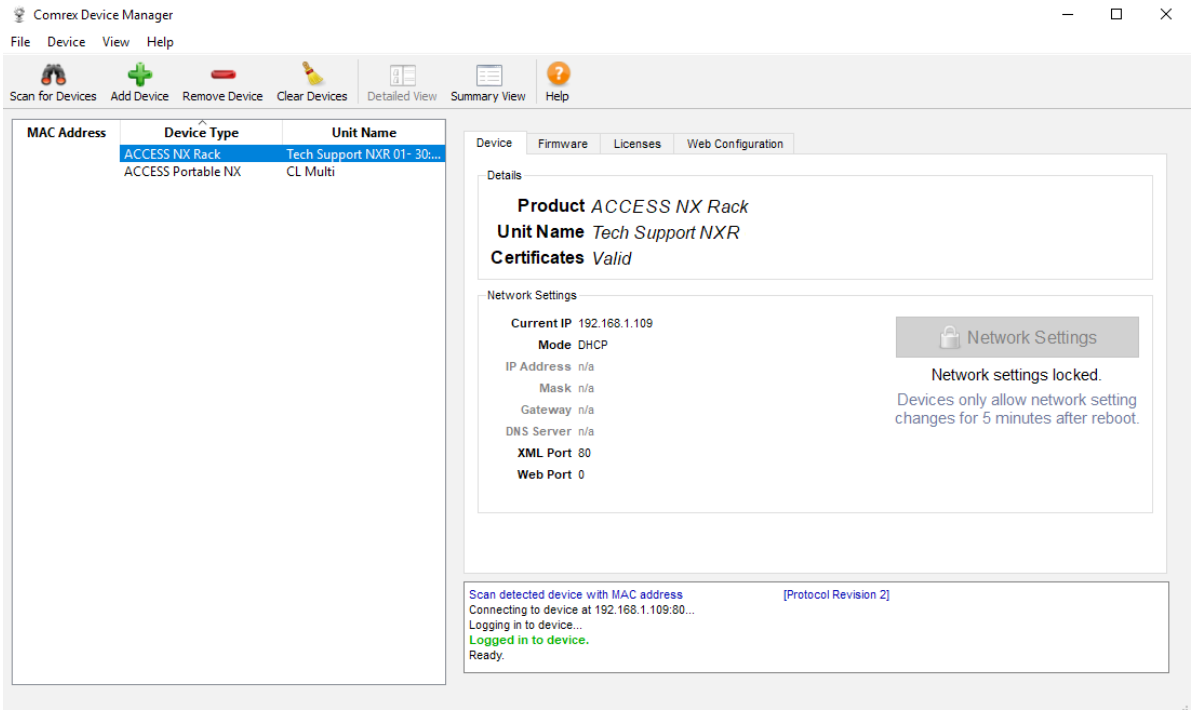

FIGURE 6 **DEVICE MANAGER**

As shown in **Figure 6**, running the **Device Manager** and clicking the "**Scan**" button will produce a list of all Comrex devices found on the LAN. If the default password has changed, **Device Manager** will prompt for the password to BRIC-Link after the scan.

Figure 6 shows the four tabs that appear on the right-hand pane after **Device Manager** has logged in. The fourth tab is labelled **Web Configuration**. This will open a simplified setup interface on the BRIC-Link called **Toolbox**. The **Toolbox** interface allows for configuration of several options including the Ethernet port. Log in to **Toolbox** with a username (any) and password (default = **comrex**) to enter the **Toolbox**.

Once logged into **Toolbox**, choose the **Network/Admin/CrossLock** option and then choose **Set up Ethernet**. Choose the Ethernet port that appears in the list, which will look like **Figure 7**.

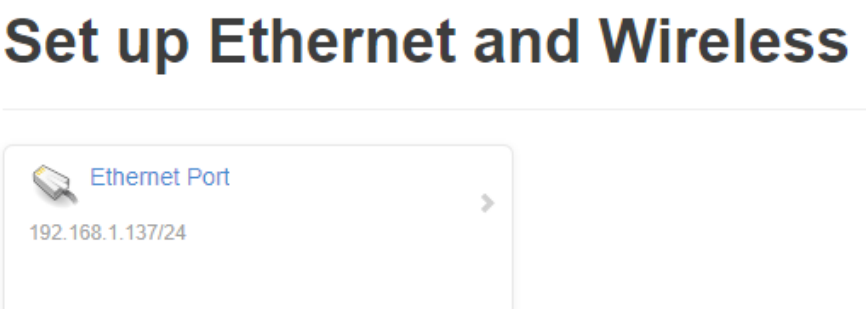

FIGURE 7 **SET UP ETHERNET AND WIRELESS**

Generally, it is recommended to configure the Ethernet port of a BRIC-Link for a static IP. This will facilitate access to the **Web-based Interface** with a browser and allow for easier configuration of routers or firewalls (if necessary). If the BRIC-Link is to be installed on a managed LAN, Comrex recommends consulting with the IT services provider about obtaining a static IP address.

As mentioned in the previous section, the BRIC-Link is configured for **DHCP** by default. This means that it tries to extract an unused IP address from the network router upon booting. To change the Ethernet IP addressing to **static**, select the "**default**" location at the bottom of the list and change the "**IP Type**" to **static**. The system will prompt a list of static settings as shown in **Figure 8** (on the following page).

As can be seen in **Figure 8,** the *static IP address*, *the Netmask*, *the Gateway Address*, and at least one *DNS Server Address* must be configured in the proper fields to set a static IP address. Once that information has been inputted, click the "**back**" button and select **Apply Changes** to have the BRIC-Link accept and activate the new Ethernet settings. Note that if the IP settings of the Ethernet port have been changed, the connection to the **Toolbox** interface will no longer work. Click the "**Scan**" button on **Device Manager** to re-sync with the new IP address.

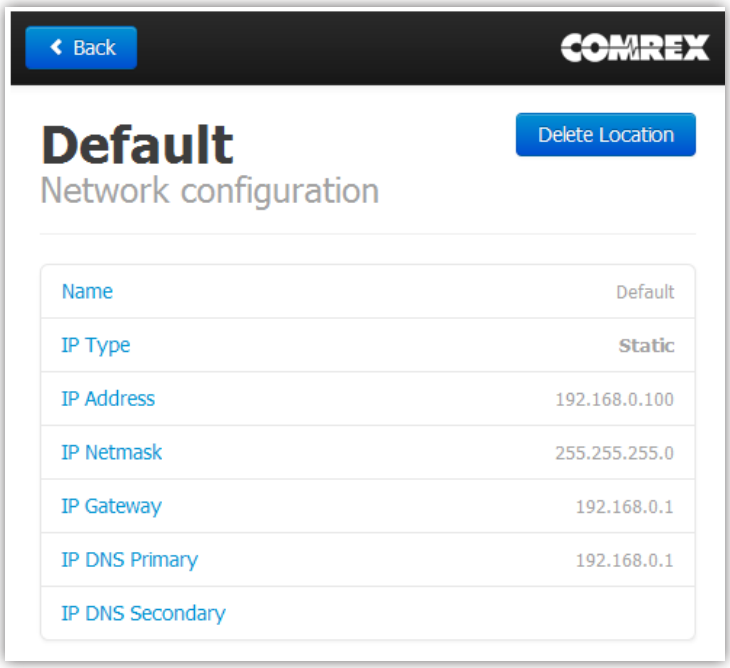

FIGURE 8 **NETWORK CONFIGURATION**

UPDATING FIRMWARE USING DEVICE MANAGER

While Device Manager is open and synced to a codec, it's a good time to check to see if an update is available for the product.

To do this, select the Firmware tab, shown in **Figure 9** below.

The unit's current firmware and the most recent version of firmware for the unit are listed at the top of the tab (**1** in **Figure 9**). If the device isn't running the latest version of firmware, click the "Get Latest Version" button (**2** in **Figure 9**) and download it. (If the unit's Firmware is current, the button will be grayed out.) Next, select "Update Device" (**3** in **Figure 9**), choose the .upd file just downloaded and click OK, and Device Manager will then update the unit's firmware.

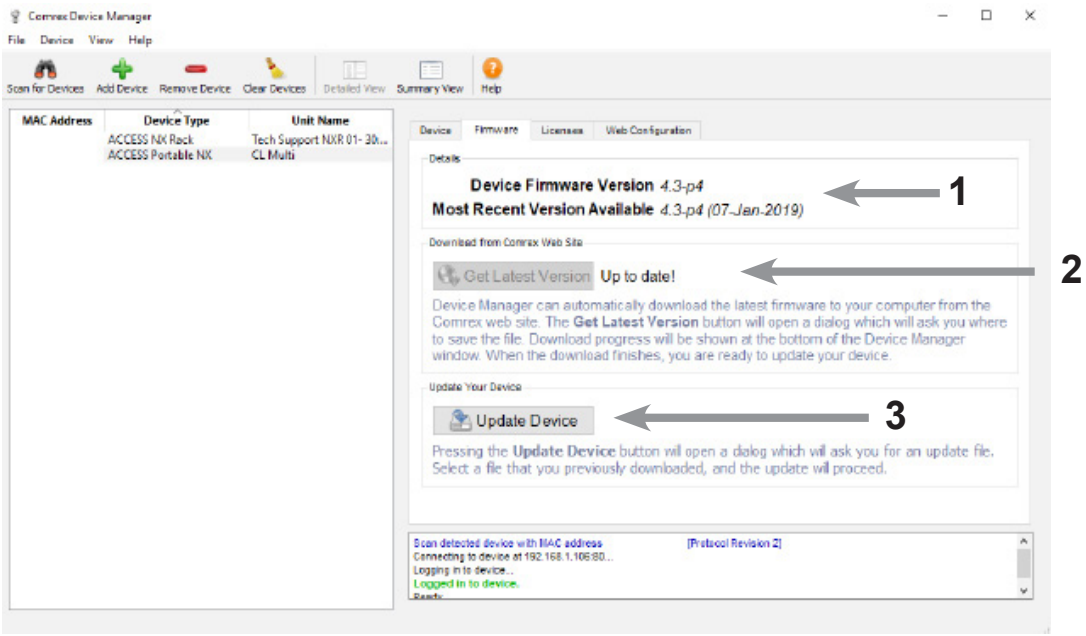

FIGURE 9 **FIRMWARE TAB**

NETWORK RECOVERY MODE

Since the Ethernet settings are made with a web connection, keying in incorrect static IP information can result in losing access to the **Network Manager** interface entirely. If this happens, it is possible to be "locked out" of the unit (i.e., unable to log in). **Device Manager** has a network recovery tool to help with this: **Network Recovery Mode**.

For security reasons, **Network Recovery Mode** is only available during **the first five minutes** after a BRIC-Link unit has (re)booted. Once those five minutes have elapsed, the unit will need to be rebooted in order to perform network recovery.

Figure 10 shows **Network Recovery Mode**. The "**Scan**" button has shown the presence of a BRIC-Link on the network. On the "**Device**" tab on the right pane, the "**Network Settings**" button is activated and a countdown timer is started. Selecting this will allow changing of the primary Ethernet settings in the same way as Toolbox.

Once the IP address is set up via the **Device Manager**, the rest of the setup and operation of the BRIC-Link is done via the **Web-Based Interface**. This process is addressed in the following section.

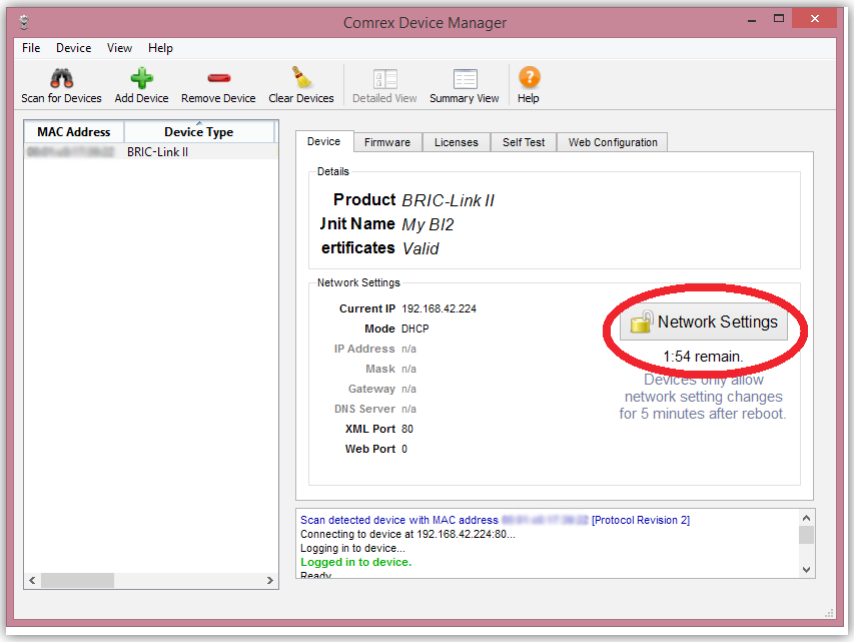

FIGURE 10 NETWORK RECOVERY MODE

V. CONFIGURING THE BRIC-LINK

LOGIN

Upon connection to the BRIC-Link, a login screen will appear, **Figure 11**. Any username can be chosen with the default password: **comrex**. This will access the **Main User Interface** display.

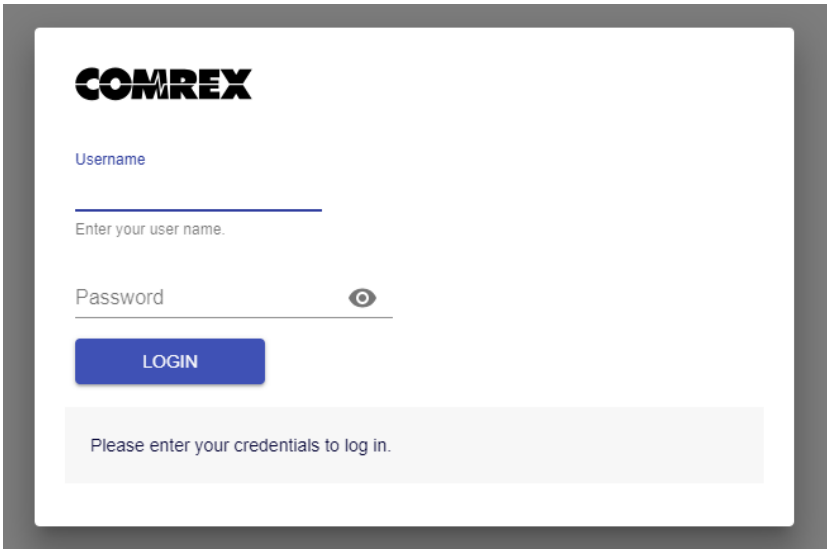

FIGURE 11 **WEB INTERFACE LOGIN**

INTERFACE PAGE SECTIONS

There are two parts to the primary interface screen (**Figure 12**):

- **Main Audio Meter** (**1**): This meter displays audio levels for active connections to the BRIC-Link.
- **Configuration Tabs** (**2**): The primary focus of the BRIC-Link configuration interface. These tabs consist of Connections, Dashboard, Performance, Profile Manager, and System Settings to control and obtain status of BRIC-Link. They are described in detail in the following sections.

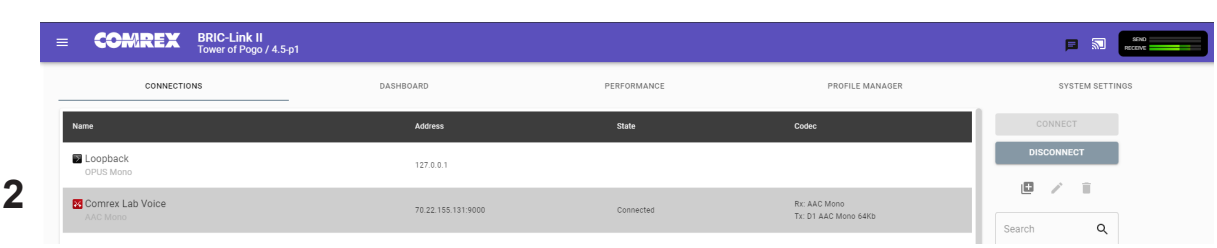

FIGURE 12 **CONNECTIONS TAB**

CONNECTIONS TAB

The **Connections** Tab is the first window in the configuration interface. This allows for monitoring device connectivity and controlling connections. In this tab the names and IP addresses of remote units can be saved. To add a new remote unit to the list, select the "**+**" icon on the right side of the list. A dialogue box will appear asking for a name for the unit, as well as its IP address. An algorithmic profile must be selected for the new codec unit. To get started, choose one of the default profiles provided. Custom profiles are possible and are covered in a later section. In the event that a stored unit is no longer desired, it can be deleted through the **Trash Icon** option.

The **Connections** tab will display **Name** and **Status** information of a remote Comrex codec when it has initiated a connection to the BRIC-Link. Information from units connected this way will only appear while the connection is active.

By default, three remotes appear on the list. These remotes are used for troubleshooting connectivity and include:

1. **Loopback** - Allows for localhost, testing the connection of the rack and remotes on the network.
2. **Comrex Lab Voice** - This provides a talk feed from the Comrex headquarters in Massachusetts, USA for testing network connections.
3. **Comrex Lab Music** - This provides a music feed from the Comrex headquarters in Massachusetts, USA for testing network connections.

DASHBOARD TAB

The Dashboard Tab is designed to be open during active connections (**Figure 13**). It provides a quick view of some vital parameters for use during live streaming.

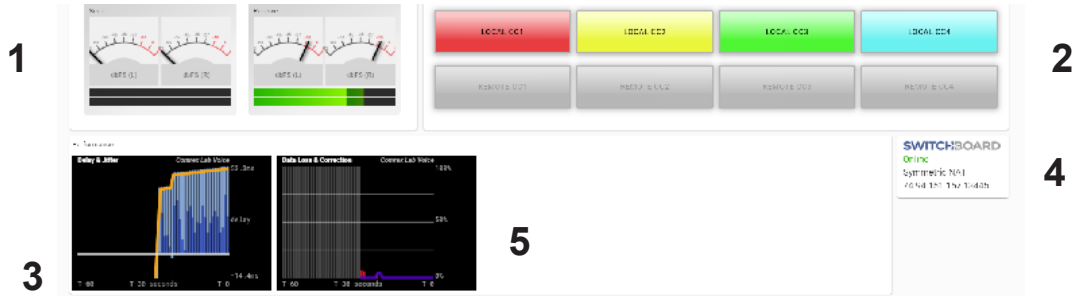

FIGURE 13 **DASHBOARD TAB**

1. The audio level meters give a quick indication of send and receive levels.
2. The Contact Closure section gives a visual indication of the state of each input (local) and output closure (remote). The input closure boxes also function as buttons to trigger closures locally.
3. The Active Connections section gives an indication of any currently active connections. If more than one connection is active, they will display in a list here.
4. Switchboard status, Public IP, and router information are displayed in the status box.
5. A quick view of the codec's receive stats are presented in the lower section. This is similar to the statistics presented under the Performance->Active Connection described in the next section.

PERFORMANCE TAB

The Performance Tab includes information on data transmission and reception rates from BRIC-Link to active remote connections. This allows for real-time monitoring of network quality during connections.

ACTIVE CONNECTIONS

Clicking the header "Active Connection" will show a basic chart of real-time codec receive performance. Channel Statistics, as shown in **Figure 14**, will give numeric statistics for the current active call. If several calls are active (Multistreaming), each will appear in a separate section.

Active Connection

Remote Unit	Duration	RX Rate	RX Overhead	RX Delay	TX Rate	TX Overhead	TX Delay	Frame Loss	Remote Loss
Nagelfar	00:00:43	1.2kbps	16kbps (93%)	12ms	48.4kbps	16kbps (24%)	29ms	0%	0%

FIGURE 14 **CHANNEL STATISTICS**

Figure 15 displays a real-time graph. This shows only statistics for the incoming data of the local codec. If a connection does not use the optional CrossLock reliability layer, this graph will be the only real-time network graph available. CrossLock connections also display the CrossLock statistics graph, which has more information.

FIGURE 15 **JITTER/PACKET ERROR GRAPH**

The left graph represents the work of the **Jitter Buffer Manager**. The area of most interest is the light blue area as shown in **Figure 15**, which illustrates a spread of jitter values (referenced to the current play out 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, less jitter is 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 Jitter Buffer Manager is shown by the yellow line, which is the target buffer delay that the system is trying to achieve, based on measurements calculated over the jitter window.

The right side of the 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 the percentage of lost packets over the one-second interval.

CODEC CHANNEL FIELD

Clicking on the Codec Channel field delivers information on the BRIC-Link's total receive rate and transmit rate, including information for multiple connections when applicable. When multiple transmit connections are active, this will show an aggregate rate of all outgoing connections (**Figure 16**).

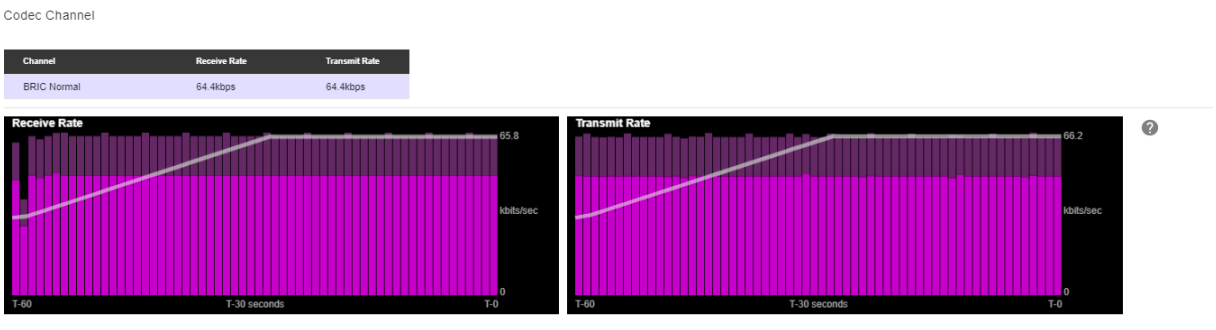

FIGURE 16 **CODEC CHANNEL**

CROSSLOCK FIELD

Clicking on CrossLock opens a set of real-time graphs which monitor the status of the optional CrossLock reliability layer. These fields will not appear when non-CrossLock connections are active. These stats are a powerful tool for monitoring and diagnosing the quality of connections, as well as for managing the delay settings during the connection.

The CrossLock Stats are similar to the information available on the Active Connections graph, which shows streaming performance without regard to the CrossLock layer. The CrossLock Stats show finer details about network performance in both directions than can be obtained through the Active Connections graph. CrossLock stats are shown for both the data being transmitted from the local codec and the data being received by the local codec. All relevant stats are available for both directions.

PACKET LOSS GRAPH

Figure 17 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 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 play out. **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.

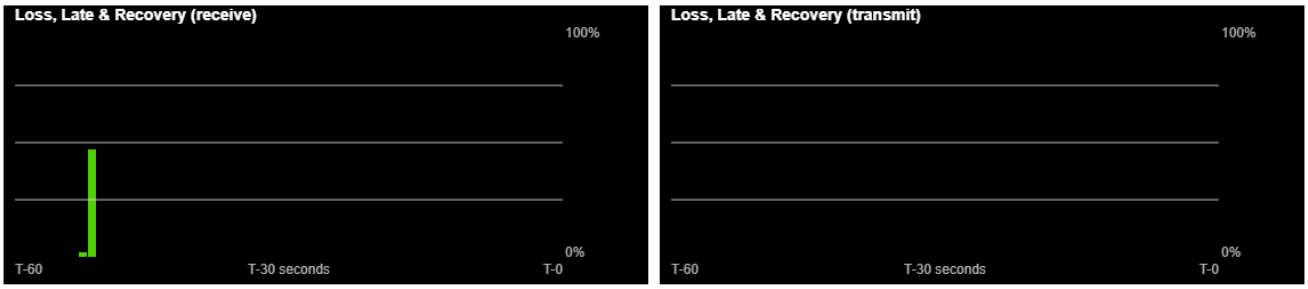

FIGURE 17 **PACKET LOSS GRAPH**

UTILIZATION GRAPH

Figure 18 contains 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 possible that the size of these bars will vary because CrossLock (in some modes) has control over data rate through a technique called "throttling". Based on network feedback statistics, CrossLock will reduce or 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 on the under graph. Overlayed on the network utilization graph is a gray line. This is the encoder target rate, which reflects the bitrate chosen in the profile used in the connection. This is treated as a maximum value, so utilization should mostly remain below this line.

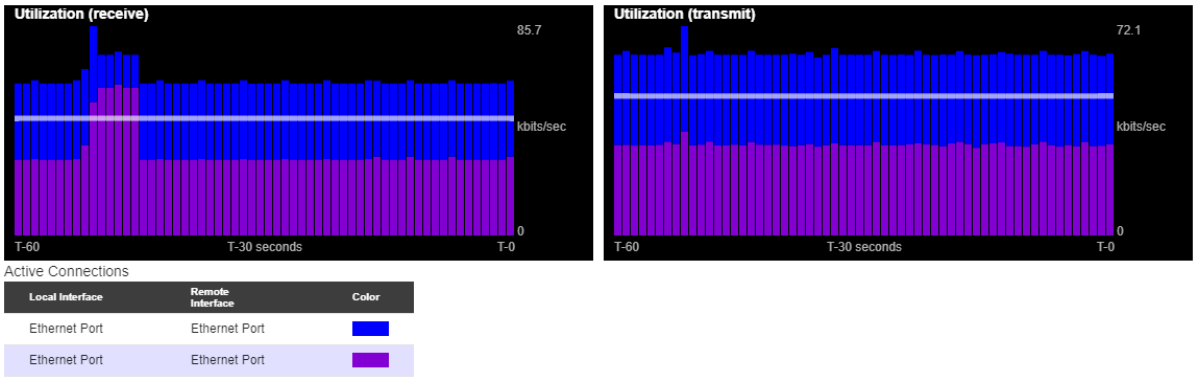

FIGURE 18 **UTILIZATION GRAPH**

CROSSLOCK SETTINGS

Clicking the CrossLock Settings field during an active connection will display the CrossLock sliders. There is a slider available for transmit and receive operation.

For most CrossLock connections, the sliders should be left at their default Automatic Delay Mode settings. But during connections on unusual networks, these sliders are designed to quickly adjust the current delay settings. The sliders will reset when a CrossLock connection ends.

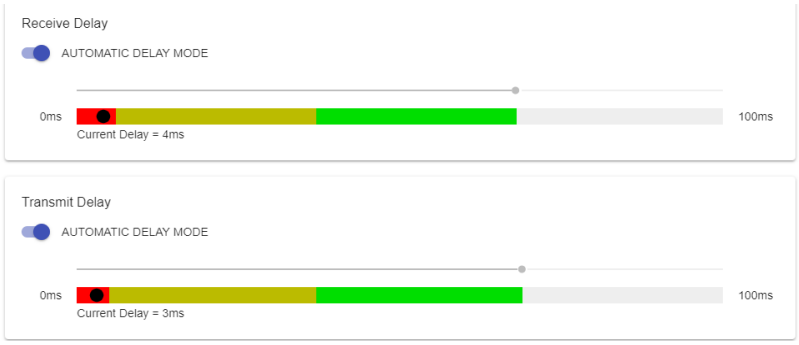

FIGURE 19 DELAY SLIDER BARS - AUTOMATIC DELAY MODE

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). CrossLock uses a combination of decode delay buffering and error correction to keep connections stable.

At the start of a CrossLock connection, the sliders are in “Auto Delay” mode and the information on the sliders 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 with a mouse. 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 overlayed on the slider, to signify delay “zones” of safety.

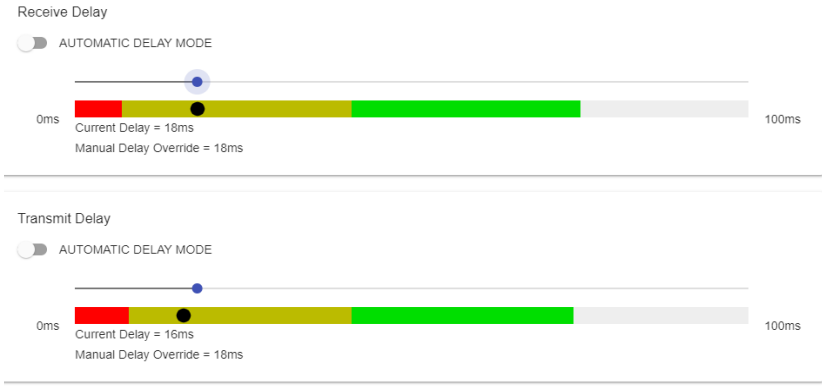

FIGURE 20 DELAY SLIDER BARS - MANUAL DELAY MODE

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, the dark dot signifies the “Current Delay”, which is the best compromise value calculated by the system to balance stability and delay. By changing the “Automatic Delay Mode” switch to manual, the “Target Delay” indicator can be dragged left or right to override the automatic settings, and increase or decrease the delay.

Please note: Any settings made in Manual Mode will be erased after the current CrossLock session is terminated. In order to make delay buffer changes permanent, use the settings in the Profile Manager as outlined in the unit manual.

PROFILE MANAGER TAB

BRIC-Link provides a powerful set of controls to determine how it connects. The **Profile Manager** tab (**Figure 21**) allows the definition of one or more profiles to assign to outgoing remote connections. It is often unnecessary to create any new profiles since BRIC-Link ships with a set of factory-default profiles that cover most users. This tab allows for creating custom profiles when necessary. Please remember, though, that these profile settings only apply to connections initiated from BRIC-Link. Incoming connections from another unit are defined by that unit’s profile settings.

Profile creation is segmented into commonly used and advanced options. In order to simplify the interface, **Advanced Options** are normally hidden from the user. Please note: Building a profile doesn’t change how any remotes are connected *until that profile is assigned to a remote on the* **Connections** *tab*. Once a profile is defined, it will be available on the **Connections** tab to be assigned to any defined connection.

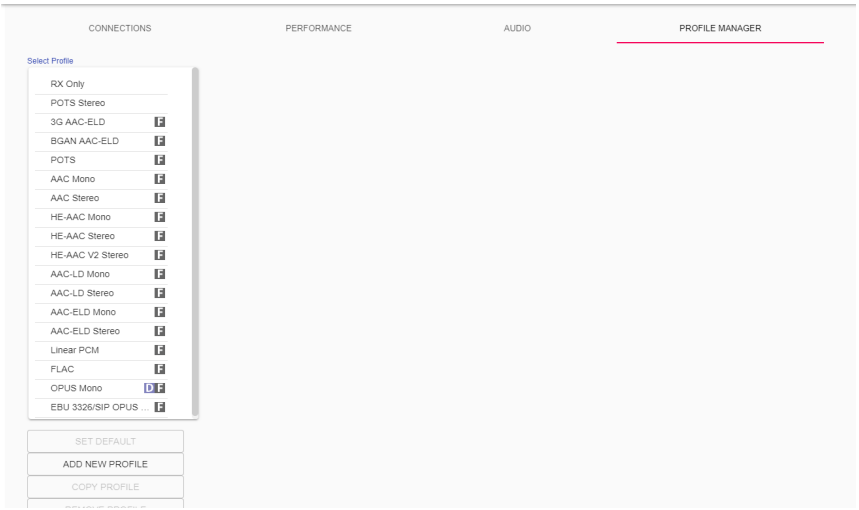

FIGURE 21 PROFILE MANAGER TAB

BUILDING A PROFILE

To build a new profile, select **Add New Profile** (**1** in **Figure 22**), and a new profile (labelled **New Profile)** will appear on the list. Select it to populate a set of options, starting with the profile Name (**2** in **Figure 22**). Here the profile can be renamed to something easier to remember.

Next is the **Channel** option (**3** in **Figure 22**), which allows for selecting between a standard Comrex IP connection (BRIC normal) or one of the other connection modes offered by BRIC-Link. Note that when using the CrossLock reliability layer, BRIC Normal mode is chosen here, as this is the protocol that runs with the CrossLock VPN.

Other Channel options include a modem-based connection, IP Multicast (a method to deliver audio to multiple locations), EBU3326/SIP for compatibility, and less often used protocols like standard RTP, TCP, and HTTP. Different aspects of these channel types are described in later sections.

Note: It's important to define the channel of a profile before moving on to other options, since the choices in the subsequent sections will vary based on this choice. Make sure to press **Apply Changes** in order to confirm each change made.

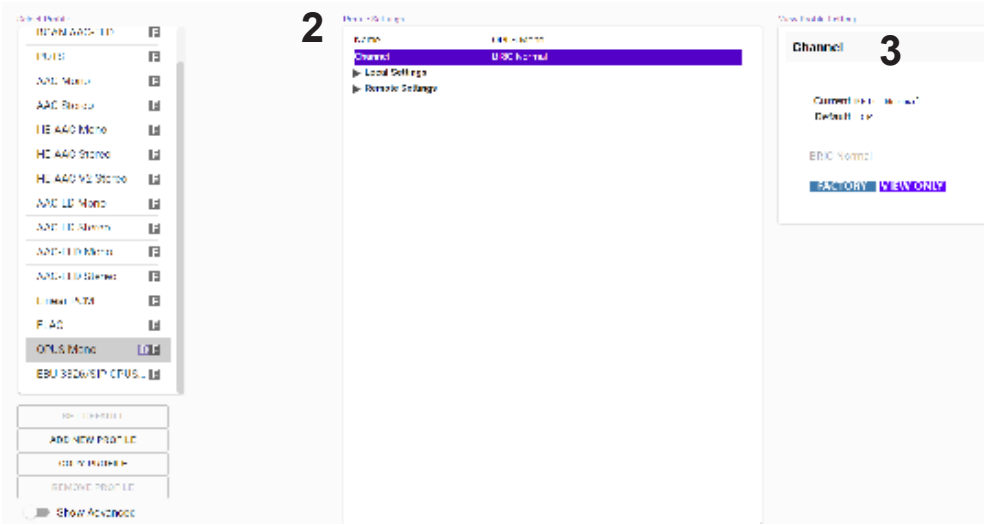

FIGURE 22 **PROFILE MANAGER TAB**

PROFILE SETTINGS: LOCAL & REMOTE ENCODERS

When choosing an IP-based channel (i.e., BRIC Normal), users will be presented with two categories of options: Local and Remote. The Local Settings are used to determine how a transmitting BRIC-Link behaves, and the Remote Settings will determine how the receiving Comrex codec on the far end behaves. Each category lists identical options, so only Local Settings will be covered.

Connection Timeout - Under normal circumstances, a connection will be terminated on one end, and the other end will drop the connection in turn. However, if a network failure occurs or a connection is ended abruptly (e.g. because the power to one unit was unexpectedly killed), the system will drop the connection after a predetermined time. The default is 60 seconds, but this can be shortened or lengthened as desired. If an indefinite connection is necessary, refer to **Operating BRIC-Link in a 24/7 Environment** on **Page 65** for additional information.

Encoder - It is unnecessary to define any decoder types when using Comrex codecs because they automatically adapt to the incoming stream. Using this menu, users can select the encoder used to send audio from this BRIC-Link (local) as well as the encoder used to send audio to this BRIC-Link (remote). The default value of the remote encoder is to follow the local encoder (i.e., it will send exactly the same codec mode it receives). This is defined as Follow Mode in the remote encoder selection table. See the **About the Algorithms** section on **Page 68** for more information on selecting encoders.

Transmit On/Off - This option determines whether the selected encoder (local or remote) is actually sending any data. By default, Transmission and Reception on all encoders is turned on, but there may be circumstances where one-way operation is desired (e.g. **Multistreaming**, as described on **Page 71**). Turning off the local encoder transmission disables ***outgoing*** audio, and disabling the remote encoder transmission disables ***incoming*** audio.

ADVANCED LOCAL & REMOTE OPTIONS

The following advanced options apply to both the local and remote entries, and largely deal with the performance of **Jitter Buffer Manager**. This is actually a very complex decision-making process involving many variables, and most of the time the default parameters should work well. These advanced options are a means of overriding these defaults, and Comrex recommends that users take care when changing them. Note that when it comes to settings that effect the jitter buffer manager, local settings affect the decoder on the local side, and remote settings affect the decoder on the remote end.

Frames per Packet - This function allows the encoder to wait for variable "**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 packet overhead bits like IP and UDP headers are sent less often.

Decoder Downmix - This option controls the method by which decoded stereo audio will be down-mixed to mono.

Loss Cushion - Packets may arrive at the decoder displaying a range of statistical properties. They may arrive in reasonably good timing and in order, or half may arrive quickly with the other half delayed significantly. In some cases, most of the packets arrive in a timely manner, but a small percentage of them may be extremely late. It is usually preferable to allow these late packets to be left out of the stream entirely and keep the delay lower. The decoder error concealment hides these packet losses. The **Loss Cushion** parameter instructs the buffer manager to ignore a certain percentage of late packets in its calculation. The default value is 5%. Applications that are not delay-sensitive may wish to reduce this value to zero, while extremely delay-sensitive applications may prefer to have this closer to 25%.

Retransmit Squelch Trigger - Retransmit Squelch options are used to determine how the buffer manager reacts to typical data dropouts like those seen on wireless networks. The Trigger option determines the amount of time the decoder must experience 100% packet loss before the Retransmit Squelch function is triggered. Default is one second.

Retransmit Squelch Max - The longest period of data loss during which the squelch function is active. Default is two seconds). During the squelch period, the buffer manager ignores the relative jitter experienced and does 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 jitter buffer manager works to keep absolute delay to a minimum. Some applications are not delay-sensitive and rely less on the jitter buffer manager. The **Delay Cushion** setting is a way to instruct the manager not to attempt to drive the delay below a certain value. (For example, if the delay cushion is set to 500 ms, this 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 go below the 0.5 second level.

Delay Limit - The inverse of the **Delay Cushion**, this parameter instructs the manager not to 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, but use of the delay limit can result in very poor performance if the network jitter dramatically exceeds the limit.

Jitter Window - This parameter defines the amount of time (in minutes) that historical network performance is analyzed in order 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 and the buffer manager reacts (perhaps by increasing the buffer), the event will be included in the manager's calculations for the next five minutes. If the network experiences improved performance over this period, the manager may choose to wind the buffer back down after the five minutes has passed.

Buffer Management On/Off - This is a diagnostic setting used to troubleshoot buffer manager performance by the factory. For usage, it should always remain "on".

CrossLock Managed Delay - There are two ways BRIC-Link can calculate its target delay, and, therefore, how much decoder buffer to add. The first is the BRIC-Normal way, and is the default for **non**-**CrossLock** connections. Buffer size is set based on a histogram of past jitter performance. This will incur the shortest delay possible. For **CrossLock** connections, the buffer is increased to allow the use of error correction, so buffer is thus based on a combination of the jitter histogram, and the round-trip delay as calculated by the system. This will generally result in bigger decode buffers (and higher delays). Because it is lower, the default setting is to use the jitter histogram for all connections. This setting allows the profile user to use alternately the **CrossLock** "error correction friendly" setting, for connections where delay is less important.

The following three settings are available to users in BRIC Normal mode. They are legacy settings for use in non-CrossLock connections. Most users should leave these settings as-is, because they can interfere with CrossLock connections. CrossLock settings now incorporate these functions.

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 a license to step down to a lower encode data rate if desired. This will happen

automatically and with no audio interruption. Step down congestion avoidance is not enabled in the Linear PCM mode.

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 when appropriate above the base UDP level. This UDP reliability is useful on some wireless connections that have unsatisfactory performance due to packet loss.

Max Retransmission Rate - This parameter places 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. For example, if an 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.

SYSTEM SETTINGS TAB

The **System Settings** tab defines parameters that are not specific to a particular remote connection. Examples are how incoming calls are handled, codec name, and assignment of contact closures. The **System Settings** tab is shown in **Figure 23**, and has several categories: **Security**, **Connections**, **Contact Closures**, **Switchboard Server**, **Crosslock VPN, System Clock,** and **Alternate Modes**. As with the **Profiles** tab, basic options are shown by default, and less frequently used settings are hidden until the **Show Advanced** option is selected.

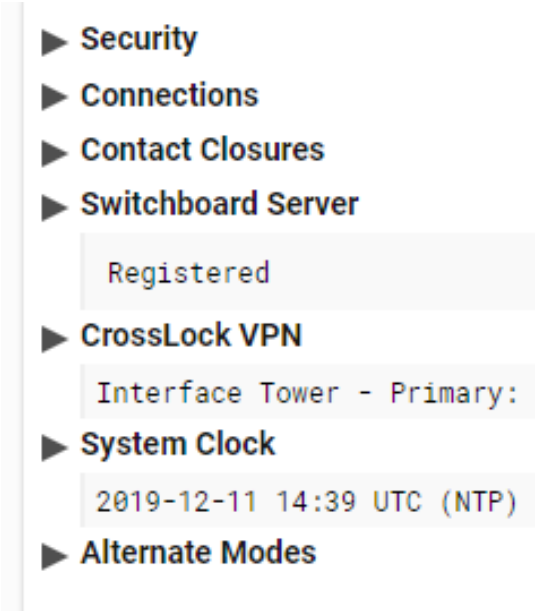

FIGURE 23 **SYSTEM SETTINGS TAB**

SECURITY SETTINGS

Remote Control Password - This allows for a defined password for the web GUI and firmware updates. The default password is **comrex** (lowercase).

CONNECTIONS

Unit Name - Users are encouraged to name their codecs here. The default name of a codec is the unique Switchboard ID (MAC address) of the unit. By changing this to something familiar and unique (e.g. roving reporter, weather guy, etc.), you will see this name change reflected in several places:

1. In the browser used to show the remote control page;
2. In Comrex-provided utility software such as **Remote Control** and **Device Manager**;
3. In Switchboard Traversal Server Buddy lists.

Incoming Connection Password - This allows users to define a password that must be attached to all incoming connections before they are accepted. Remote units placing outgoing connections to BRIC-Link must know this password and apply it to the outgoing stream. Leaving the field blank will disable this function. Note: Connections made with Switchboard do not use this function.

Always Connect to Remote - This field is available to designate a remote for "always on" operation. This is useful in "nailed up" environments, where a signal is required across the link 24 hours a day. To assign an *always on* remote, simply pull down the menu and select which remote to designate as **Always On**. A connection will be made and sustained to the chosen remote. Remote connections must be created in the **Connections** tab before they can be assigned to this function. Note: This functionality is not supported in Switchboard Connections.

Show Offline Switchboard Units - If enabled, shows offline Switchboard remotes in the remote list.

CONTACT CLOSURES

CC Connect Status - Allows for the activation of contact closure #4 out when connected. If this is selected, the signal follows the BRIC-Link front panel **Ready** light, and will be valid (closed) when a valid connection is present and invalid (open) when no connection is present. The additional options (CC1, CC2, and CC3) allow for assigning a particular remote that will be connected when its corresponding contact closure is engaged. To assign a remote connection to a contact closure, simply 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.

SWITCHBOARD SERVER

Switchboard Enabled - This option enables the use of Switchboard to connect to remote units. (See **Making Switchboard Connections on BRIC-Link** on **Page 47** for more information on using the Switchboard Traversal Server.)

Switchboard Address - IP address of the Switchboard server.

Secure - Enables secure connections to Switchboard Server. This is enabled by default.

Static Crosslock Peers - When using CrossLock without Switchboard, remote peers can be managed in this list.

CROSSLOCK VPN

Enable - This option enables the Crosslock VPN added reliability layer to connect to remote units. (See **Making BRIC-Link Connections Using Crosslock** on **Page 45** for more information on using the Crosslock VPN.)

Retransmit Delay - This section allows the selection of additional delay for the retransmission of lost packets when calculating auto-delay targets. The 2xRTT setting is selected by default.

Redundant Transmission - When calculating auto-delay target, allow enough additional delay for the retransmission of lost packets. The default setting is Off.

Encoder Throttle - This option will allow the system to reduce the bitrate of encoded media when network conditions deteriorate. Disabling this option will prevent the system from lowering the quality of the encoded media but will also significantly reduce the ability of the system to handle networks with variable performance. This setting is set to Yes by default.

Hotswap CC Indicator - When enabled, this setting will activate a selected contact closure when a CrossLock backup interface is configured and has become activated due to failure of the primary interface(s). This is set to Disabled by default.

Hotswap CC Unit - This setting allows users to select which unit to indicate HotSwap failover on. This is set to Remote by default and additionally includes a Local and Both selection.

SYSTEM CLOCK

NTP Enabled - Enables the use of NTP network time synchronization. This setting is set to Yes by default.

NTP Server - This allows users to set the address of the NTP server. This is set for 0.comrex.pool.ntp.org by default.

Timezone - Users can set their Timezone in this setting. This allows for inputting a User's Timezone by Region, Country, and Timezone.

ALTERNATE MODES

BRIC Normal Settings

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

EBU3266/SIP Settings

- **Accept Incoming Connections** - This determines whether incoming calls are accepted in EBU3326/SIP format (used for compatibility with other manufacturers who follow this protocol).

- **Incoming Connection Profile** - This allows users to select whether SIP calls will take place using a specific encoding algorithm. Note: If this option is chosen, only calls using the selected algorithm are allowed. Default is “None”.
- **Use SIP Proxy** - This option determines whether the SIP function is “registered” to a SIP cloud server. If this setting is enabled, then the address, user name, and password for the proxy must be added in the relevant fields.
- **SIP Proxy Address** - IP address or URL of the SIP proxy used.
- **SIP Username** - Username for logging into registered SIP server; provided by the SIP service provider.
- **SIP Password** - Password for logging into registered SIP server; provided by the SIP service provider.

ADVANCED SYSTEM SETTINGS

When the **Show Advanced Settings** option is enabled, additional options and categories are displayed.

SECURITY

Remote Control - This enables remote control and firmware update functionality. This option may be changed in the System console only, and is View Only in the Web Interface.

Remote Diagnostics - When activated, this option allows for remote diagnostics capability. The default setting is Off.

Web Server Port - This controls the port that the UI web server uses when remote control is enabled. The default setting is TCP 80.

AUXILIARY SERIAL

Baud Rate - Allows for controlling the Baud Rate of the serial port. Default is set to 9600.

Data Bits - Allows for the configuration of number of data bits. Default is set to 8.

Stop Bits - Configures the number of stop bits. Default is set to 1.

Flow Control - Allows for selection of the flow control method. Default is set to None with options for HW (RTS/CTS) and SW (XON/XOFF). This has no functional effect on BRIC-Link.

Parity - Users can select parity protection with this setting. Default is set to None with the additional options for Odd or Even.

CROSSLOCK VPN

UDP Port - Sets the UDP port used for Crosslock VPN Connections. Default is set to UDP 9001.

Permissive - Allows users to accept Crosslock connections from any unit. This is set to No by default.

Authentication - Enables the authentication of connections. Default setting is No.

Protection - Enables AES encryption and payload integrity protection to prevent tampering with or interception of the transmitted content. This option has a SIGNIFICANT system overhead. Default setting is No.

Maximum Delay - Maximum allowed target delay, in milliseconds. Set to 5000 ms by default.

FEC - Enables data loss protection. This option controls protection on data transmitted to the remote end. Disabled by default.

FEC Delay - Amount of delay to allow for FEC. Lower packet rates will require higher delay to remain effective.

Rentransmit - Enables retransmission of lost data. This option controls protection on data transmitted to the remote end.

Header Compression - Enables the compression of headers to reduce overhead, especially at lower bitrates. Default is set to Yes.

Base FEC - Applies a constant base amount of FEC sufficient to recover the specified rate of packet loss. Default is set to 0%.

STUN Server - Displays IP address of the STUN Server. Default is stun.comrex.com.

Always Connect - Allows users to attempt to maintain a VPN connection to a selected peer whenever possible. Default is set to None.

BRIC NORMAL SETTINGS

IP Port - This option defines the incoming UDP port—the number to be used for incoming IP connections. The default is **UDP 9000**. Crosslock connection is defaulted to **UDP 9001**. Note that since most BRIC-Link codecs attempt a connection on this port number, changing it can mean the remote units in the field must dial specifically to the new port number in order to connect to the BRIC-Link. An outgoing call must be made to a specific port number in the form of **IP-ADDRESS:PORT#**. For example, dialing port **UDP 5004** on the Comrex test line is formatted **70.22.155.131:5004**.

HTTP

Accept Incoming Connections - Users can set BRIC-Link to listen for and automatically answer any HTTP incoming calls. This option is set to No by default.

IP Port - This option defines the incoming UDP port—the number to be used for incoming HTTP connections. The default is TCP 8000.

Encoder - This defines the encoder used for HTTP streaming. Default is HE-AAC V2 Stereo 48 kb.

User Agent Blacklist - List of SIP user agents that are **not** allowed to communicate.

Genre - Users can define the Genre for HTTP streaming. Default value is set to Live.

Info URL - Informational URL associated with the stream. This setting is left blank by default.

Public - Allows users to define the HTTP stream as a Public Stream. Default setting is No.

STANDARD RTP SETTINGS

These settings offer several modes that allow compatibility with specific IP coding devices. For complete details, please review the **IP Compatibility** appendix on **Page 90**.

Accept Incoming Connections - Listen for and automatically answer incoming calls.

Incoming Connection Profile - Use this profile for incoming connections.

IP Port - Allows users to designate an incoming network port.

RTP Compatibility Mode - Enables compatibility with select RTP audio streaming devices.

Return Channel Enable - Enables a return channel sent back to the transmitter for incoming calls.

Return Channel Encoder - For incoming calls, this specifies the codec to be used for the return channel.

Return Channel Frames per Packet - Determines how many audio frames are included in each packet. Values over 1 will reduce network bandwidth but will increase delay. This is set to 1 by default.

Incoming Timeout - For incoming calls, this specifies time connection timeout. Set to 60 seconds by default.

EBU3266/SIP SETTINGS

IP Port - The port used by the SIP negotiation channel when using EBU3326/SIP Mode. If this port is changed, it's likely to break compatibility with other manufacturer's codecs.

User Agent Whitelist - List of SIP user agents that are allowed to communicate. **Only** SIP agents on this list can communicate with the BRIC-Link. Note: This setting is not enabled when using a registered SIP proxy.

User Agent Blacklist - List of SIP user agents that are **not** allowed to communicate.

VIP QC Password - For legacy purposes with the **VIP QC** app, which has been deprecated.

RTP IP Port - The port used for audio transfer during EBU3326/SIP mode. Since this port info is transferred during the negotiation process, it can be changed without breaking compatibility. Note: RTSP data is **always** sent and received on the port **one number higher than this**.

Public IP Override - Enable this in an environment where ports have been forwarded through a router to the BRIC-Link. SIP protocol assumes no ports are forwarded and may have trouble connecting if this function is not enabled.

Use STUN Server - Determines whether or not to use the STUN-derived address in the outgoing fields. BRIC-Link has alternate NAT Traversal ability so this is off by default.

SIP Proxy Keepalive - Defines how often the SIP proxy handshake happens when no call is present.

SIP Domain - When registering with some SIP services, a separate domain entry is required. If this is not populated, the domain of the SIP proxy entry is used.

SIP Auth Username - When registering for some SIP services, a separate **Auth Username** is required. Do **not** populate unless a specifc entry is required by the provider.

Send RTP To Source Port - A NAT Traversal function used with smartphone apps. Enabled by default.

SIP Routing - Specifically required by some SIP servers (e.g. **OpenSIPS**). Modifies the behavior of the route header.

TCP SETTINGS

BRIC-Link 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 when their profile is configured. BRIC-Link normally listens for incoming calls on both TCP and UDP ports, and chooses the first to arrive. If a TCP call is detected, BRIC-Link will attempt to use the same TCP link to transmit in the reverse direction.

Accept Incoming Connections - This allows turning TCP Auto Answer on and off. Disabling this function means only outgoing TCP calls can be established.

IP Port - Users have the option of setting the incoming TCP port number, which can be different than the UDP port number.

Note: Warnings given above about changing port numbers also apply here—calls with mismatched port numbers ***will*** *fail.*

MISCELLANEOUS

Meter Demo Mode - This setting will put the front panel LED meters into a demonstration mode. This setting is set to No by default.

VI. NETWORK MANAGER

NETWORK MANAGER

Located in the three-line “hamburger menu” in the upper left hand side of the Web-Based Interface, the Network Manager allows configuration to the network settings for BRIC-Link. Selecting Network Manager will bring up the screen shown in **Figure 24**. The available networking connections from BRIC-Link are presented on the left-hand side of the screen in the Select Network Device section. This area will populate with the available Ethernet Port used to make a Network connection. Here the IP and SSID settings for this network connection can be configured. Because there may be bandwidth, firewall, and/or security concerns involved when installing BRIC-Link on a managed LAN, Comrex **strongly** recommends that users consult their IT manager in environments where these concerns are present.

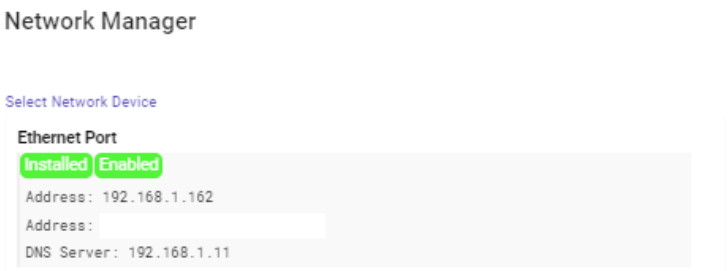

FIGURE 24 **NETWORK MANAGER MAIN SCREEN**

The primary ethernet port for BRIC-Link is configured for **DHCP** by default. In this configuration, BRIC-Link will be assigned an IP address from a pool of available IP addresses from the network router upon booting. If BRIC-Link is connected to the Internet, it should display connection information for the Ethernet Port, including IP and DNS server addresses. (If it doesn’t display this information, confirm that the unit is connected to the Internet and that the Ethernet Port is enabled.)

ETHERNET PORT SETTINGS

Select the top **Ethernet Port** (for the primary Internet) on the upper left of the screen in the **Select Network Device** section. The default configuration for the Ethernet Port will display in the **Device Settings** box as seen in **Figure 25**. This port can be renamed, as well as enabled or disabled in these settings. The Active Network Location section of the device settings will note which network configurations the unit is using for the Ethernet Port. By default, the Active Network Location will be populated with the “Default” location. This “Default” location is configured for DHCP and is initially enabled on all new units. See the next section for a description of network “locations”.

FIGURE 25 **ETHERNET PORT DEFAULT SETTINGS**

For users who wish to have a Static IP address for their units, this can be configured by editing the settings for the "Default" Active Network Location. First, select to expand the Default settings under Network Locations. Select **IP Type** to open a drop-down selection screen. This will give users the option to change the "Default" Network Location to Static IP, DHCP, or Gateway IP types as shown in **Figure 26**.

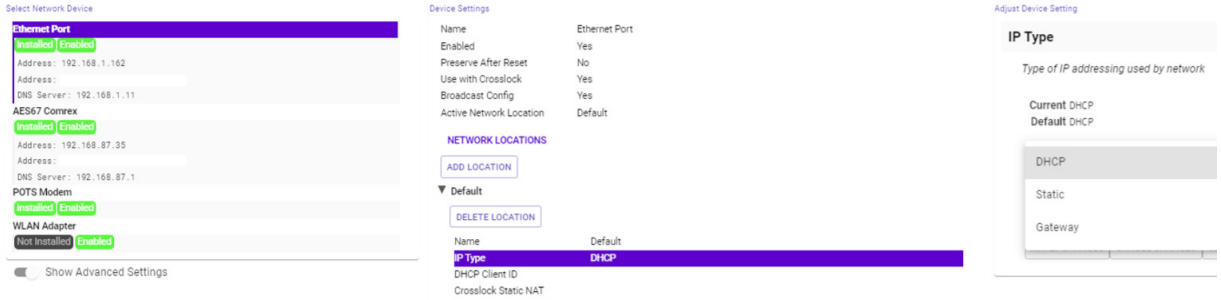

FIGURE 26 **ETHERNET PORT DEFAULT SETTINGS**

NETWORK LOCATIONS

While the "Default" setting may work for many users in a stationary environment, BRIC-Link includes **Network Location** settings for configuring different connections to different Networks known as "Locations". This allows for on-the-fly connection to different Networks by storing connection and configuration data as a Name-able Location.

To do this, select the **New Location** under the Network Location header. Change the name of the Location to something memorable and then select **IP Type** (**Figure 27)**. This controls the IP address type amongst DHCP, Static, and Gateway settings. If selecting a Static IP address, make certain to enter the unit's new **IP address**, its **Netmask**, and its **Gateway Address**, as well as at least one **DNS Server Address**.

Static Route Settings present advanced network configuration for users with complex and multilayered networks. As this is an uncommon need for most users, Comrex recommends users interested in learning more refer to the Static Routing Technical Note at www.comrex.com.

FIGURE 27 **ETHERNET PORT DEFAULT SETTINGS**

Once a Network Location has been added, it can be easily implemented through the Active Network Location selection in the **Adjust Device Settings**.

ADVANCED ETHERNET PORT SETTINGS

When **Show Advanced Settings** (in the lower-left corner) is selected, the following options also appear:

Preserve After Reset - This option ensures that changes to the unit's network configuration will be preserved even if the device is reset to factory defaults. This setting is disabled by default, and Comrex advises users to be cautious when enabling it. If the Ethernet parameters are set incorrectly, it is possible to be locked out of the BRIC-Link, and you will then have to use the **Device Manager** program's Network Recovery Mode (discussed on **Page 22**) in order to log into it.

Use With CrossLock - This option allows for specifying whether this Ethernet port will be used for **CrossLock** connections, and is enabled by default.

Broadcast Config - This option allows the unit to be identified and configured via broadcast communication on the web-based interface and **Device Manager**. It is enabled by default.

VII. MAKING CROSSLOCK CONNECTIONS ON BRIC-LINK

Comrex first introduced **CrossLock**—its technology that creates an additional reliability layer to ensure quality broadcast connections—with version 4.0 firmware in 2016. As an increasing majority of users updated their units to CrossLock-capable firmware, connections made using CrossLock became the norm for Comrex codecs and are considered standard in BRIC-Link and ACCESS Codec connections.

HOW CROSSLOCK WORKS: A BRIEF OVERVIEW

CrossLock is available on BRIC-Link and older products running at least 4.x-level firmware. To understand how CrossLock works, it's helpful to first focus on non-CrossLock connections as shown in **Figure 28**. Without CrossLock active, a codec will make BRIC Normal connections to BRIC-Link on port 9000.

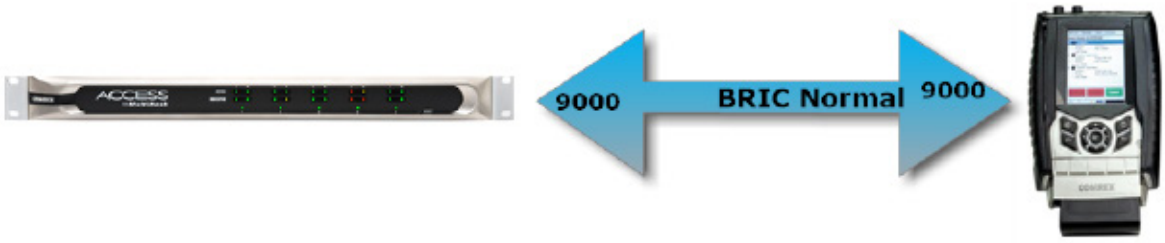

FIGURE 28 **NON-CROSSLOCK CONNECTION**

Alternatively, when CrossLock is used, it establishes a Virtual Private Network (VPN) between the hardware on both the transmitting and receiving units before a connection is established. Using this VPN, codecs can transfer much more information than is possible on Non-CrossLock legacy connections. This information includes network status, packet loss statistics, error correction parameters, media statistic information to set encoder throttle rates, and information required to establish links over multiple networks.

When enabled, the CrossLock VPN is created immediately when the first new connection is initiated, and remains for a short time after the last connection ends. In order to use CrossLock, both units in the connection must be running 4.x-level firmware or higher. CrossLock generally supports all algorithms that operate on 4.x-level firmware, but only supports data-intensive algorithms (e.g. Linear PCM and FLAC) on units running 4.3-p4 firmware or higher. As shown in **Figure 29**, BRIC Normal connections happen over the CrossLock VPN Layer. The CrossLock connection between the Comrex hardware happens over a single port (9001), but the BRIC Normal connections take place virtually on their usual legacy ports within that VPN.

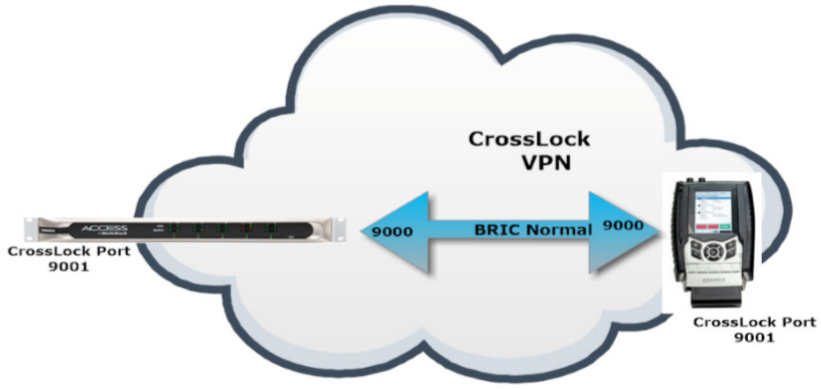

FIGURE 29 **CROSSLOCK VPN**

One limitation of CrossLock is that each codec that joins the CrossLock VPN must be familiar with the others. This process takes place automatically when Switchboard is used. As detailed in section IX, connections that don't use Switchboard need special configuration.

CROSSLOCK CONNECTIONS TO MULTIRACK

Without CrossLock active, a codec will make BRIC Normal connections to MultiRack instance #1 on port 9000. Instance #2 will connect on 9002 and instance #3 will connect on 9003. These are on the MultiRack side, and the remote codecs will all use their default ports of 9000.

The CrossLock connection between the Comrex hardware happens over a single port (9001) but the BRIC Normal connections take place virtually on their usual legacy ports within that VPN. The system will show these virtual connections happening on ports 9000, 9002 and 9003 (these are the BRIC Normal ports), but the only actual connection between hardware is happening on 9001. For this reason, if you only intend to make CrossLock connections to MultiRack, only UDP port 9001 needs to be open or forwarded.

VIII. MAKING SWITCHBOARD CONNECTIONS ON BRIC-LINK

This section describes the procedure of making and receiving connections on BRIC-Link via the Comrex Switchboard server. This is the easiest way, but not the only way, to make BRIC-Link connections. Before connections are made this way, you must set up and configure a Switchboard Account as described in **Section X**.

If you don't want to use the Switchboard server to make connections, skip this section and go to **Section IX**, Making Manual CrossLock Connections. **Note:** BRIC-Link requires a Switchboard Traversal Server License to be used with Switchboard.

Switchboard Connections can be made with or without the CrossLock protection layer. Note that this choice affects which IP ports are used for connections, so there are implications concerning firewalls and routers.

When Switchboard is used, the choice of "peers" to connect to appears in a dynamic list, as shown in **Figure 30**. Any peer showing a "gear" icon is a connectible codec. If that gear is green, the far-end is available for incoming connections.

By selecting a Switchboard peer and clicking the edit "pencil' icon on the right side, you can change several important aspects of the Switchboard connection:

1. **Use CrossLock** - Determine whether the connection will be made over the CrossLock Layer and port arrangement, or over the legacy BRIC Normal protocol and port arrangement.
2. **Connection Password** - This adds an extra layer of security to the connection. This is a password that has been programmed into the receiving codec, and will be required on the outbound side for proper connection. Since Switchboard provides its own connection filtering, passwords are not normally used in this mode.
3. **Profile** - Choose one of the factory-supplied or custom built profiles for this connection. This defines encoders used in both directions, along with a long list of other parameters. See the Profile section in the setup section for more. If none is specified, the profile designated as default will be used.
4. **Backup/Fall Forward settings** - Described in the section "Making Manual Connections".

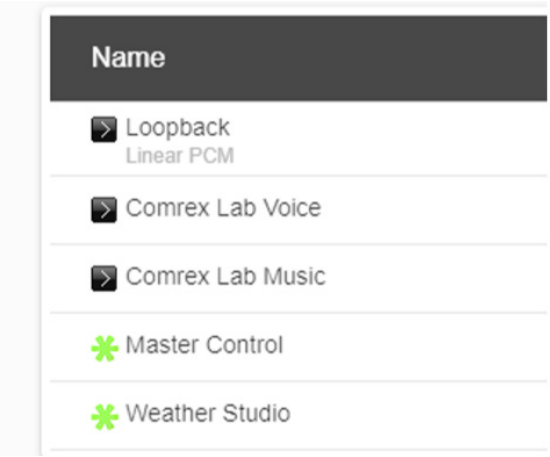

FIGURE 30 **SWITCHBOARD PEER REMOTE**

Once your Switchboard peers are configured, connecting to one is simple:

1. Select the desired Switchboard peer.
2. Make sure the “gear” icon is green.
3. Click “Connect” in the upper right corner.

Switchboard connections can be ended on either end of the link, by choosing the active connection in the list and clicking “Disconnect”.

Incoming connections will appear as new entries in the Switchboard peer list while they are active. They can be disconnected the same way.

IX. MAKING MANUAL CROSSLOCK CONNECTIONS

CREATING NEW REMOTES

When connections are added to the list manually, we call them “remote entries,” or “remotes” for short. To create a new remote connection, click on the “Plus Sign” (+) on the right of the screen (**1** in **Figure 31**) to **Add A New Remote Connection**. This will bring up a dialogue box where a new remote’s parameters may be defined (**Figure 31**).

FIGURE 31 EDIT REMOTE SETTINGS

Choose a name for the remote (e.g. WXYZ), followed by the IP address of the remote. If there’s a non-standard port being used on the receiving codec (e.g. MultiRack instances #2-5), you’ll need to apply it here after the IP address (e.g. 192.168.7.23:9004). This is particularly true when connecting to an ACCESS MultiRack, where each instance beyond instance #1 at UDP 9000, i.e., instances #2-5, will be configured to a different UDP that must be directed to in a new remote entry.

Choose whether this connection will use the CrossLock protection layer. For manual connections, this requires special configuration on each end of the link to authorize CrossLock between the codecs. See the section below about special notes for CrossLock connections.

The Switchboard ID field is only required when using the CrossLock function without the Switchboard server. For most codecs, this is the primary Ethernet MAC address of the far-side codec. If you are at Firmware 4.5 and newer and connecting to an ACCESS MultiRack instance, you may need an additional step. Add the instance number suffix as a “-x” to the end of the unit’s Switchboard ID (MAC Address) to designate the instance ID (e.g. Instance 4 as: 00:01:0c:c0:78:12-4).

The Connection Password function can be used to filter incoming connections. With this function, attempted incoming connections will be rejected without the proper case-sensitive password. For outgoing connections, the password is entered when the remote is created during the Add New Remote process. For incoming connections, the password is set on the System Settings tab. There is no way to retrieve a forgotten password. The only way to address a forgotten password is to change it.

Remotes require selection of a codec profile as seen in **Figure 32**. The BRIC-Link includes several factory profiles to choose from, each of which enables a full-duplex link. Factory-provided profiles offer commonly used encoders and settings. Depending on use and environment, custom profiles can be made in the Profile Manager tab (Figure 40). See the section on Profile configuration for more on this. Once defined on the Profile Manager tab, the new profiles will be available in the Select Profile window and can be assigned to an outbound remote.

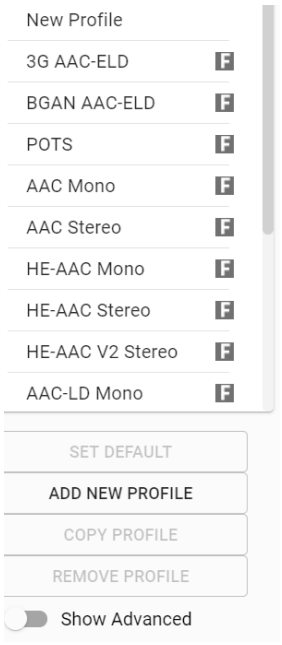

FIGURE 32 **PROFILE MANAGER TAB**

BACK UP REMOTE

BRIC-Link features an ability to have an automatic backup to a designated remote connection. A specific backup connection (for when the primary fails) is designated when a new remote is created. As shown in **Figure 33**, selecting the backup option opens a menu allowing selection of other outgoing remotes that have been created.

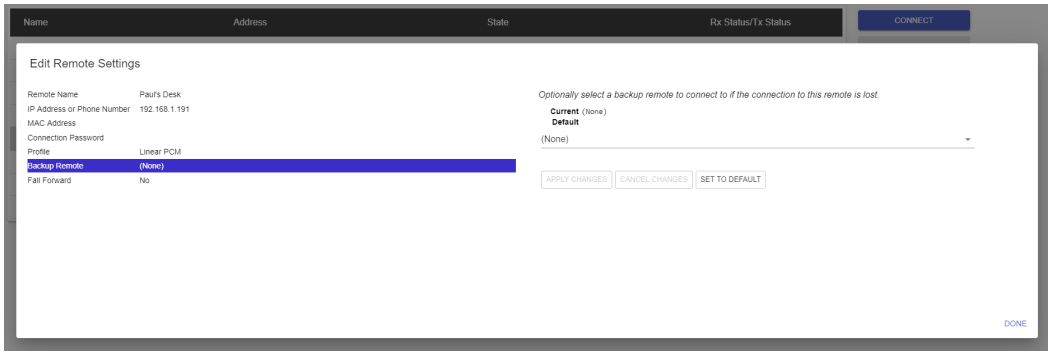

FIGURE 33 **EDIT REMOTE SETTINGS**

The **Backup Remote** feature works in conjunction with a remote's Local Timeout parameters defined in the primary remote's profile. BRIC-Link can sense an IP Connection failure, and will wait the defined Local Timeout parameter in the primary remote's profile. If the connection is restored during this time, no backup will occur. If the timeout lapses without re-connection to the primary remote, BRIC-Link will automatically connect to the designated **Backup Remote**. This connection will be retained until the connection is either manually terminated or the **Fall Forward** function reestablishes connection to the primary remote.

If the primary remote is restored and BRIC-Link can detect a valid signal, it will automatically disconnect the backup and revert back to the primary remote. To enable **Fall Forward**, click the "**Fall Forward**" option in the **Edit Remote Settings** prompt and select Yes (**Figure 33**).

CONNECTING AND DISCONNECTING

Once the remote connection entry is completed in the Connections Tab, highlight the remote and select Connect. When a connection is attempted, the State column in the connection table will change to reflect the progress of the connection (**Figure 34**). If the connection fails, the reason for the connection failure will be shown in the State column. When the remote connection succeeds, the encoder and decoder mode will be reflected in the Rx Status/ Tx Status column. To end a connection, highlight the remote and select Disconnect.

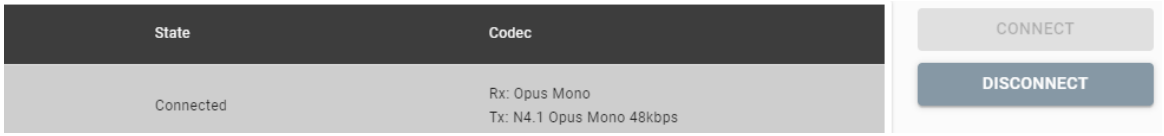

FIGURE 34 **REMOTE CONNECTION STATUS**

SPECIAL NOTES FOR 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 the 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 if connecting to an ACCESS MultiRack, instances #2-5 have special Switchboard IDs consisting of the primary Ethernet MAC followed by a "-x" 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 BRIC-Link 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".

x. SETTING UP YOUR SWITCHBOARD ACCOUNT

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. Use the instructions in the user interface chapters of this manual to configure **Switchboard** on the BRIC-Link unit. The following sections describe how to set up and configure your **Switchboard** account online. **Note:** BRIC-Link requires a Switchboard Traversal Server License to be used with Switchboard.

LOGGING IN AND SETTING UP 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. Clicking on **Add New Unit** will open a dialogue box that asks for the Switchboard ID (Ethernet MAC address) of the BRIC-Link (**Figure 35**).

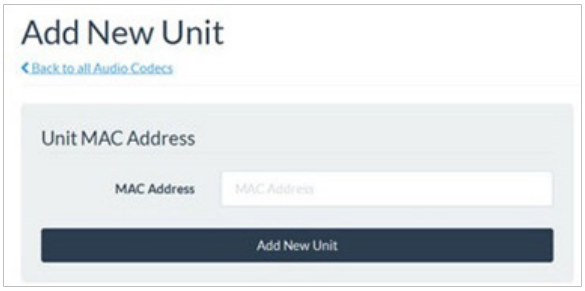

FIGURE 35 **ADD NEW UNIT**

After inputting each remote's Switchboard ID (MAC address), it will populate in the unit list (**Figure 36**). At this point is necessary to break the network connection to the codec (by rebooting it or disconnecting the network connection for several seconds) in order for the device to properly sync with Switchboard.

FIGURE 36 **SWITCHBOARD UNIT LIST**

Note: MultiRack instances must be added to Switchboard individually. Instance 1 Switchboard ID is the same as the unit MAC Address, while Instances 2-5 use the same MAC address, with a suffix added to designate the instance Switchboard ID. As an example, if the primary Ethernet MAC address on a MultiRack 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.

CREATING USERS

It is possible to add additional Switchboard users who can access the Switchboard interface. This is done via the **Users** tab at the top of the main codec list (**Figure 37**). This allows for the creation of accounts for users that can later be deleted. Several user accounts can be created with unique passwords.

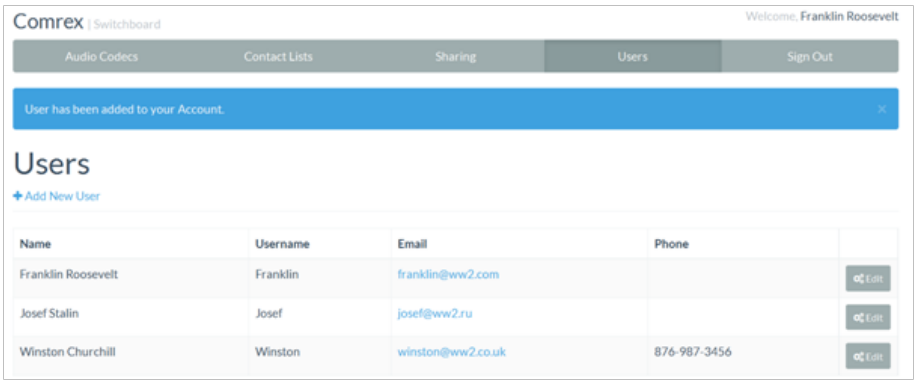

FIGURE 37 **USERS TAB**

CONTACT LISTS

In some situations, it might not be desirable for every codec to see the Switchboard status of every other codec. To help filter what's displayed on a codec's interface, Switchboard has implemented the concept of **Contact Lists**. Contact Lists contain a subset of a user's codec fleet on their account (**Figure 38**). Users can create multiple Contact Lists that consist of different subsets. With the exception of Shares (discussed next), only units within a user's Switchboard account may be assigned to Contact Lists.

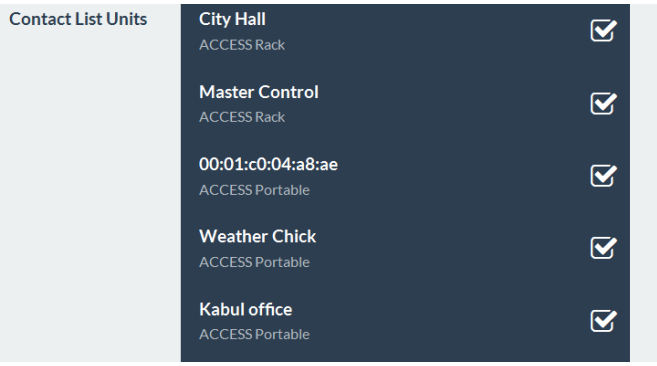

FIGURE 38 **CONTACT LIST**

By default, a master Contact List is created that contains all codecs in an account. Every codec in the fleet uses the master list by default. For users uninterested in segregating codes on their account, the default configuration will work fine.

NOTE: Assigning a Contact List to a codec determines what gets displayed in its own list. It does not have any impact on how that codec is displayed on other devices.

FOLLOWING CONTACT LISTS

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.

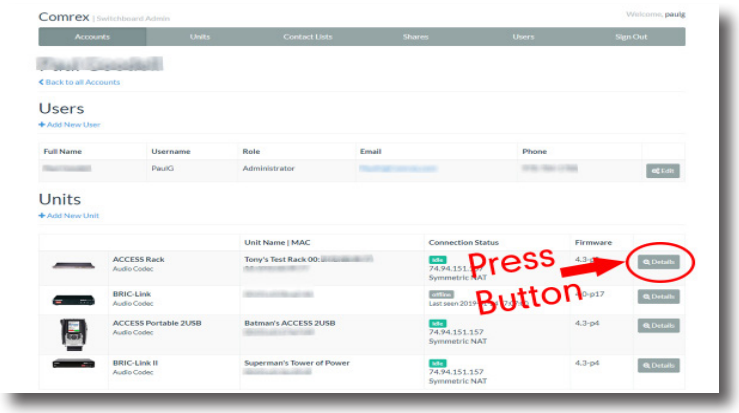

FIGURE 39 **SWITCHBOARD MAIN SCREEN**

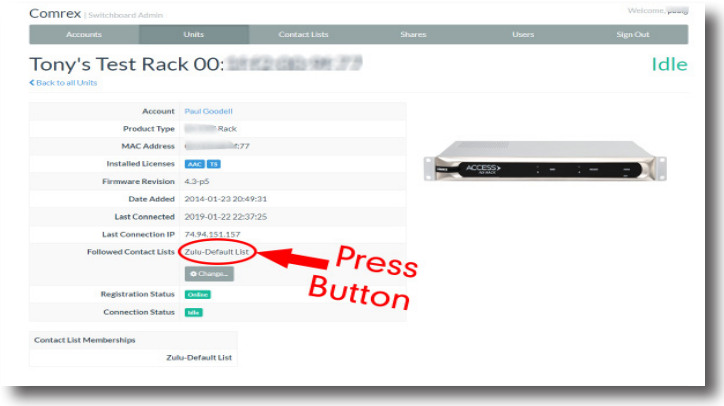

FIGURE 40 **UNIT SCREEN**

To follow a Contact List on a codec, first click on the “Details” button for that codec on the main screen in Switchboard (**Figure 39**). Next, press the “Change” button near the middle of the following screen (**Figure 40**).

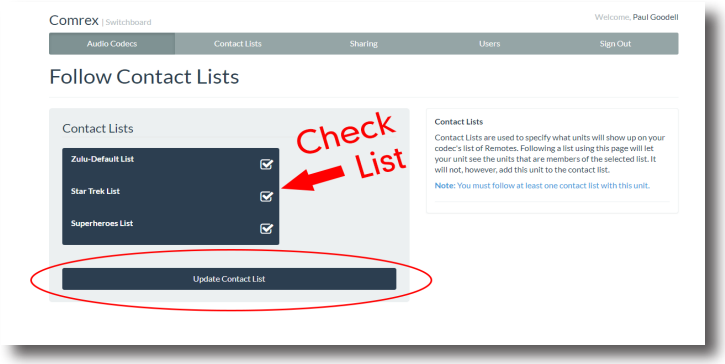

FIGURE 41 **FOLLOW CONTACT LIST**

On the next screen, check the Contact List(s) that you want this codec to Follow and press “Update Contact List” (**Figure 41**).

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

Switchboard users outside of an account can be granted permission see the status of others’ devices through the implementation of **Shares**—which, like Contact Lists, are also subsets of a user’s codec fleet that can be defined. Other Switchboard accounts can be added via Shares allowing codecs to become visible across accounts.

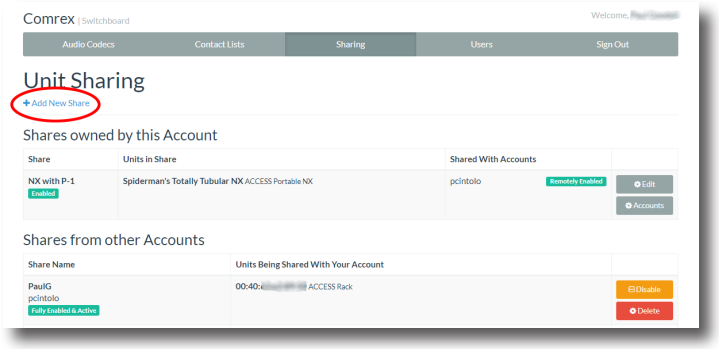

FIGURE 42 **UNIT SHARING TAB**

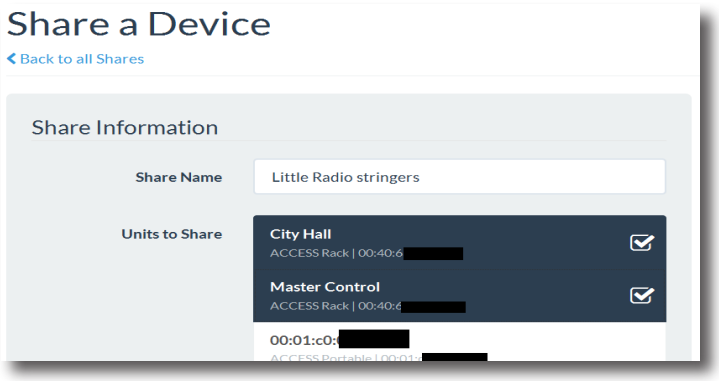

FIGURE 43 **SHARE A DEVICE**

To create a Share, click the **Sharing** tab and then select "**Add New Share**" (**Figure 42**).

The following screen allows users to choose which codec(s) they want to include in a Share (**Figure 43**).
After making a selection, users will need to enter one of the following to identify the account they wish to Share their 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 (**Figure 44**).

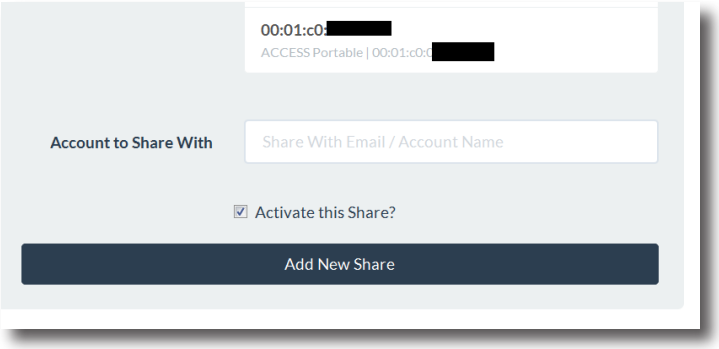

FIGURE 44 **ACCOUNT SHARE**

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

Please note: Shares are a **one-way transaction**. For shares to work both ways, with each user able to view each other's devices, both users must ***send*** each other a Share invitation and then each ***accept*** the other's invitation (as illustrated in **Figure 45**). 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.

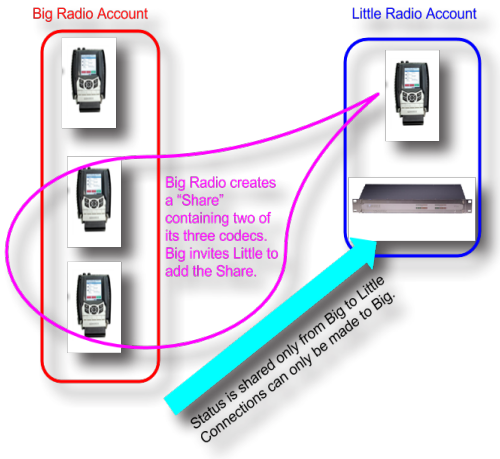

FIGURE 45 **SHARING ACCOUNTS**

Finally, while it is possible to delete Shares, Comrex recommends ***disabling*** them instead. This will stop the Share and won't require any future work to recreate it. To disable a Share, simply click the orange **Disable** button on the bottom right of the Share edit page (**Figure 46**).

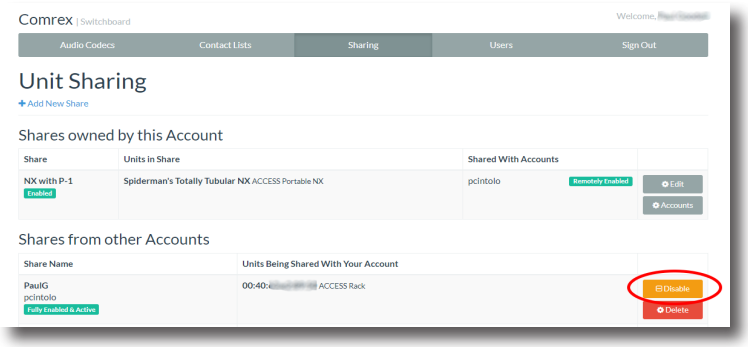

FIGURE 46 **DISABLE SHARE**

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.

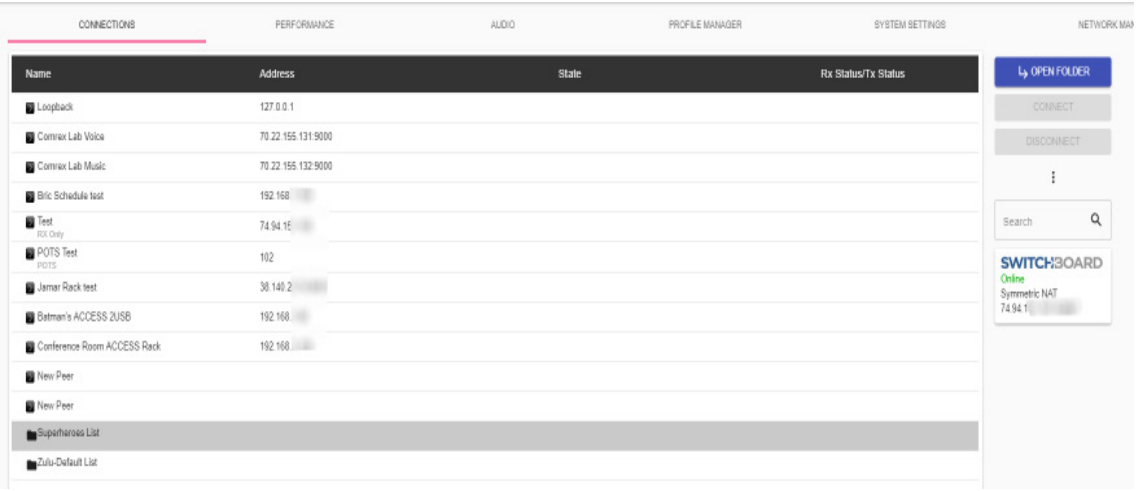

FIGURE 47 **MULTIPLE CONTACT LISTS**

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 Connections tab (**Figure 47**). To view and/or connect to the unit(s) within a list, select the list and press the **Open Folder** button on the upper right.

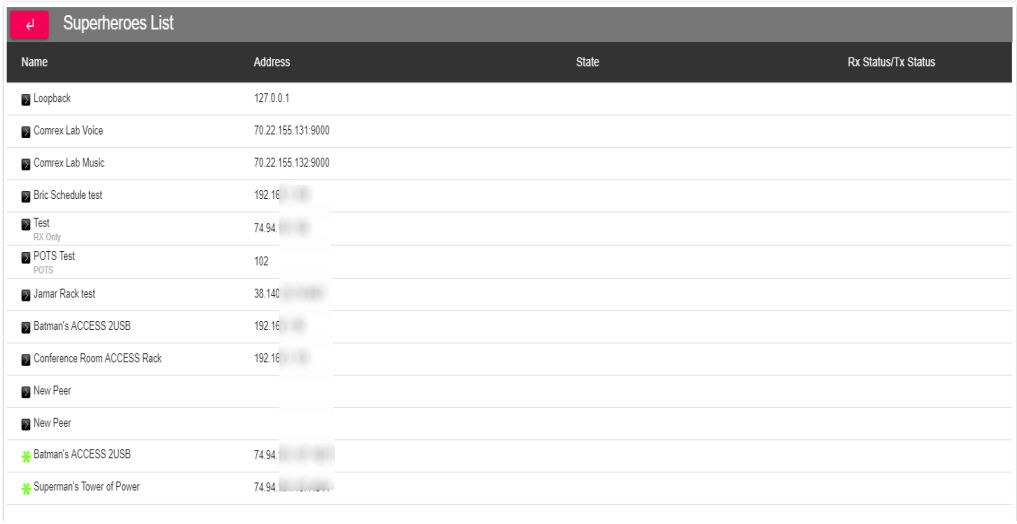

FIGURE 48 **VIEWING LIST DEVICES**

While viewing the units in a list, the units will be displayed and the lists themselves will temporarily disappear from the screen. To view the lists again, press the red "**Back**" arrow as seen in **Figure 48**.

Please note: Only Contact Lists that a codec is actively following can be viewed from that codec.

BULK ACTIONS FOR CONTACT LISTS

It is possible in Switchboard to perform actions that impact all codecs in a given Contact List in a single step called a **Bulk Action**.

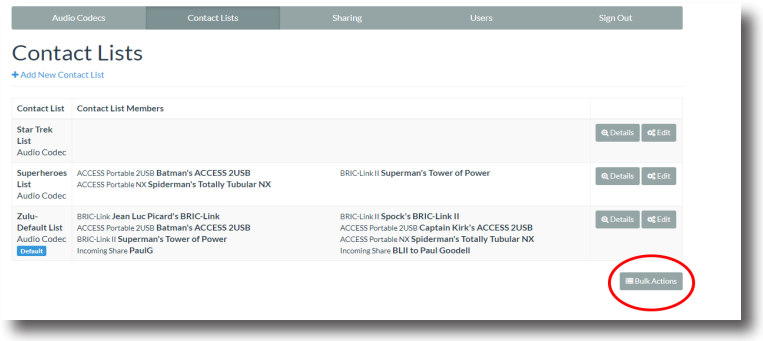

FIGURE 49 **BULK ACTIONS**

To do this, press the **Bulk Action** button in the bottom right corner of the Contact List tab (**Figure 49**).

The three steps to create a Bulk Action are:

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

Step 1: Choose the Action Type

First, select which of the four types of Bulk Actions to perform (**Figure 50**):

- 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).

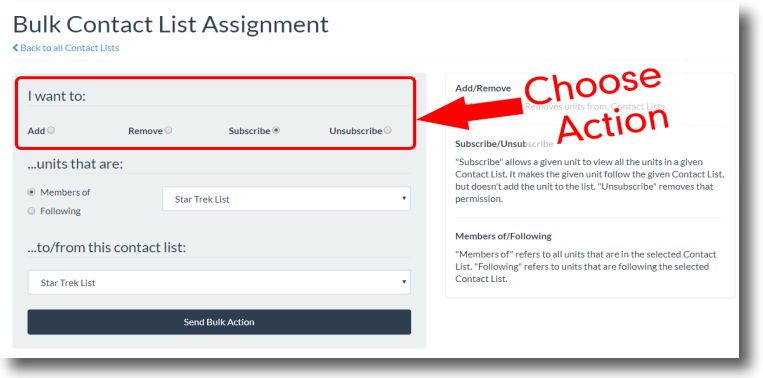

FIGURE 50 **BULK CONTACT LIST ASSIGNMENT**

Step 2: Select the Target Codecs

Next choose which list of codecs to target with this Bulk Action (**Figure 51**).

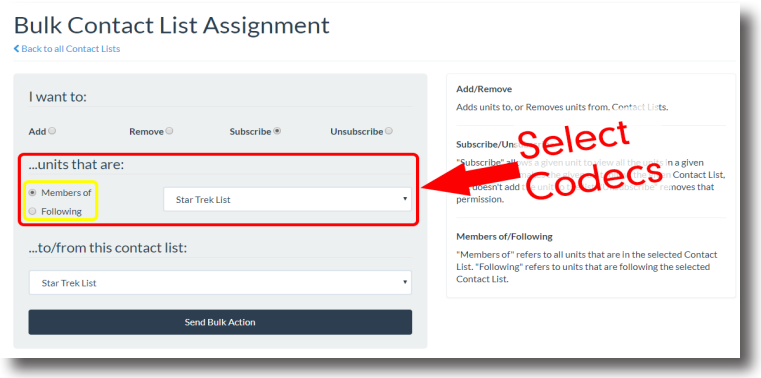

FIGURE 51 **BULK DEVICE SELECTION**

After completing this step, specify whether to target the units **that are a 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.

To only change a subset of the codecs in a list, try creating 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, 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 completed, press the **Send Bulk Action** button (**Figure 52**).

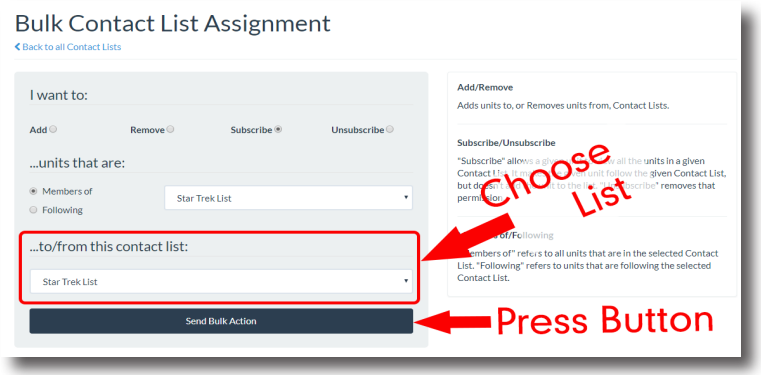

FIGURE 52 **SEND BULK ACTION**

Switchboard Theory and Concepts

Switchboard is useful because it's not always simple to connect two devices which are essentially "peers" over the Internet. There are two major reasons for this. First, to initiate a stream to a device over the Internet requires knowing 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 (**Figure 53**).

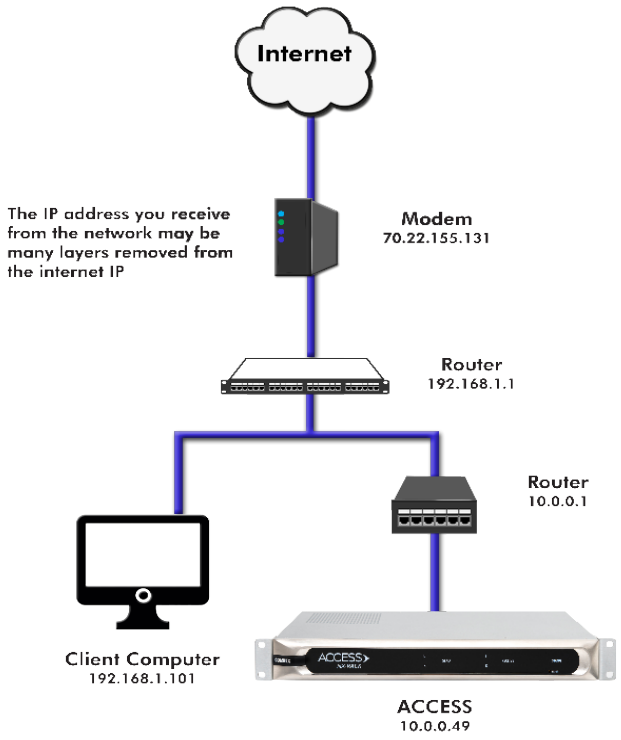

FIGURE 53 **LOCAL AREA NETWORK**

The challenges of connecting codecs behind NAT routers will be addressed in more detail shortly. For now, remember that one of the problems NAT servers add is that private IP addresses delivered to codecs (and the only addresses of which the codecs are aware) have no bearing on the public addresses seen from the Internet. In extreme scenarios, several layers of address locality can be stacked, assuring that the IP address assigned to a 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 had a fixed, public IP address. This meant that the address was allocated exclusively by the ISP, and that address was entered manually into the configuration of the codec and not subject to change. This scenario worked 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. 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, and does this by acting as a Directory Server. Codec users simply log in to the free server and are given an account, username, and password. Once logged in, it's a simple process to input the details of each owned codec. On the codec itself, the user should input a familiar name by which the codec will be known within that group.

Once enabled, a codec in a 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 "Buddy List" of sorts 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 different icons. 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. Additionally, forwarding functions are implemented differently depending on the hardware. One can easily imagine the complications of obtaining or managing port forwarding on the LAN when arriving at a new remote venue. This 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 (**Figure 54**).

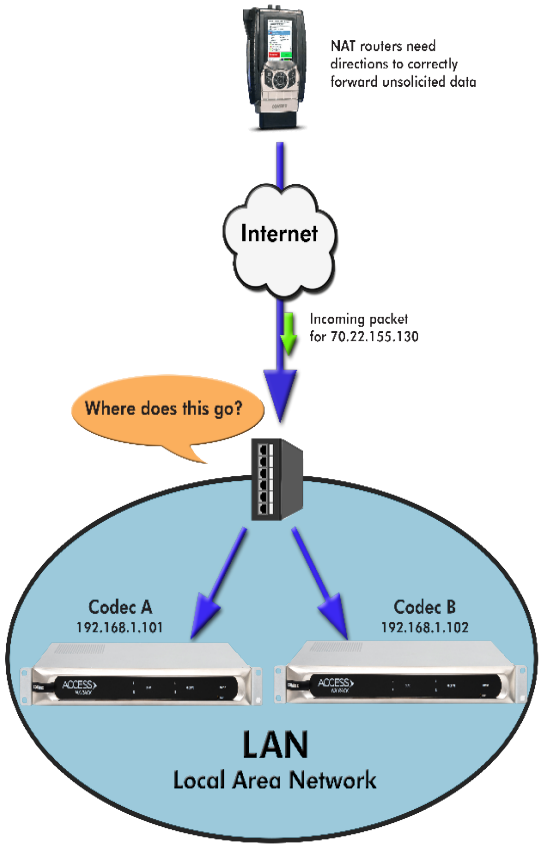

FIGURE 54 **NAT TRAVERSAL**

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 (**Figure 55**).

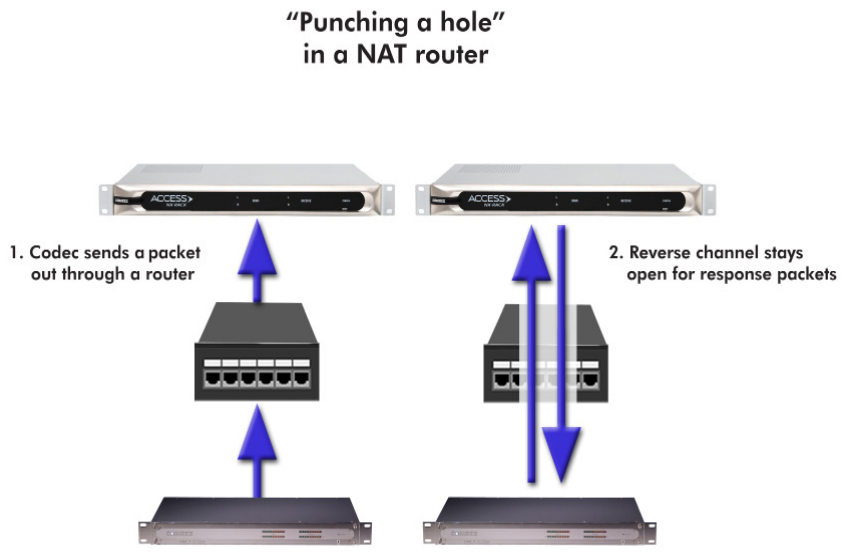

FIGURE 55 **BIDIRECTIONAL COMMUNICATION**

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.

XI. OPERATING BRIC-LINK IN A 24/7 ENVIRONMENT

BRIC-Link can be configured for “always on” operation. This allows for constant STL communication and operations requiring long-term connections.

In BRIC Normal mode (the default mode of operation), BRIC-Link transfers all its audio data via the UDP 9000 protocol. This is in contrast to most web-based connections like browsing and email, which use the bidirectional TCP protocol. UDP, unlike TCP, is not “connection oriented” (i.e., 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 make its best effort to deliver the packets in a timely fashion. If a packet is delayed or lost, no error message is sent from the receiving unit and no packets are retransmitted. It is up to the receiver to cover up any lost data, if possible. This allows the Internet to deliver packets with the smallest amount of overhead and delay. As there is no coherent connection built between the codecs, there isn’t any connection to break in the event of network failure. The encoder simply propels packets into the network, regardless of whether they arrive. If the network fails and is later restored, the packets stream will be restored to the decoder.

For most applications like remote broadcasting, it’s useful to simulate a connection-oriented stream, so BRIC-Link 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” where UDP exists. By default, it monitors the health of a connection and if no data is detected as received by the decoder for 60 seconds (this is a user-defined timeout), it “tears down” this connection and reverts to an idle state. This indicates to the user that the network has failed and the problem must be addressed.

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

ALWAYS CONNECT TO

To set BRIC-Link 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 status.
2. BRIC-Link is configured to re-establish the connection in the event of a power-up.
3. The local **Disconnect** control is disabled. The **Disconnect** function on the receiving side is still enabled, but will result in an immediate re-connection by the initiating side.

As seen in **Figure 56**, under **Connections** in the **System Settings** tab (with “Show Advanced Options” selected), there is an **Always Connect To** option with a pull-down menu of your unit’s available connections. Selecting “ON” in these remote connections will configure the unit for 24/7 operation to that remote. (No configuration is necessary on the remote side.)

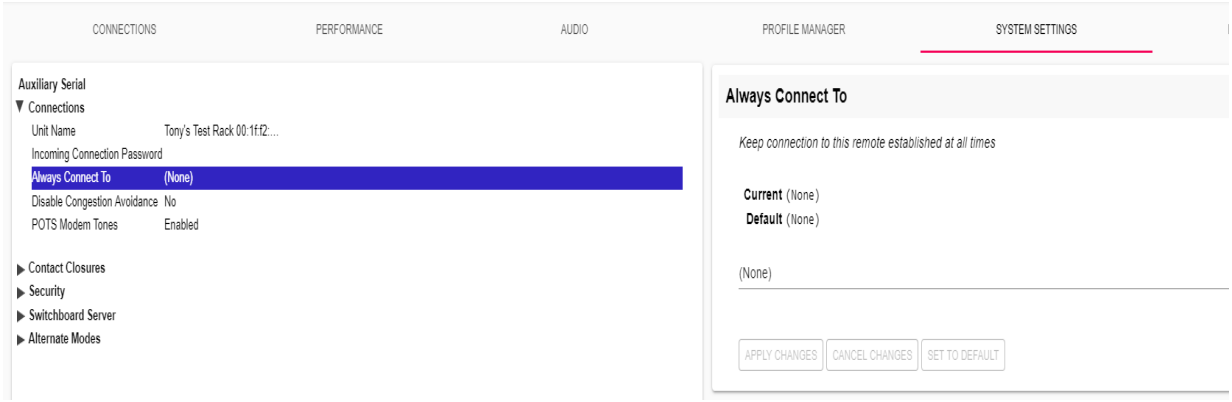

FIGURE 56 **ALWAYS CONNECT TO SETTING**

BACKUP REMOTE

BRIC-Link has an additional option for constant connections. When building a remote entry, a field is available for backup options, and one of these options is “Keep Retrying This Remote” mode. In a similar fashion, using this mode will allow the unit to disregard the timeout value and keep a persistent connection attempt. The difference is that the Disconnect function still works and the connection will not be re-initiated on a power-up. This mode is meant for users who are making longer-term temporary connections, and do not want the system to time out and disconnect in the event of network failure.

The BRIC-Link has the capability to automatically make a backup IP connection if there is a failure in the primary connection. This is called **Fallback**, and is an option chosen after defining a new Remote connection.

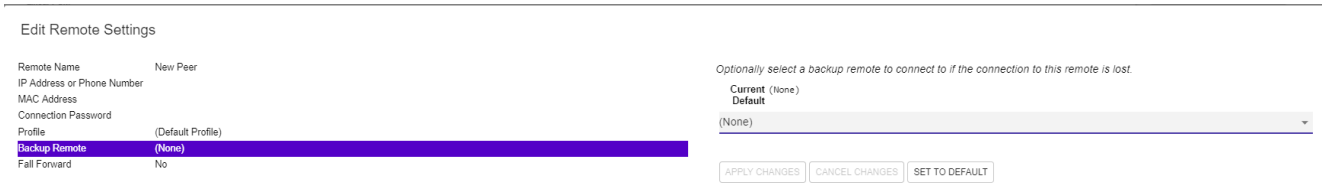

FIGURE 57 **BACKUP REMOTE**

As shown in **Figure 57**, highlight an existing connection (this will be the primary connection) and choose **Change Remote Settings**. In the pop up window, a pull-down box is available to allow selection of a fallback connection from the list of existing remotes.

After connection, if data is stopped on the primary connection for the length of the timeout value (set in the connection’s profile), a connection will be attempted and maintained to the fallback remote.

Additionally, there is a box in the **Change Remote Settings** tab labelled **Automatically fall forward**. If this box is checked, the system will constantly attempt to reconnect the primary remote while connected to the fallback remote. If connection is successful, the connection to the “Fallback” will be terminated.

XII. ABOUT THE ALGORITHMS

When building profiles for BRIC-Link and remote devices, there are several different audio encoder options to use for each direction of the link. Different audio encoder options each have advantages and disadvantages, depending on the situation. The following is a refresher on audio codec algorithms to assist in making the best choice.

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 kb/s 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 BRIC-Link. Enhancements like HE-AAC attempt to maintain a similar quality with reduced bandwidth and delay.

HE-AAC

This is a newer version of AAC designed for increased efficiency. The goal of this 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). SBR is a technique that partially synthesizes these high frequencies. HE-AAC is trademarked by other companies as AACPlus™. HE-AAC (and close derivatives) is 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. Reduced rate HE-AAC mono is grouped into this category, although it does not contain v2 coding.

LINEAR PCM*

This encoder does not compress audio at all. It uses a 48 kHz sampling rate (using analog inputs or 48 kHz AES3) and 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 804 kb/s while Stereo (Dual Mono) Mode requires a network bandwidth over 1.56 Mb/s.

In Linear PCM, if the input AES3 sampling rate is 32 kHz or 44.1 kHz, the network stream will also run at this rate and the required bandwidth will be lower.

FLAC*

This encoder compresses 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 artefacts. 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.722

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

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 (see Technotes about WebRTC on the Comrex website). Special CBR modes are offered for compatibility with Tieline products—avoid these in other applications. Due to its versatility in audio quality and low networking drain, Opus is the default profile for Comrex codecs.

**Linear PCM and FLAC are only supported for CrossLock connections on devices running 4.3-p4 firmware or higher.*

Algorithm Comparison Chart for ACCESS			
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.722 coding algorithm for compatibility with SIP-style VoIP phones.
64 kb/s	35 ms	7 kHz	**X3 G.722**

FIGURE 58 ALGORITHM PROFILES

XIII. MULTISTREAMING

BRIC-Link supports the ability to run one encoder per connection, but this single encoder stream may be sent to up to three destinations simultaneously. This capability is referred to as a **Multistream**, as the encoder creates a separate but identical outgoing stream to each decoder. (Note: A User's Internet connection must be able to support these streams. For example, if an encoder runs at 35 kb/s network utilization, sending to two locations will require 70 kb/s upload speed from the network.)

Multistreaming should not be confused with IP Multicast, which is described in the next section. Each BRIC-Link can only run one decoder, so it's important that in a **Multistream** environment, a maximum of one stream is sent in the reverse direction. This means that users interested in hearing a Multistream must turn off their encoders. This can be a bit confusing because **Multistream** can be initiated from either end of the link.

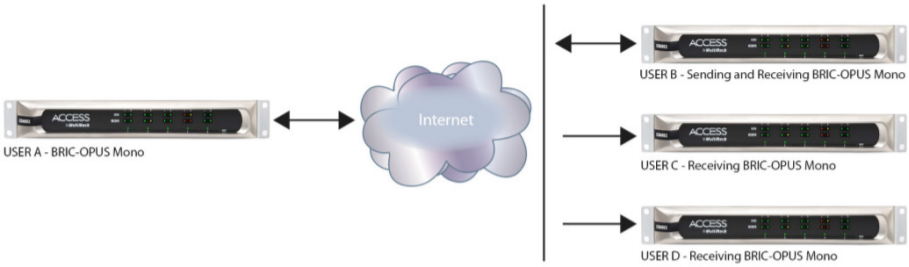

FIGURE 59 **MULTISTREAMING ARRANGEMENT**

Figure 59 shows a BRIC-Link **Multistream** arrangement. BRIC-Link A is the Multistreamer, with BRIC-Link B, C and D listening to the same audio. In order to set up a Multistreaming scenario, the BRIC-Link encoders must be turned **Off**. This is done by building a profile with either the **Local** or **Return Transmitter** mode set to **Off**, as shown in **Figure 60**.

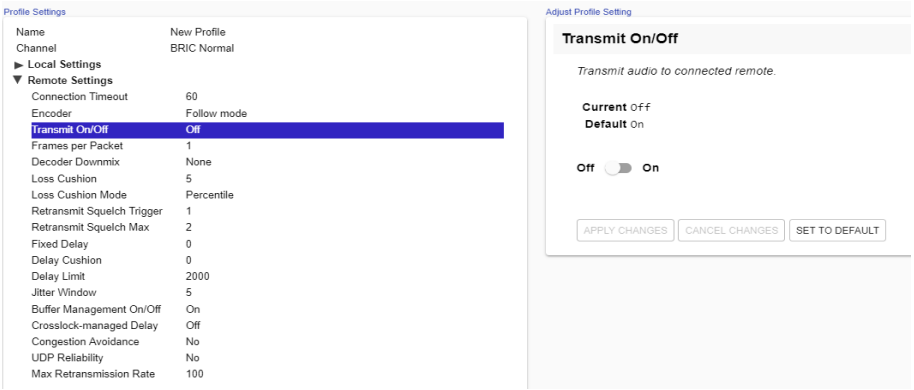

FIGURE 60 **TRANSMIT ON/OFF**

MULTISTREAMING ARRANGEMENTS

The following includes two examples of **Multistream** arrangements involving the BRIC-Link. In the first environment, the BRIC-Link that is serving the Multistream initiates calls, and in the second, the serving BRIC-Link accepts all of the incoming connections.

BRIC-LINK INITIATES THE CALL

In the “Multistreamer as caller” model, two different profiles will be built on BRIC-Link A. The first profile, labelled “Multi-Duplex”, will be defined as a standard, duplex BRIC-Link 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 BRIC-Link B, C, and D. They will assign the “Multi-Duplex” profile to BRIC-Link B, and “Multi-Simplex” profile to the others. They will then establish a connection with BRIC-Link B first, followed by C and D.

BRIC-LINK RECEIVES THE CALL

In model number 2 where the serving BRIC-Link accepts all incoming connections, all the profiles are built on the **Remote Receivers**. BRIC-Link B will use a simple profile by defining the encoders in each direction, and assign it to BRIC-Link A. BRIC-Link C and D will each define a profile with their **Local Encoders** turned **Off**, and assign them to A. BRIC-Link 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 **Multistream** 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.

USING CROSSLOCK WITH MULTISTREAM CONNECTIONS

CrossLock functionality in Multistreaming has been introduced with BRIC-Link. Previous Comrex BRIC-Links did not support CrossLock VPN when performing a **Multistream**. With the introduction of BRIC-Link, the added broadcast reliability of CrossLock brings increased connection stability in Multistreaming environments.

XIV. IP MULTICAST

IP Multicast is an efficient way of delivering BRIC-Link 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.

Performing an 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 does not support duplex connections, and only supports a single direction stream. An encoder can not receive input streams when multicasting. CrossLock is not supported and should be turned off for all IP Multicast connections.

The following section presupposes that IP Multicast users will be familiar with the basic concepts of setup and operation of the network, and will thus focus on how to configure BRIC-Link for Multicast mode.

MULTICAST PROFILES

To configure remotes for Multicast, first create a profile for either a Multicast Sender or a Multicast Receiver on the **Profile Manager** tab.

As shown in **Figure 61**, when defining a new profile there is the option to choose **Multicast** as the profile type. Multicast profiles have fewer options than other profile types, however, and some of the available options will have no effect (e.g. setting an encoder type on a Multicast receiver has no effect).

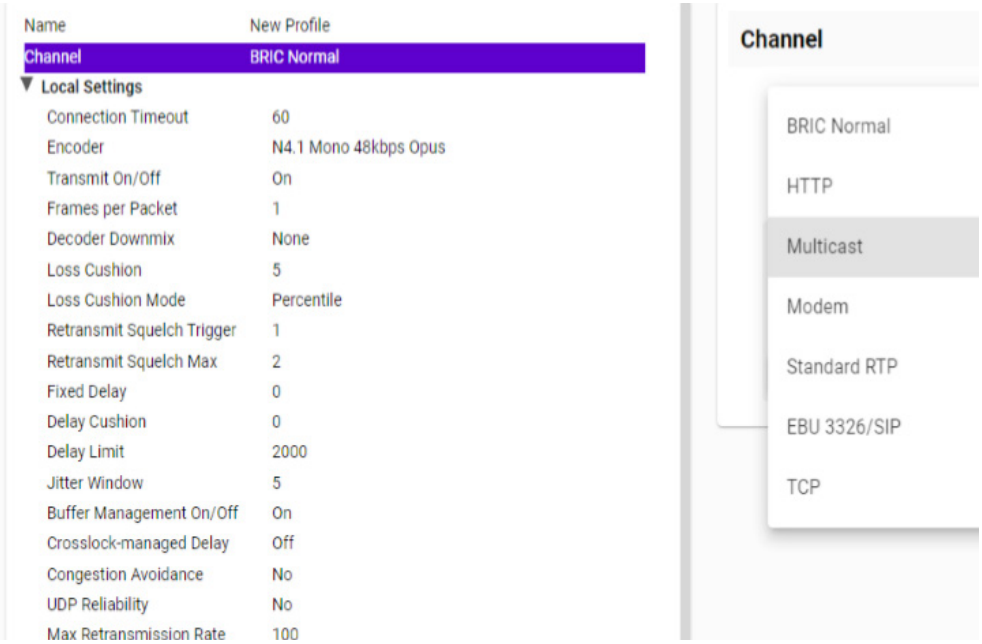

FIGURE 61 **MULTICAST SETTINGS**

The important settings for Multicast are:

- **Sender/Receiver** - Determines whether this particular BRIC-Link is designed to generate and encode the IP Multicast stream (send) or decode one (receive).
- **Encoder Type** - Determines the algorithm format 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 BRIC-Link 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 "/", followed by the TTL value. An example 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 standard socket format, 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**.

XV. STREAMING SERVER FUNCTION

BRIC-Link 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,** and **Windows Media Player 12** and up.

By default, streaming server functionality is turned off. To enable it, go to the **System Settings** tab of the User Interface and choose **HTTP Settings** option. Under the first option, set **Accept Incoming Connections** to **Enabled** (**Figure 62**). This allows outside users to initiate a "pull" connection to the codec.

FIGURE 62 **ACCEPT INCOMING HTTP CONNECTIONS**

The default port for serving streams is TCP 8000. Creating a custom port can be done in the HTTP settings under **IP Port**. Note that this port will need to be referenced in the URL provided to listeners.

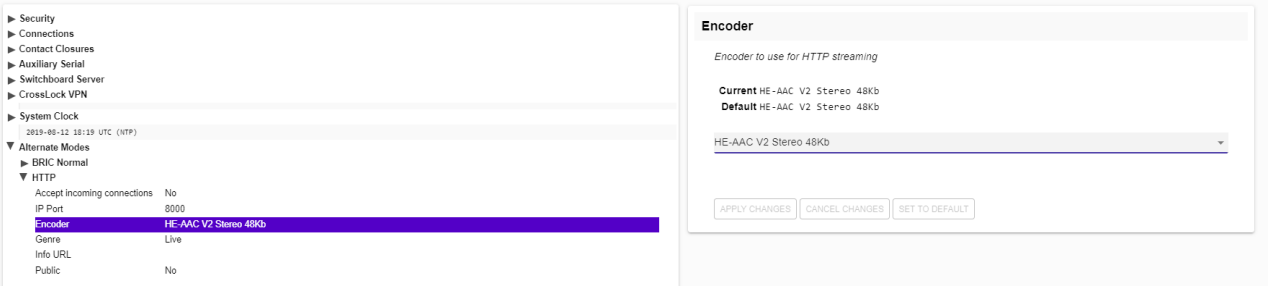

FIGURE 63 **HTTP STREAMING ENCODER**

Next select an encoder for use by the streaming server (**Figure 63**). 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, 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 STREAM

To decode a stream, open one of the supported players and select the option to open a URL-based stream.

In **Winamp** and **VLC**, input the address of the BRIC-Link in the following format:

http://192.168.0.75:8000
(using the actual IP address, and the actual port—if not changed from the default, it will be **8000**)

In **Windows Media Player**, input the address like this:

http://192.168.1.75:8000/stream.asx
(using the actual IP address, of course)

SIMULTANEOUSLY CONNECTING BRIC-LINKS AND STREAMING

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

XVI. MAKING EBU3326/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 **EBU3326**, a technical document describing how best to achieve this goal.

EBU3326 by and large establishes a set of features each codec should support, and then leaves most of the heavy lifting to other, previously established standards like SIP (IETF RFC 3261). Topics not covered (yet) by EBU3326 include things like carrying ancillary data, contact closures from end-to-end, codec remote control, monitoring, and complex NAT traversal—which at this point are still left to the individual manufacturer's discretion. If these topics are important to a user's application, it's best to stick to a single codec vendor and their proprietary protocols.

MORE ABOUT EBU3326

The Tech 3326 document defines several mandatory encoding algorithms, and the transport layer that could be used on them for compatibility. But 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 is called **SIP**, which is used extensively by VoIP phones and therefore was a logical choice. SIP carries the advantage of making BRIC-Link compatible with a range of other non-broadcast products, like VoIP hardware, software, and even mobile phone apps.

EBU3326 IN BRIC-LINK

BRIC-Link does not fully comply with EBU3326, as it does not feature the mandatory MPEG Layer II codec. Aside from this, BRIC-Link has been tested to be compatible with several other manufacturer's devices using encoders supported by both products. When using **EBU3326/SIP Compatible** mode (how the user interface describes EBU3326), ancillary data, contact closures, Switchboard TS, Multistreaming and Multicasting are not supported. Outgoing call profiles built with the EBU3326/SIP channel may lack some advanced options, and cannot be set for different encoders in each direction (i.e., EBU3326/SIP calls are always symmetrical).

EBU3326/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**.

The BRIC-Link allows EBU3326/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 EBU3326/SIP** mode is simple—just build a profile, but instead of choosing **BRIC Normal** channel, choose **EBU3326/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 EBU3326/SIP relate to **Registered** mode.

REGISTERED MODE

Registering with a SIP server in **EBU3326/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. Comrex's Iptel user URI would be comrex_user@iptel.org. Comrex devices do not use the designation "sip:" before a SIP address.

If a connection is 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 BRIC-Link with a SIP server:

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

- The password on the SIP account.

Figure 64 shows how this information can be applied: by enabling the **Use SIP Proxy** option under **EBU 3326/SIP** on the **Systems Settings** tab.

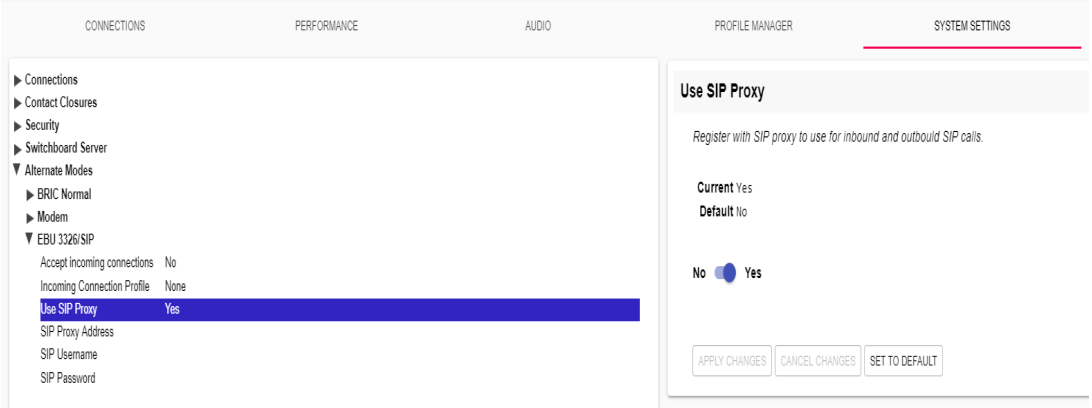

FIGURE 64 **EBU3326/SIP SETTINGS**

Once this information is correctly entered, a new field appears in the “Registration Status” box located on the **Connections** tab (**Figure 65**).

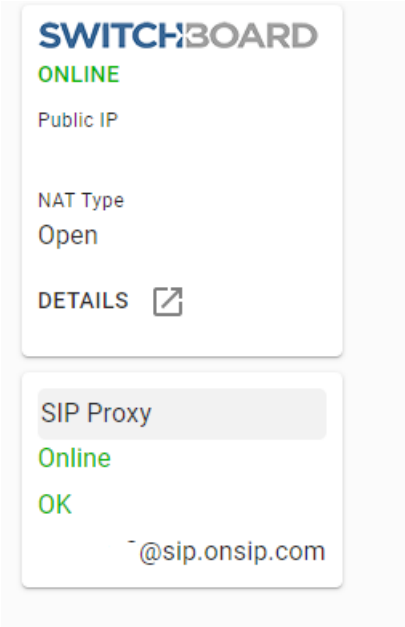

FIGURE 65 **SIP STATUS**

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 means that registration likely failed. It’s best to go back and carefully check the registration info. It might also be useful to ensure the registration information is valid by configuring a VoIP phone or softphone with it and attempting registration.

SIP registration can be very simple with some servers, and others can require more advanced settings, which are described in the **Advanced Topics** section on the following page.

MAKING REGISTERED SIP CALLS

When registered, calls made using an EBU3326/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. Reasons for call rejection by a server are numerous. Some examples are:

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

ADVANCED EBU3326/SIP TOPICS

The basic entries provided will allow support for the vast majority of EBU3326/SIP based applications. There are inevitably situations where the defaults won't work, however. Comrex has provided some advanced options that can help. 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 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, as **5004** is the default port for other services on Comrex codecs.
- **Public IP Override** - See the **SIP Troubleshooting** section for more information on this option.
- **Use STUN Server** - See the **SIP Troubleshooting** section for more information on this option.
- **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** - This only applies to **Registered** mode. It’s 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 for calls to be established correctly.

The primary area where SIP complicates matters is how an audio channel is established once the handshake channel is defined. In the common-sense world, the call would be initiated to the destination IP address, and then the called codec would extract the source IP address from the incoming data and return a channel to that address. This is the default method Comrex devices use to create and maintain a connection.

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 works fine as long as each codec knows its public IP address.

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 does not know its public address. A codec will populate its private IP address (e.g. **192.168.x.x** style) into that “return address” field. The called codec will attempt to connect to that address and fail, as its private IP Address can’t be reached from public Internet.

INCOMING CALL ISSUES

Incoming calls to codecs behind routers are complicated by the need to forward ports on the router 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>. As 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, 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, and some hacks are required to make this work. The first place to look is the router, as many modern routers are aware of this issue and may be configured to ease connectivity. If a router supports the **SIP Application Layer Gateway (ALG)**, enabling this option can fix the issue. The router will read the SIP handshake, find the outgoing address field, and replace it with the public IP. This is a valuable solution in environments where the router supports ALG. In environments where ALG is not available, **STUN** is a valuable alternative.

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 EBU3326/SIP** options and allows for the codec to learn its public IP address. It does this by contacting a STUN server on the Internet (the default one is maintained by Comrex) and requesting its Public IP. If this option is enabled, the codec itself will handle the address switching.

Be aware of the "battling workarounds" issue, as 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 are unusable for some 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. A user can thus place their Public IP address (obtainable from many websites via a browser) in this location. Keep in mind, the Public IP Address is often subject to change over time, so it's important to remember that this change has been made on a codec.

XVII. LICENSE & WARRANTY DISCLOSURES FOR BRIC-LINK

LICENSES

MPEG-4 audio coding technology licensed by Fraunhofer IIS
http://www.iis.fraunhofer.de/amm/

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 © 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 Road, 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

XVIII. SWITCHBOARD TRAVERSAL SERVER USE DISCLAIMER

TRAVERSAL SERVER DISCLAIMER

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. **Note:** BRIC-Link requires the one-time purchase of a Traversal Server License for Switchboard compatibility.

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**.

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** 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 Traversal Server 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 warranty or guarantee of suitability of any kind.

XIX. CONFORMITY AND REGULATORY INFORMATION

SUPPLIERS' DECLARATION OF CONFORMITY

Place of Issue: Devens, Massachusetts

Date of Issue: **January 23, 2006**

Equipment: Comrex BRIC-Link

Comrex Corporation, located at 19 Pine Road, Devens, MA in the United States of America hereby certifies that the Comrex BRIC-Link bearing identification number **US:DXDMD01BACCRK** complies with the Federal Communications Commission's ("FCC") Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments ("ACTA")-adopted technical criteria TIA/EIA/IS-968, Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment To the Telephone Network, July 2001.

Thomas O. Hartnett, Vice President, Comrex Corporation

Note: 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.

EC DECLARATION OF CONFORMITY FOR R&TTE DIRECTIVE

We:

Manufacturer's Name: Comrex Corporation

Manufacturer's Address: 19 Pine Road
Devens, MA 01434

hereby declare on our sole responsibility that the product:

Comrex BRIC-Link
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

Contact person: Thomas O. Hartnett, V.P., Engineering

Signed: 

Date: **23 January 2006**

U.S. AND CANADIAN REGULATORY INFORMATION FOR THE BRIC-LINK

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA, as well as the applicable Industry Canada technical specifications. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format **US:DXDMD01BACCRK**. If requested, this number must be provided to a U.S. telephone company.

Telephone line connections to the Comrex BRIC-Link are made via an RJ11C jack. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. **A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.** See installation instructions for details.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. The sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. The REN for the Comrex BRIC-Link is **0.1**, and is shown as the digits represented by ## in the product identifier **US:DXDMD###ACCRK**.

If the Comrex BRIC-Link causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with the Comrex BRIC-Link, please contact Comrex Corporation at 978-784-1776 for repair or warranty information. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is solved.

No user serviceable parts are contained in this product. If damage or malfunction occurs, contact Comrex Corporation for instructions on its repair or return.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. This equipment cannot be used on telephone company provided coin service.

If you have specially wired alarm equipment connected to the telephone line, ensure the installation of the Comrex BRIC-Link BRIC-Link does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

APPENDIX A - IP COMPATIBILITY

The BRIC-Link is capable of encoding and decoding a choice of three different types of non-BRIC-Link streams: **Standard RTP**, **Luci Live** and **Zephyr Xstream**. The choice is exclusive—i.e., you must set the BRIC-Link specifically for the type of stream you wish to be compatible with and you will remain incompatible with the other two types unless you change it. This setting has no effect on normal BRIC-Link functions, which continue to operate as before.

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. BRIC-Link 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:
   - **Initial Setup** - This will define all Standard RTP connections to be Luci Compatible
   - **BRIC-Link** - On the **System Settings** tab, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, choose **Luci Live**.
   - **Incoming Connections** - **Luci Live** sends either an AAC or HE-AAC stream to the BRIC-Link 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.
   - **Outgoing Connections** - Build a profile using the **Profile Manager** on the BRIC-Link 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 BRIC-Link.

2. **Zephyr Xstream** - Xstream Firmware version 3.2.0 and higher support an "RTP Push" function that is compatible with BRIC-Link in some modes. BRIC-Link 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 BRIC-Link is only compatible with the AAC mode.
   - The Xstream uses downsampling in modes below 96 kb/s, which is not supported by BRIC-Link.
   - In order for an Xstream to decode an BRIC-Link 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**:
   - **Initial Setup** - This will define all Standard RTP connections to be Xstream Compatible.
   - **BRIC-Link** - On the **System Settings** tab, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, select **Zephyr Xstream**.
   - **Incoming Connections** - **Zephyr Xstream** sends an AAC stream to the BRIC-Link 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.

- **Outgoing Connections** - Build a profile using the **Profile Manager** on the BRIC-Link 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 BRIC-Link.

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.

APPENDIX B - BRIC-LINK ON UNIDIRECTIONAL NETWORKS

Under most circumstances, BRIC-Link requires an IP path in both directions for successful connections, even when audio is being sent only 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 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.

- On the BRIC-Link, click the **System Settings** tab and select **Show Advanced Options.**
- Find **Standard RTP Settings** and choose to edit the **RTP Compatibility Mode.**
- Change this setting to **Standard** and click **Apply.**

STANDARD RTP SETTINGS

The following setting instructions apply to both codecs in the link (encoder ***and*** decoder):

DECODE SIDE SETTINGS ONLY

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

ENCODE SIDE SETTINGS ONLY

Connections of this type must be established from the encoding side of the link. A new Profile must be built that uses the **Standard RTP** channel mode under the Profile Editor. Choose an outgoing encoder along with any other special attributes in the profile editor. Name the Profile something descriptive like “Simplex”.

Next, create an 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.

APPENDIX C - INFORMATION FOR IT MANAGERS

The purpose of this appendix is to describe all open ports and services available on the Comrex BRIC-Link.

The Comrex BRIC-Link 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 **Device Manager**, a Windows- or MAC-compatible application, 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 BRIC-Link, you have five minutes before this function is disabled.

IP parameters can also be changed online using the **Network Manager** in the Web GUI Main Menu**.** 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 80-85	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	SIP	Off
UDP 5004, 5005	Standard RTP	Off (On for products shipped before 1 July 2017)
UDP 6014, 6015	SIP RTP	Off
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	0.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)

APPENDIX D - 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" on www.comrex.com

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 username 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 Switchboard ID (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 Switchboard ID. Each instance must be added to Switchboard individually. Instances 2-5 use the same MAC address with a suffix (e.g. -2, -3, -4, and -5) added to designate the instance Switchboard ID.

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.

FIGURE 66 **MULTIRACK INSTANCE ENTRIES IN SWITCHBOARD**