ACCESS
NX

Product Manual

COMREX

ACCESS NX MANUAL

I. COMREX ACCESS NX 4.1-P1 FIRMWARE RELEASE NOTES

Please note that during operation, the metal side plates of ACCESS NX get very warm. This is because NX contains a high-power quad-core processor, and the NX design incorporates some elaborate heat spreading to vent the CPU heat to the side plates. It is completely normal for these plates to get very warm, and NX has been tested to operate of it's full temperature range.

UPDATES WITH 4.1-P1 FIRMWARE

- Raise CPU/GPU core voltage at 400 & 800MHz for stability improvements
- Older Realtek wi-fi driver added
- GUI signal handling fixes – system shutdown works again
- Fix bug where if you navigated away from Network Manager or Remote Connection view when a modal dialog popped up (device editor, remote editor, or confirmation dialog), that dialog would be broken until the next reboot and not allow further editing because it was stuck waiting for the hidden modal dialog to close
- GUI transition animation bug fixed where title would briefly show the wrong name when flipping between views with F2 key
- Bug fixed where wrong title was shown after hitting the "Home" button to go to Remotes view
- GUI crash recovery – if the GUI crashes due to segmentation fault or other catastrophic error,a watchdog script will restart it. The "sick NX" screen will be briefly shown before the GUI restarts.

-
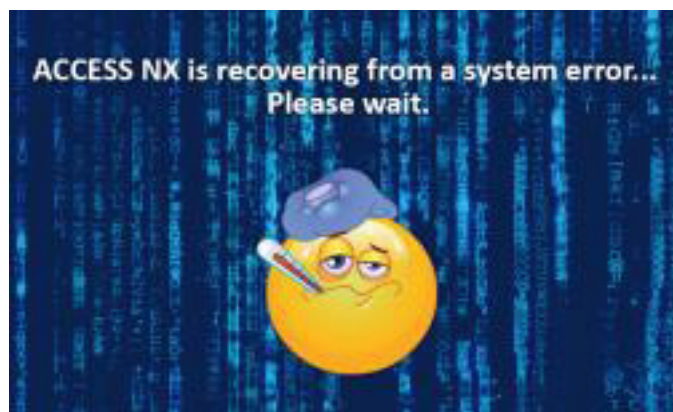
- Adds the missing "(Keep retrying this remote)" to the Backup Remote option when editing a Remote Connection
- Several layout fixes in two-pane editors (profile editor, remote editor, network manager, system settings, etc) – new view-only / advanced / factory icons replace text, overlapping text and buttons fixed, bug where profile node commands (copy profile/set default/remove profile) were appearing on profile options instead of just on nodes
- Layout fixes/improvements on dashboard - text overlapping graphics, hide mutes 3,4,5,6 for non-mixer units

- On CrossLock stats view show "No active CrossLock session" when no sessions active .. fix minor text/graph layout issue

- Fix bug with missing advanced options in network manager device editor (e.g. preserve after reset, use with CrossLock, etc.)

- Virtual keyboard bug (once popped up, it will re-open when navigating to different screens)

- CrossLock delay slider and auto-mode for TX/RX is now implemented via popup bubble from the status bar – press status bar CrossLock icon once to show press again to hide (no autohide)

- CrossLock sessions now properly destroyed and CrossLock status indicator will go gray as it should

- New consolidated audio I/O screen for mixer-less units puts input and output functions onto one screen ... still works the same as before when mixer is present

- Half measure to get keypad support for very basic operation on the peer list (up/down/enter)

- Improve title bar icons for left/right popout panels – match left menu with the icon on the keypad

- Fix size issue of title bar and status bar that crept into recent versions, this was cascading into creating layout issues on some dialogs

- Stereo/mono channel assignment fixed

- Power/heat improvements (GPU changes)

- Touchscreen reset fix

- Bump to Qt 5.9.2 release

II. INTRODUCTION

Congratulations on purchasing the Comrex ACCESS NX codec system with CrossLock technology. Since ACCESS was introduced over a decade ago, it has become the world's leading IP audio codec. And in that time, IP transmission technology has developed significantly. We've taken our world-class platform, along with the last decade of technical growth, and built a brand new platform for the future – ACCESS NX.

Designed from the ground up as a platform for CrossLock, our sophisticated custom reliability layer, ACCESS NX is the next step in innovative portable broadcasting.

UNPACKING AND CHECKING CONTENTS

The following items are shipped with a new ACCESS NX Portable:

1 ACCESS NX Portable Stereo BRIC IP Codec

2 Lithium-Ion Battery

3 Edimax Wi-Fi USB Adapter

4 DC Power adapter with cord

5 Manual on CD

6 Printed Quickstart Guide

7 Warranty card*

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

ABOUT ACCESS NX PORTABLE

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

ACCESS NX Portable has several features:

- Intuitive 5-inch capacitive touchscreen
- Built-in Ethernet port
- 2 USB ports for use with the supplied Wi-Fi adapter, compatible USB 3G/4G modems, Comrex Connect modems or the optional POTS modem
- Battery Pack with internal charger (capable of up to 6 hours of power when fully charged with no accessories)
- Switchboard Server
- CrossLock Technology

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 800-237-1776. Product information along with engineering notes and user reports are available on our website at 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.

III. CONTROLS AND CONNECTIONS
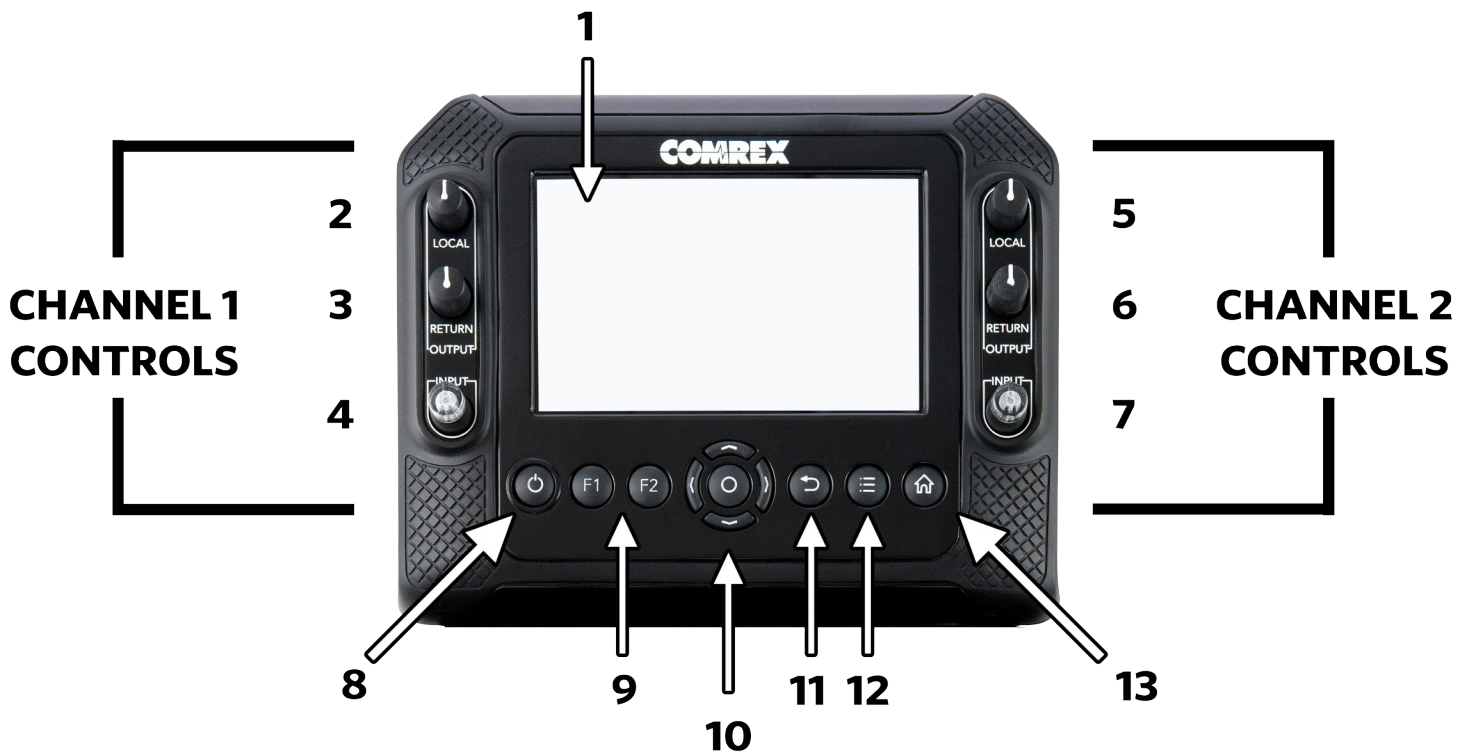
FIGURE 1   **FRONT PANEL DIAGRAM AND DESCRIPTIONS**

1   **DISPLAY** – Touchscreen display. This is where you initialize your broadcast from the NX to the studio unit (typically an ACCESS Rackmount), view and edit settings, and monitor connections.

2, 5   **CH1 and CH2 LOCAL OUTPUT control knob -** Adjusts the level of local audio to the corresponding headphone jack.

3, 6   **CH1 and CH2 REMOTE OUTPUT control knob -** Adjusts the level of remote audio to the corresponding headphone jack.

4, 7   **CH1 and CH2 INPUT control knob** - Use this knob to adjust the level of **INPUT** audio (CH1 and CH2 XLR inputs that you are sending back to the studio.)

8   **POWER KEY -** Hold this down for 3 seconds to turn the NX on or off.

9   **F1 & F2 KEYS** - The F2 key scrolls through several important screens including Audio Inputs, Audio Outputs, Control Dashboard and Remote Connections. F1 will be implemented in future firmware.

10   **DIRECTION CURSORS & ENTER KEY**S - May be used instead of touchscreen to navigate and select options in the user interface.

11   **BACK KEY -** Brings you to the previous screen on the interface.

12   **MENU SELECT KEY -** Opens the menu items on the interface.

13   **HOME KEY** - Navigates to the **Remote Connections** homepage.
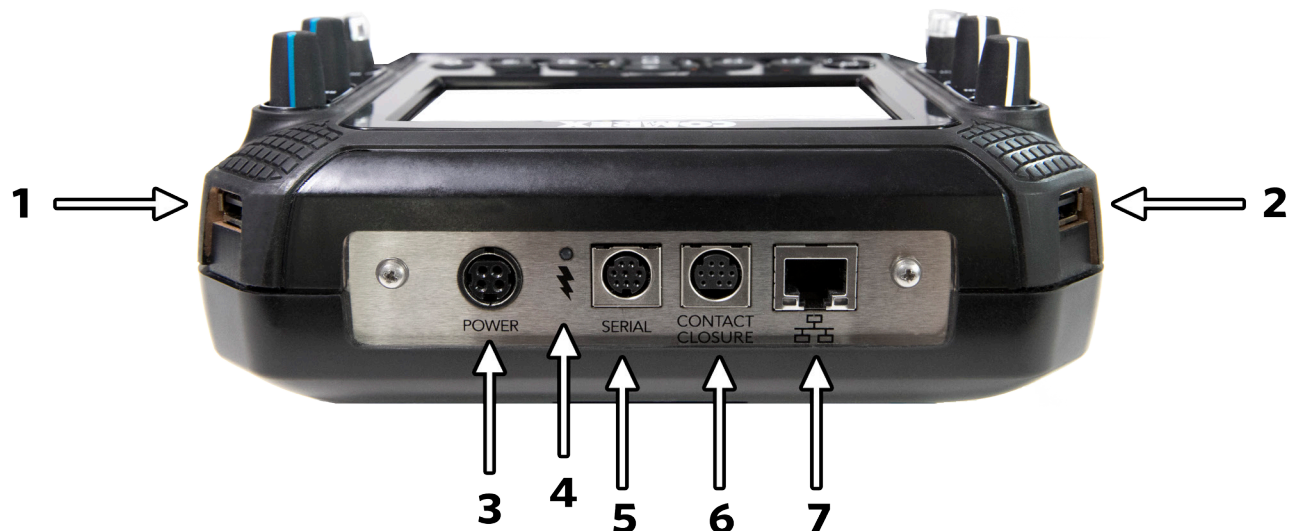
1, 2 **USB HOST PORTS** - These ports are for connections to the included USB Wi-Fi adapter, Comrex Connect Modems, compatible USB 3G/4G devices and the optional POTS modem. To learn how to use two networks simultaneously, go to the **CrossLock Details** section on page 67 for details.

   NOTE: Not all 3G/4G modems are compatible. Check our website for compatible modems at http://www.comrex.com/products/compatible-3g4g-modems or contact techies@comrex.com

3 **POWER CONNECTION** - 4 Pin connector for attachment of Comrex approved DC power adapter. Requires 24V DC @ 1A (Be sure to use only Comrex supplied power adapter.)

4 **CHARGE INDICATOR** - Indicates the battery charging state: Red = Charging, Green = Fully Charged.

5 **SERIAL JACK** - This is an 8-pin mini-DIN jack for connection of a serial cable to facilitate ancillary data transfer. See the next section **PINOUTS** for more details.

6 **CONTACT CLOSURES** - This 9-pin mini-DIN jack is used for contact closure input and outputs. See the next section **PINOUTS** for more details.

7 **1000 BASET ETHERNET** - For connection to wired IP networks.

IMPORTANT: Make careful note of the direction you are plugging the power into the connector. The arrow on the connector should be facing down when connecting to the NX. The same applies to the Serial cable. The Contact Closure cable will have the flat section facing down.
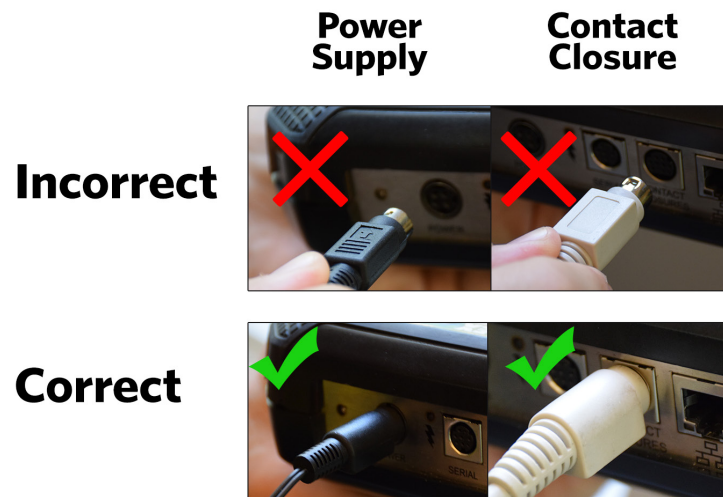
FIGURE 3   SIDE PANEL DIAGRAM AND DESCRIPTIONS

1 **MIC/LINE IN** - 3-pin female XLR connectors designed to accept a balanced, microphone or line level audio feed. This input level is adjustable via the **INPUT** control knob for each channel respectively. There are 3 input settings: **Line, Mic HI** and **Mic LO**. **Mic LO** is for standard dynamic microphones. **Condenser mics** or **"Sportscaster"** headsets should use **MIC HI.**

2 **HEADPHONES** - This 3 conductor 1/4" connector is designed to deliver audio to stereo headphones. The output audio can be user-adjusted by the **LOCAL** and **RETURN** knobs on the top of the unit.

3 **LINE OUT -** This 3 conductor 3.5mm connector delivers unbalanced stereo output audio. The output is selectable in the software to be either **Local**, **Return**, or both.
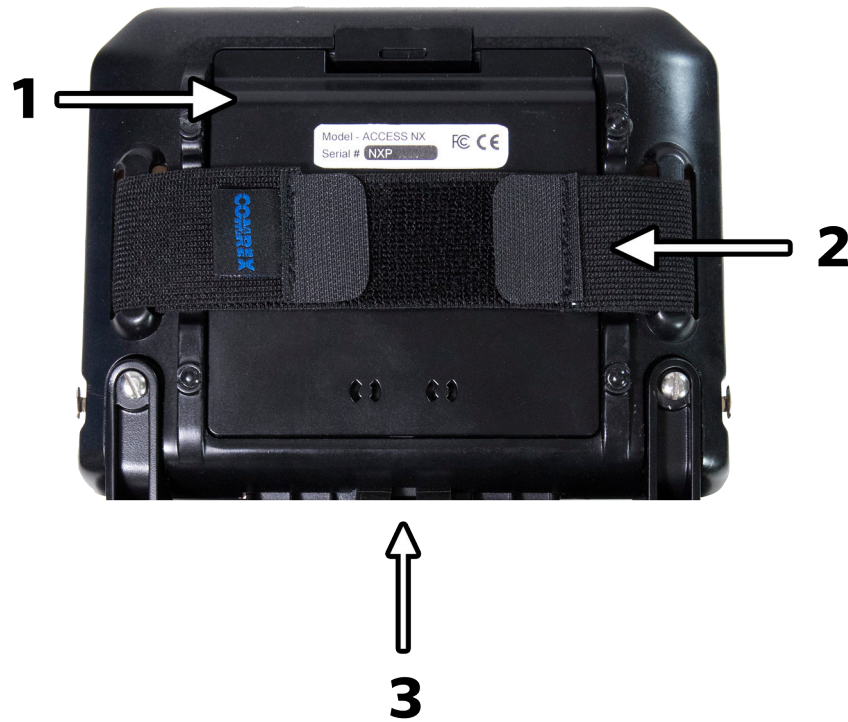
FIGURE 4 **REAR PANEL DIAGRAM AND DESCRIPTIONS**

1 **BATTERY COMPARTMENT** - This internal battery compartment holds the supplied Lithium-Ion battery.

2 **ADJUSTABLE STRAP** - Use this padded adjustable strap to carry the unit.

3 **MIXER PORT** - This connector is for docking to the optional 4 channel NX Mixer.

MONO VS. STEREO

Because NX 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. There are separate mono/stereo settings for each input channel, as well as a setting to determine whether your audio encoder has one or two channels.

Inputs - When inputs are configured for mono mode, CH1 & CH2 (and 3-6 when mixer is attached) inputs are always delivered to both the left and right encoder inputs. This means that when you are encoding audio in stereo, these signals are sent to both channels equally. When using profiles with mono encoders, only the left channel of the stereo line input is delivered to the mono encoder.

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

IV. A SIMPLE NX REMOTE BROADCAST

In this example, we will show you how to set up a simple broadcast with an NX in a remote location using a compatible 4G Verizon adapter.

As shown below, the reporter has a microphone connected to the **MIC/LINE IN** XLR connector. Headphones are connected to the **Headphone** output. The Verizon adapter is plugged into the USB port on the top of the NX.

Verizon 4G adapter

Headphones

STEREO LINE IN

MIC/LINE IN

1
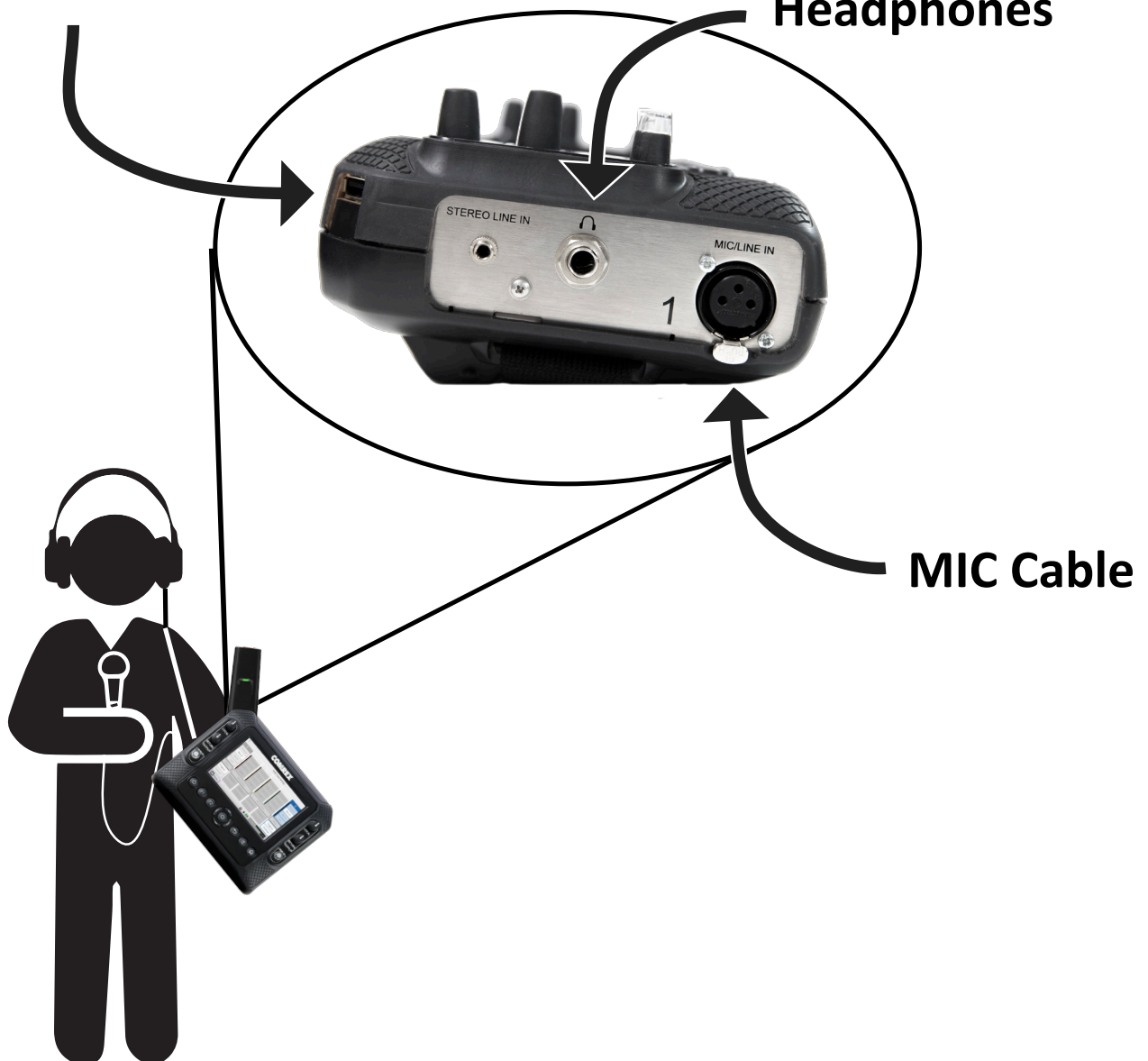
MIC Cable

With the device powered on, verify internet connectivity with the Verizon modem. On the NX display in the bottom status bar, any connected network will be displayed. Click on the 4G device listed, and an IP address will appear if you are successfully connected to the network.
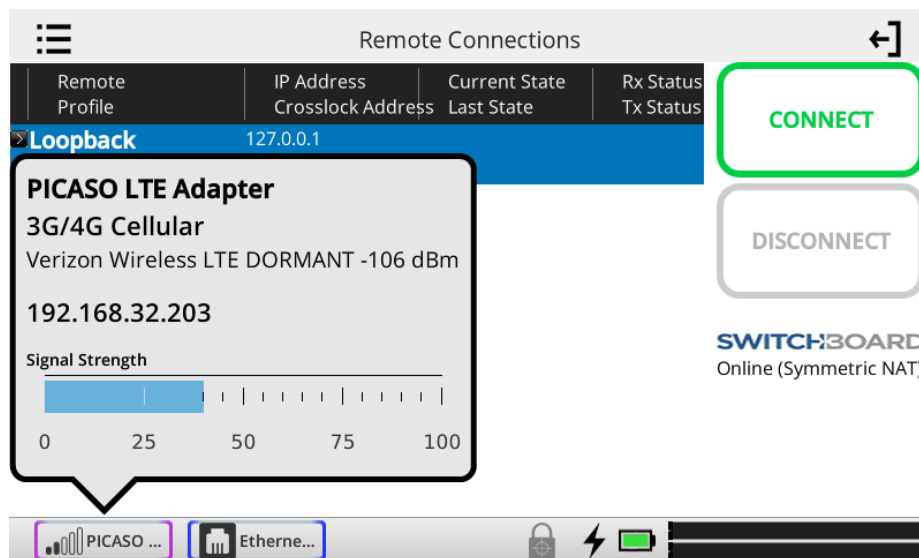
Let's assume your codec fleet has an account on the Comrex Switchboard server (explained in the **Introduction to Switchboard** section), and both ends of your connection are properly registered with it in advance. Navigate to the **Remote Connections** menu by pressing the home key under the display. This page contains the information needed to connect to a device. Units that are in your Switchboard account on the same contact list will automatically appear in this list with a gear icon next to it.

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

Once finished, select **Disconnect** on the right of the screen.

Audio level meters for both the local and return (remote) audio are in the bottom right of the display. Adjustments can be made on the audio levels being sent to the studio and on your headphones using the knobs on the corresponding channel of the NX.

v. INTRODUCTION TO CROSSLOCK

CrossLock is an enhanced reliability layer that can be added to links made between Comrex codecs. CrossLock is optional but recommended, and is available in all Comrex codecs running firmware 4.0 and higher. In the case of connecting to Comrex codecs with earlier firmware, CrossLock is not used.

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

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

The overall result of CrossLock's function means a higher level of reliability for remotes. This goes a long way towards eliminating the frustration of dropouts and other failures during a broadcast.
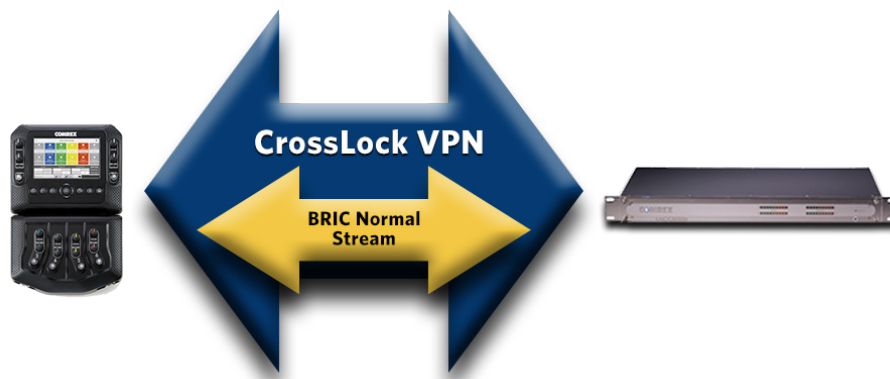
In addition to carrying the audio media, **CrossLock** allows lots of other information to be shared between the endpoints, including information about network quality and far-end delay settings. This provides for much better delay management on both ends of the link.

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

For more information CrossLock, go to the **CrossLock Details** section on page 67.

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

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

When codecs are turned on and have network connectivity, they open a channel to the **switchboard.comrex.com** server, and provide the current public IP address, connection status, firmware revision, and the type of router (if any) that exists in the link.
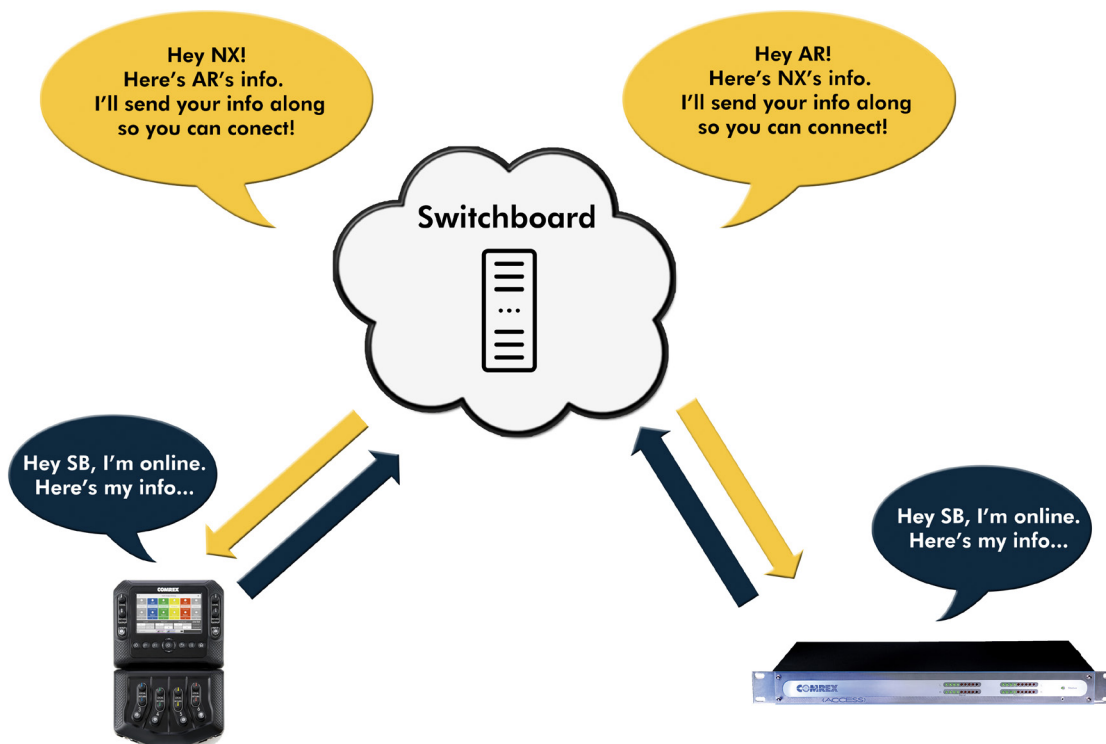
Switchboard recognizes devices by their MAC address and provides information to any units in the same Switchboard fleet that are also online.

To learn more about Switchboard and how to utilize it with your codecs, visit the **Switchboard Details** section on page 67.

GETTING STARTED WITH NX

POWERING UP NX

NX can be powered from its internal battery or an external supply. The internal battery has a low-voltage lockout function that prevents power-up if the battery voltage is too low.

Whenever the external supply is attached, regardless of the whether NX is turned on or off, the internal battery will be charging. The battery status is always available by looking at the rear-panel battery LED (red = charging, green = full).

Power up NX by pressing the recessed power button (left-most on the keypad) for three seconds. The display will "wink" when NX has accepted the keypress. NX takes approximately 30 seconds to boot, and the display will be blank for part of the boot cycle.

POWERING DOWN NX

After use, NX is powered down by pressing the recessed power key (left-most on keypad) for three seconds. Note that if the internal battery is installed and charged, simply pulling the power cord from NX will not result in a shutdown, as the backup battery function will keep NX active.

CONTROLLING NX FROM THE TOUCH SCREEN

NX has a five-inch capacitive touch screen for programming settings and making connections. It might not respond when the user wears gloves or tries to use a stylus or other pointing device. Most functions can also be controlled by the navigation keypad below the display.
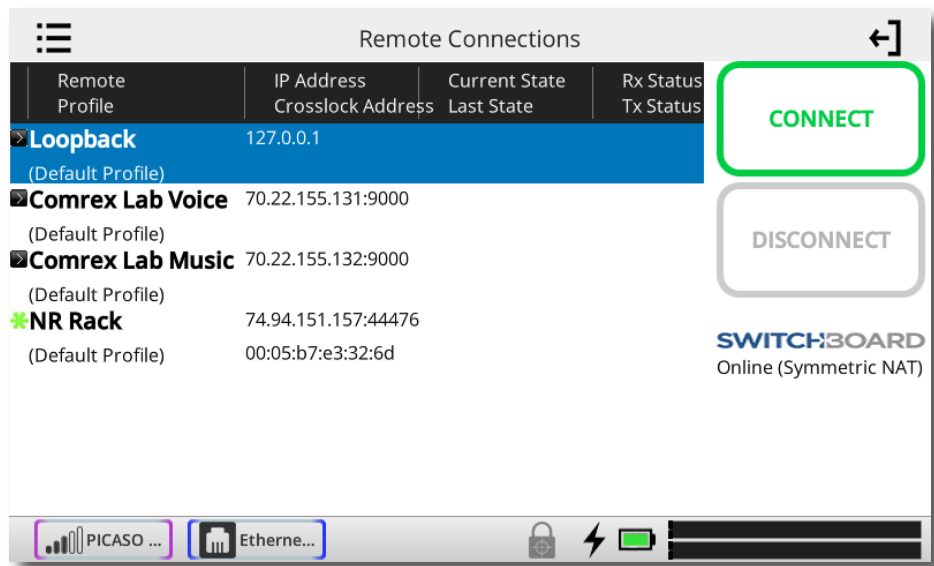
When first booted, NX displays the "**Remote Connections**" screen as shown in the previous figure. Remote Connections is one of the main screens available on NX, and is the default because connections are initiated and terminated from there. Remote Connections can be found easily by pressing the "**Home**" keypad button from any screen.

The other main screens are selected by pressing the Menu icon on the upper left corner of the display. This will open a list of the options on the left side. The "**Menu**" key on the keypad mimics this.
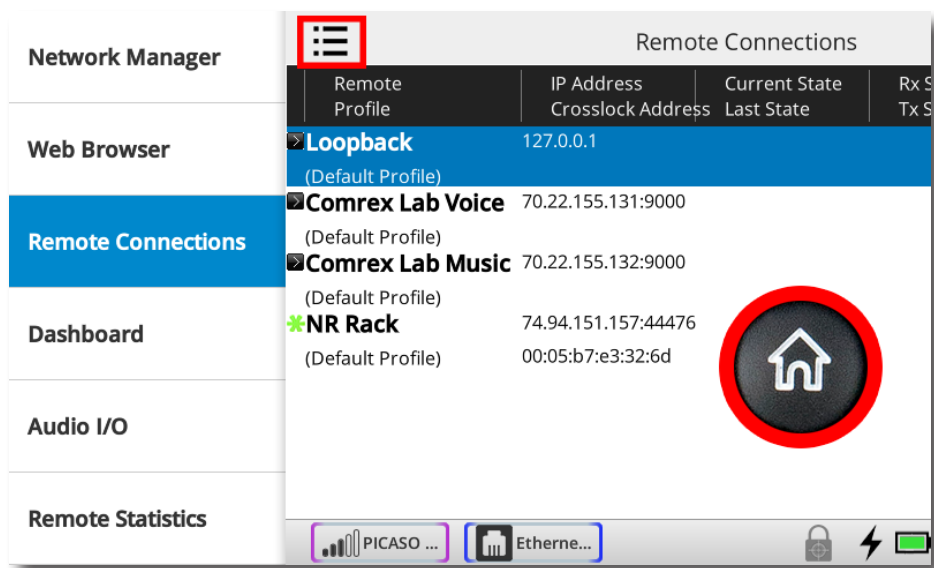
Whenever one of the main menus is chosen, options within that menu can be displayed by pressing the Options icon on the upper right side of the display.
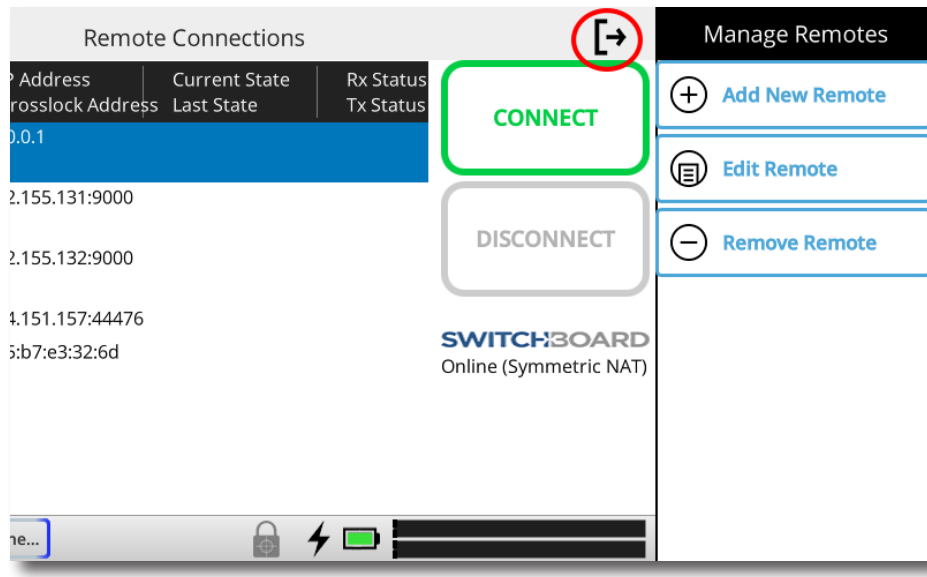
Pressing either the "**Menu**" or "**Options**" Icon again removes the slide-out list.

The main screens available for operation, status and configuration are:

1 **Network Manager** - Configure and check the status of Ethernet and attached network devices like Wi-Fi, 3G/4G, and POTS modems. Allows the creation of "**Locations**" for each device (to save specific parameters in memory) and Wi-Fi scanning, network selection and configuration.

2 **Web Browser** - Used in situations where your network requires "click through" agreement or password entry to connect to the Internet.

3 **Remote Connections** - Add, edit and delete connection destinations, show incoming connections, make outgoing connections, and check Switchboard status.

4 **Dashboard** - Designed to be active during a live feed, provides microphone mutes, control over contact closures, and shortcuts to other audio functions and levels.

5 **Audio I/O**- Configure the inputs for levels (Mic/Line), buss selection and mono/stereo. Adjust output levels and select sources for **Line Out** jack.

6 **Remote Statistics** - Provides detailed information regarding the decoder buffer manager's functions transmit and receive delays, as well as frame loss and correction rates.

7 **Channel Statistics** - Provides real-time graphs of outgoing and incoming data rates.

8 **CrossLock Stats** - Designed to be active during a live feed, displays a range of network statistics like jitter, packet loss and error correction activity in each direction of the stream.

9 **Manage Profiles** - Configure settings for outgoing calls like encoder/decoder and specialized configurations.

10 **System settings** - Configure global NX parameters like Contact Closures, Switchboard, CrossLock, Security and incoming call support.

11 **CrossLock** - Configure CrossLock parameters for remotes utilizing CrossLock.

12 **About** - Displays information about NX firmware, licenses and internal temperature.

Along with the top and bottom status bars, these screens are each outlined in detail in the following sections.

STATUS BARS
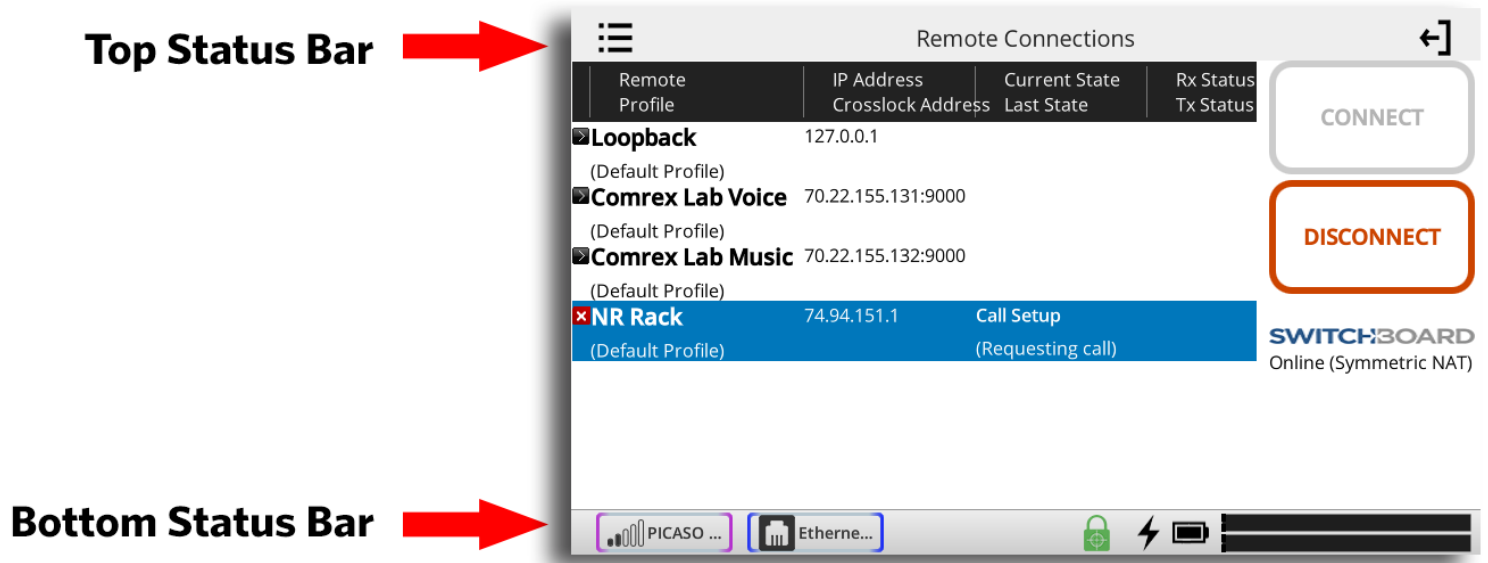
As shown above, every NX screen has the top status bar, describing the currently selected screen, and the bottom status bar, showing the status of networks, CrossLock (if active), battery and audio levels.

Each installed network has an icon that can be selected. Once selected, some basic network status will be displayed (e.g. Ethernet IP address).
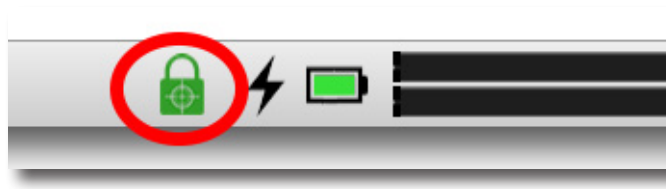
The CrossLock icon will light green when a CrossLock connection is active.

Note: CrossLock can sometimes be active before or after a remote connection is active.

Charged

Charging
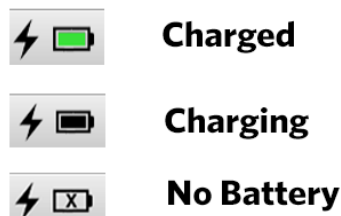
No Battery

The battery icon shows charging status or current level of the internal battery. Battery is always in charging state (or charged state) when the external supply is attached. If battery is disconnected, this icon will show an "X" over the icon.
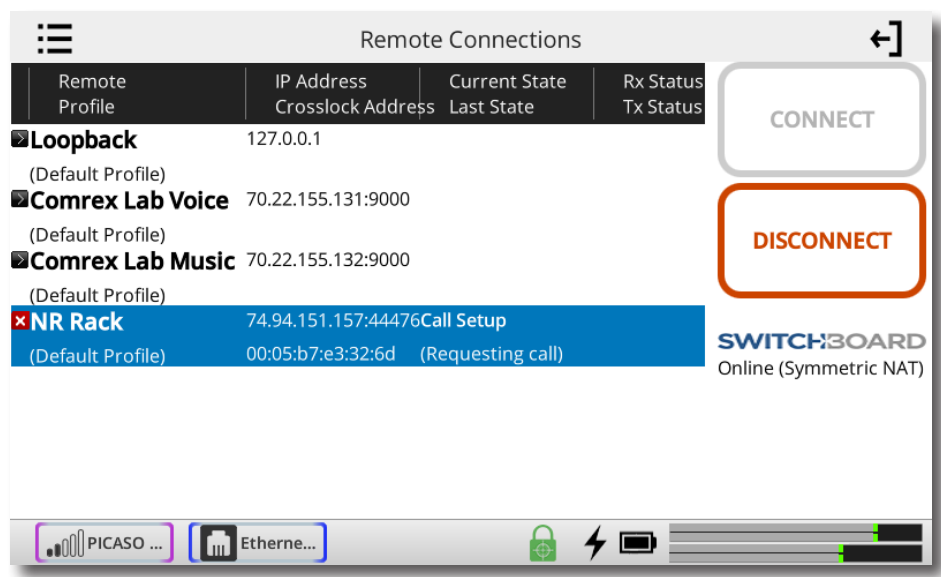
The level meters show the current audio local input level (top) and the current return audio level (bottom). The meter is stereo, and mono sources reflect on both L&R channels. This is designed as a "peak" meter, and proper audio levels should remain below the right side of the meter.

VIII. MAKING CONNECTIONS WITH NX (REMOTE CONNECTIONS SCREEN)

NX connections are made via the **Remote Connections** option in the main menu. Besides giving you list of all possible outgoing connections and active incoming connections, the **Remote Connections** screen displays Switchboard status, showing whether your NX is currently synced to the Comrex Switchboard server.

Outgoing connections are made in one of two ways:

> **Via Switchboard (recommended)** - Connections via the Comrex Switchboard server are the easiest to make. Once NX syncs with its Switchboard account, it will display an active list of other Switchboard account members. You don't need to know the IP address or any other info about your Switchboard members, you simply select one and press "connect".

> **Manually (using a discrete IP address)** - You'll need to enter the information manually for the codec you wish to connect to.

Outgoing connections can be of two types:

> **CrossLock connections** - the Comrex CrossLock reliability layer is established to the remote codec ahead of the call, and disconnected about 60 seconds after the of the call. Error correction and multiple networks are supported

> **BRIC Normal connections** - Legacy mode to connect with Comrex devices that have older firmware or don't support CrossLock for other reasons.

Because there are two ways to connect, and two types of connections, we'll discuss all these combinations, in order from simplest to most complex.

CONNECTIONS WITH SWITCHBOARD

Outgoing Switchboard connections are easy. The IP address and CrossLock choice is made automatically by Switchboard. If the Switchboard connection is active, you can select any of the Switchboard connections that appear, and select the Options icon on the upper right corner. You can then choose the "**Profile**" option and select which profile is used to make the connection. Profiles determine encoders used and other parameters). If no selection is made for profiles, the call will proceed with the default profile of Opus mono.
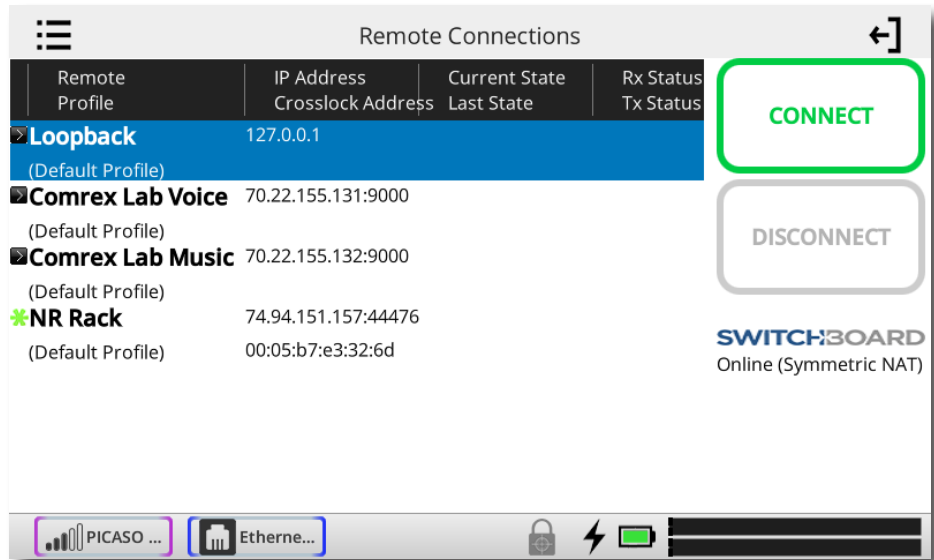
The icon that appears next to the Switchboard member is color coded to show status:

> **Green** - ready to accept call
>
> **Red** - busy
>
> **Gray** - offline

If Switchboard determines that a CrossLock connection can be made, it will opt for that. If not, it will attempt a BRIC Normal connection.

MANUAL CONNECTIONS WITHOUT CROSSLOCK (LEGACY BRIC-NORMAL MODE)
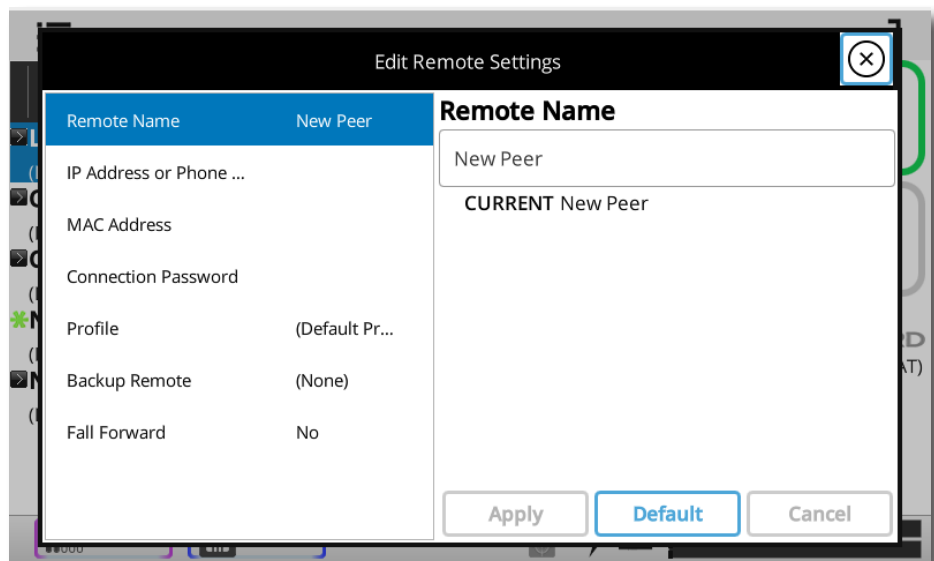
To make a manual BRIC Normal connection, you'll need to input the destination information to create an entry in the **Remote Connections** list. Select the Options icon and choose "**Add New Remote**". You'll be prompted to enter the following into the Edit box:

> **Remote Name** - Familiar name to call this entry

IP Address or Phone number - The public IP address of the destination (phone number for POTS calls). If using non-default ports, add the port number after a colon.

Profile - Select which profile is used to make the connection. (Profiles determine encoders used and other parameters - see the **Profile Manager Menu** section on page 41.) If no selection is made for profiles, the call will proceed with the default profile of Opus mono.

MANUAL CONNECTIONS WITH CROSSLOCK

Follow the directions above for Manual Connections without CrossLock, but in addition, add the Ethernet MAC address of the codec you'll be connecting to. This is an added security layer to ensure only authorized codecs connect via CrossLock.

It's important to note that in order to connect this way, the receiving codec must also have a matching entry including the MAC address of the calling codec. This must be present as an outgoing entry (even if the entry is never actually used for outgoing calls).

If these conditions aren't meant, or if the receiving codec is not CrossLock capable, a legacy BRIC Normal style connection will be attempted.

OUTGOING CALLS

Choose the manual or Switchboard entry desired and press the green "**Connect**" button. Call progress and status will appear on the entry. If a CrossLock connection is established, the "**lock**" icon on the status bar will light green.

INCOMING CALLS

No action is necessary to receive incoming calls on NX. Whether via Switchboard or manually, NX will automatically connect compatible incoming calls and show them in the remote list.
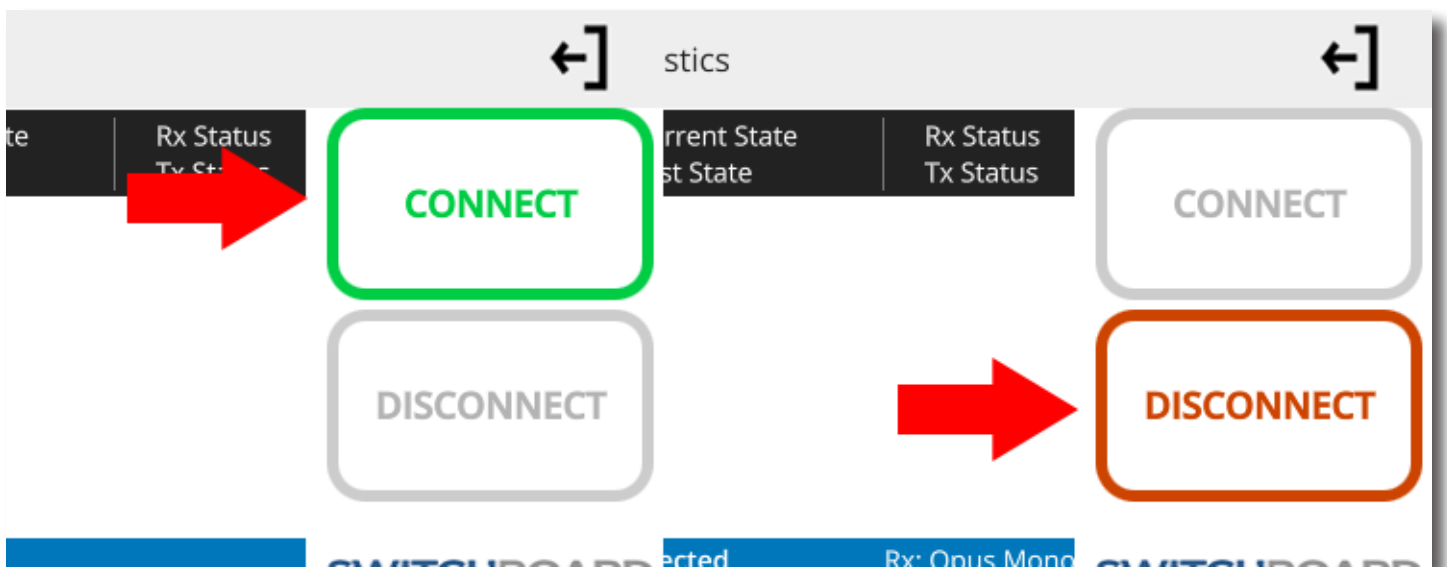
On the left side of the **Network Manager** screen, NX presents a list of all network adapters (4G, Wi-Fi etc) that have been attached to NX, along with the internal Ethernet port.

Note that with the CrossLock feature, it's possible to have multiple active networks simultaneously.

One important element of the **Network Manager** is the concept of **Locations**. A **Location** contains the settings specific to that network adapter for use on a specific network. Examples are use of the Ethernet port on a range of networks, some using DHCP and some using static settings. Using **Locations**, each of these can be stored away separately and recalled when needed. **Locations** are especially useful on Wi-Fi, since the security parameters of wireless networks can be stored for subsequent use.

Each network starts off with a "**default**" **Location**, which can be edited by the user. Some networks don't change config parameters (e.g. 3G/4G, POTS) so a single default **Location** is all that's required.

Networks fall into four distinct classes: Ethernet, Wi-Fi, 3G/4G and POTS modem. Each is discussed in greater detail next.

ETHERNET

Selecting the built-in Ethernet port shows the current status of the network
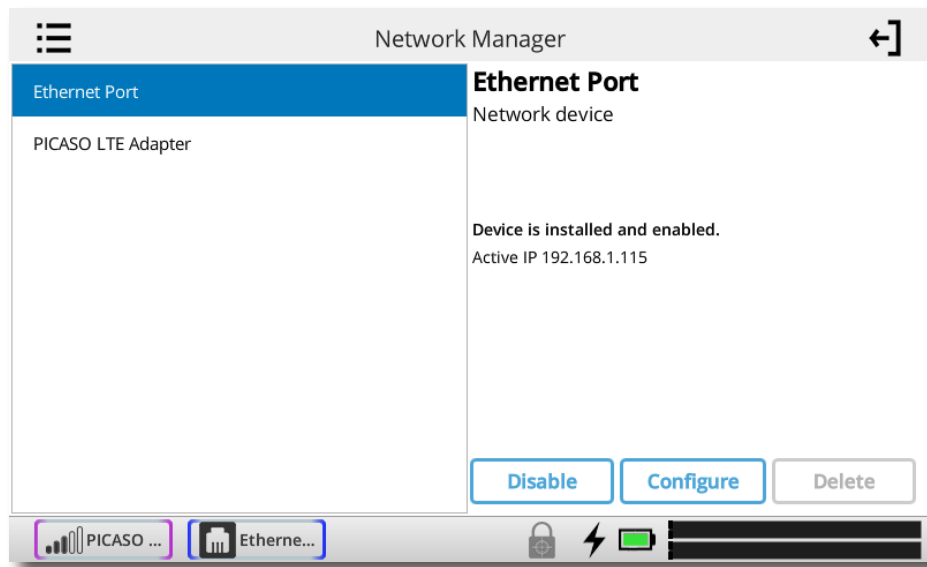
The Ethernet port can be disabled/enabled here and configured for multiple **Locations** from this screen. The internal Ethernet port cannot be deleted.

Selecting **Configure** here will open the configuration pop-up.
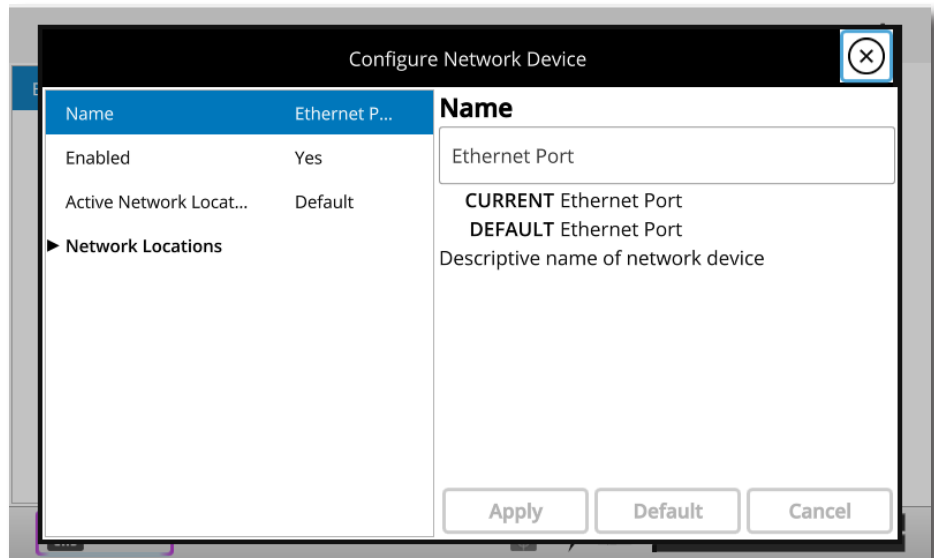
For Ethernet, it's recommended to leave the default network as-is (DHCP) for testing and upgrades, and to add static networks as additional **Locations**. To do this, select the arrow to the left of "**Network Locations**" to expand the Location list. You can then choose "**Add Location**".

You'll then be able to select the new location, rename it, and apply the required information to use the Ethernet Port at the new location. The information required is:

- IP Address
- IP Netmask
- IP Gateway Address
- IP DNS (Primary and Secondary)

Once there are programmed and saved, choose the "**Active Network Location**" option to change to the chosen Ethernet settings and back whenever required.

WI-FI

When the included Wi-Fi adapter is attached to one of the USB ports, a network entry of "**WLAN Adapter**" will appear.

Selecting it will show the status, current IP address, and network chosen (if any).
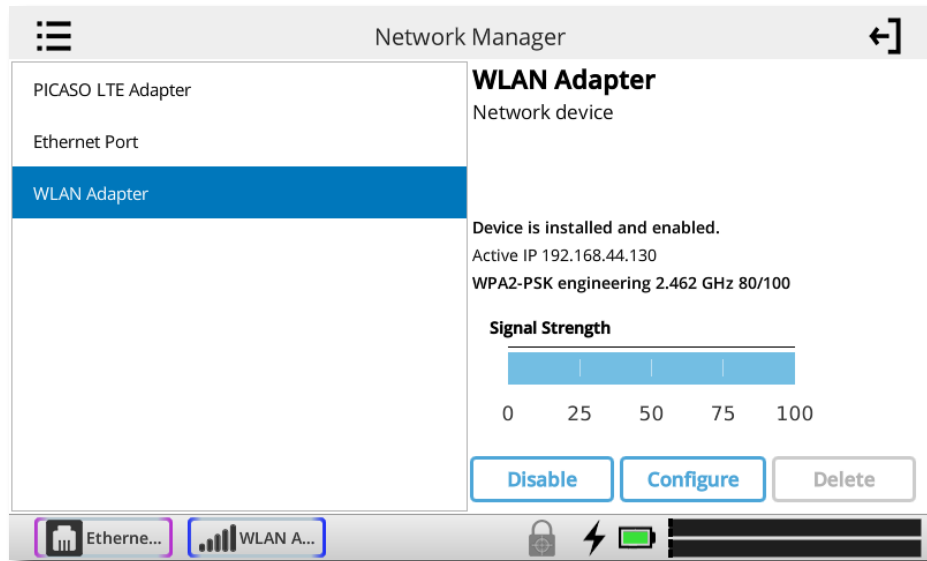
When you first attach the Wi-Fi adapter, you must enable it before using it or scanning with it. You can enable the Wi-Fi adapter by selecting it in the list and selecting **Enable** or choose "**Enabled**" under the WLAN option and set it to "**Yes**"

NX allows you to "scan" for active Wi-Fi Access Points, much like a computer or smartphone. This is done via the "**Locations**" option under the WLAN adapter. Pressing "**Scan**" will deliver a list of active Wi-Fi networks. You can choose a network from the scan results, choose "**Add Location**", then edit the location for WEP or WPA passwords.

3G/4G

Cellular-based wireless modems will appear as their model name. Under most circumstances, the default settings are correct for these modems, and they are enabled by default. It is possible to modify the APN setting if the default is not correct by choosing the SIM option under configuration and choosing "**APN**". You can input the new APN value into the field manually.

You can also choose among pre-programmed APNs based on the list of carriers programmed into NX. By setting the "**Region**", "**Country**" and "**Carrier**" option, the list will suggest the proper APN setting for your carrier.

POTS

When the optional POTS modem is attached to NX, the POTS modem will appear in the network list. Other than enabled/disabled (enabled by default), there are no user configurations for the POTS modem.
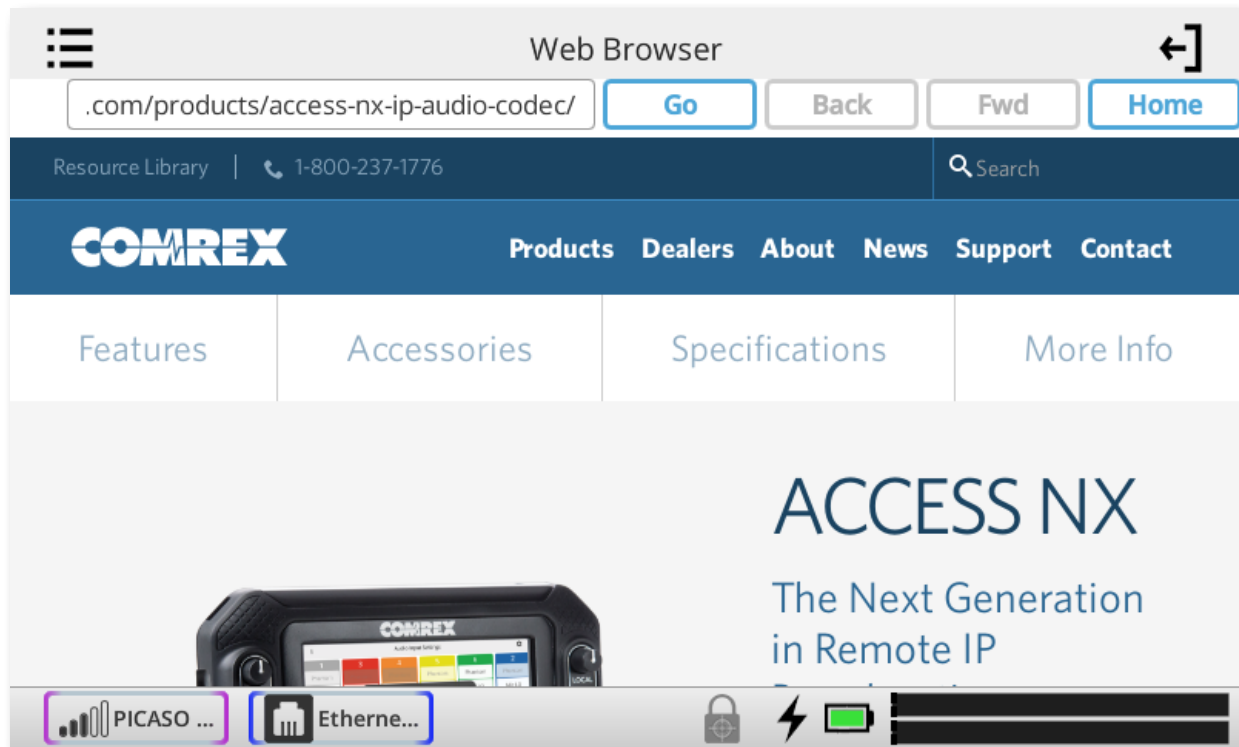
This option enables the built-in web browser in NX. The browser has all basic functions of your typical mobile browser, including SSL security and javascript. The browser is designed to be used on networks that require authorization (beyond Wi-Fi security). As an example, many hotels or retail stores redirect web users to a page, asking to accept terms or input passwords. Once a different screen is selected via the main menu, the browser stays in the background and keeps the last page open.

Besides breaking through web authorization pages, the browser is a great way to test for Internet access in general (e.g. on wireless networks when connection status is unknown).

The NX browser does not auto-update with security patches like most mobile browsers, so it's advised not to perform security-intense functions on it, like banking or email.

The dashboard screen is designed to provide common functionality to the user when streaming live audio.
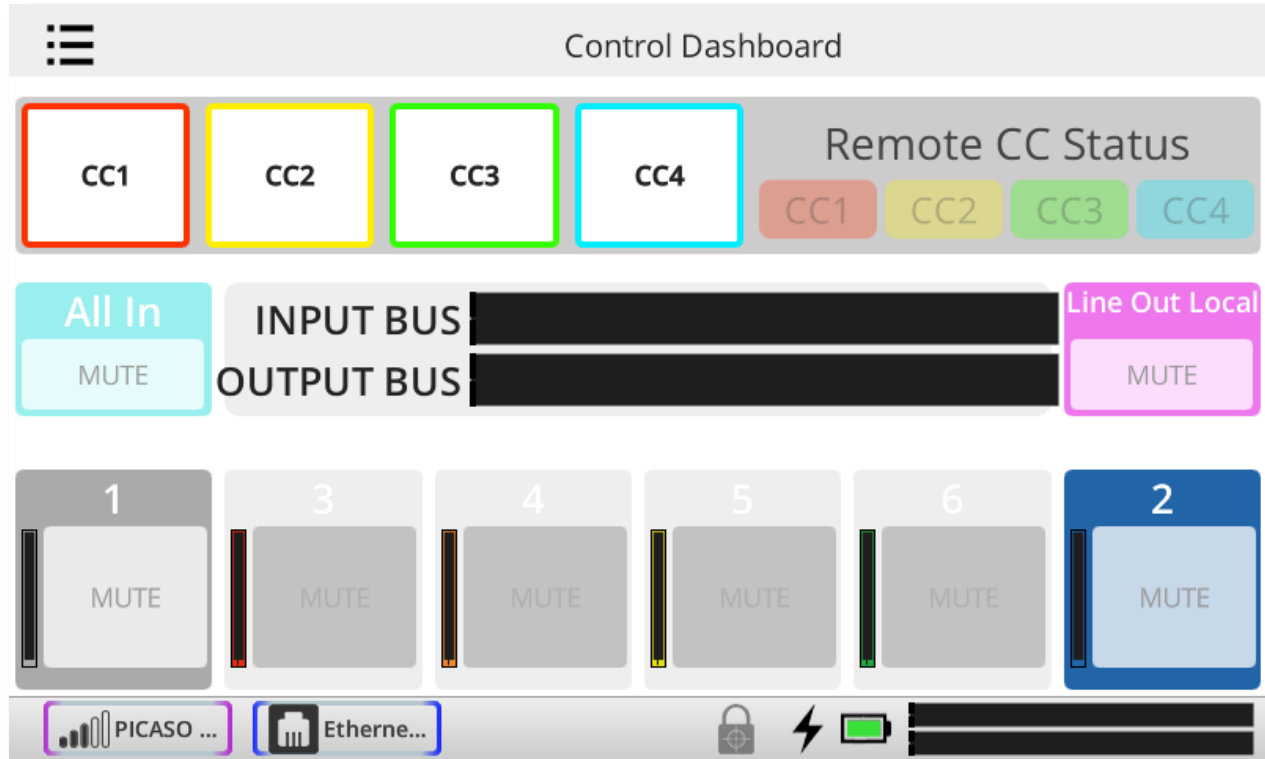
The sections are:

1. **Contact Closure triggers** - in parallel with the physical contact closure connector, allows the sending of four end-to-end closure signals.

2. **Remote Contact Closure status** - Indicates the current state of the contact closure outputs (sent from the far end).

3. **"All In" Mute** - A toggle button to mute all the inputs to NX. This will be reset when a connection is dropped, or if the unit is powered down.

4. **Input/Output Meters** - A larger version of the small meters on the status bar.

5. **"Line Out Local" Mute** - Toggle that allows temporary muting of the local audio (if enabled in the output menu) from the line out jack. Useful in remote broadcast scenarios with a PA feed during commercial breaks.

6. **Individual Mic Mutes** - Toggles to temporally muting individual inputs, without affecting the input level settings. Channels 3-6 will disappear if the optional mixer is not attached.

AUDIO INPUTS

NX has two adjustable mono audio input channels, and one fixed level stereo input. With the addition of the optional mixer, an additional four mono inputs are available. Each adjustable channel has a level indicator built into the input adjustment knob. The knob will light green (OK), yellow (hot) and red (limiting) on each channel. The audio input settings select the levels and destinations of each of these channels.

LEVELS

The Mic/Line input channels have three fixed preamp settings. **Mic LO** is designed for dynamic microphones and other low level sources. **Mic HI** is designed for use with condenser or other high level microphones. **Line** level is designed for sources at professional line levels. In addition to choosing the levels, each channel can selectively apply a 12V phantom power source for condenser microphones (when in mic modes).

The two microphone options are available because many sportscasters use condenser-based headsets with a microphone placed very close to the mouth. This has a tendency to clip the high-gain preamplifiers designed for lower level mics.

MONO/STEREO

Rather than a pair of mono inputs (which get mixed into both channels of stereo encoders), pairs of input channels can be configured as L & R stereo. This is possible on the combination of channels 1 & 2, and (with the optional mixer attached) channels 3 & 4 and channels 5 & 6. Choosing the "**Stereo**" option on either of the inputs will set both inputs to this mode.

In stereo mode, only the lower number channel has an active input level control. As an example, if channels 1 & 2 are configured for stereo, only channel 1 input control is used to control both channels. Channel 2 input control has no effect.

BUSSES

NX has two audio busses for input sources

> **Program** - Audio that is sent to the encoder for streaming to decoders

> **Producer** - Audio that is available to the headphone feeds, but not to the encoders

Each adjustable input can be assigned to one or both of these busses using the buttons for those channels. The fixed line input can only be sent to the program bus.

AUDIO OUTPUTS

The NX headphone outputs each have two control knobs, one to adjust level of the locally generated program (Local), and one to adjust level of the audio being decoded by NX (Return). The audio input and output screen gives an indication of the current setting of each of these knobs for each headphone out.

Each headphone output can be configured to add the "producer" bus to the return audio feed. If this is selected for a specific headphone, the producer feed sums together with the return audio at a fixed level. The "return" level control adjusts both audio feeds together.

The feed available to the fixed-level line output is selectable here as well. The port can output the **Local** audio, the **Return** audio, or a mix of both. The producer feed can not be applied to the fixed line-level output.

WITH MIXER ATTACHED

If the optional mixer is attached, the menu **Audio I/O** will "split" into two separate menues: **Audio Inputs** and **Audio Outputs**. The **Audio Inputs** menu will display only the Inputs, and the **Audio Outputs** menu will display only the Outputs.

AUDIO INPUTS SETTINGS WITH MIXER

AUDIO OUTPUT SETTINGS WITH MIXER

XIII. STATISTICS MENUS

There are three different statistics menus available. The **CrossLock Stats , Remote Statistics,** and **Channel Statistics.**

When making a CrossLock connection, it is best to refer to the CrossLock stats to analyze performance. The Remote and Channel statistics menus are available during a CrossLock connection because the legacy BRIC Normal protocol is still running while a CrossLock connection is active. When you are not utilizing CrossLock, the CrossLock stats menu will be blank, and you should refer to the Remote and Channel statistics.

CROSSLOCK STATS

The **CrossLock Stats** menu gives a real-time indication of network activity and quality during a CrossLock connection. You can determine how many networks are being utilized, the delay associated with both ends of the connection, loss and recovery of packets. It's a powerful tool to help analyze system performance.
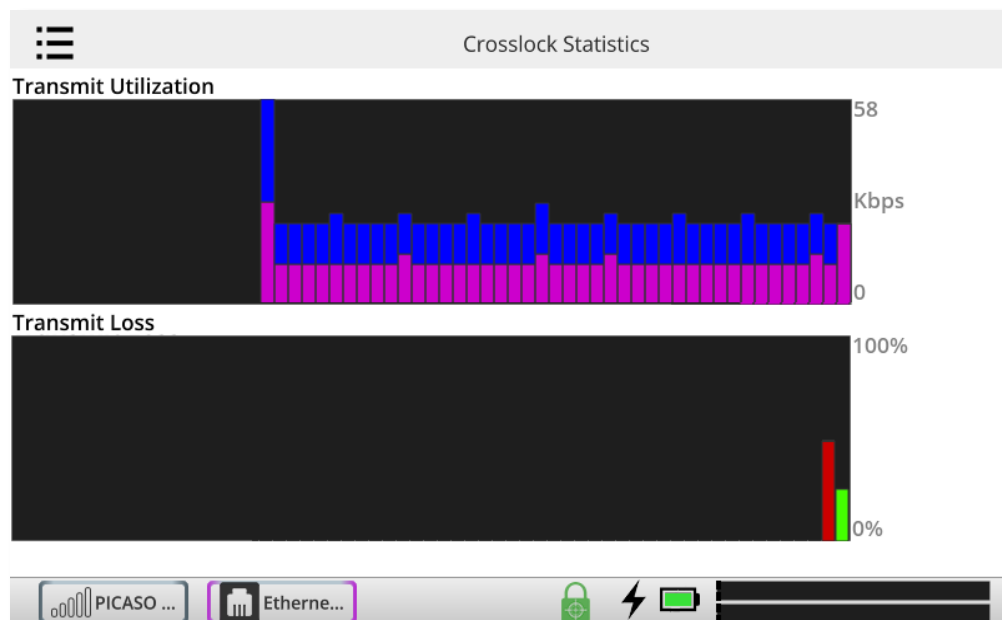
The first screen to appear is the transmit performance screen. An identical screen showing receive performance is available by swiping this screen to the left.

The statistics screens are divided in half into two real-time histograms, moving from right (now) to far left (60 seconds ago).

The top meter shows network utilization, showing data rate on an autoscaling graph. In the case of CrossLock connections using multiple networks (bonding or redundancy mode), the graph will be color-coded to show utilization of each network. Note that CrossLock has license to apportion data dynamically between networks, including making the choice not to use a network at all. This usually happens when CrossLock determines one network to have significantly lower delay and sufficient bandwidth.

The bottom meter shows loss and error correction functions. On good networks, nothing should appear here. The information displayed here is color coded:

> **Packet Loss (dark red)** - The system has detected a packet has been completely dropped by the network and was never received by the decoder.

> **Packet Late (bright red)** - The system received the packet, but it was too late for decoding and playout.

> **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.

REMOTE STATISTICS

The **Remote Statistics** menu represents the work of the Jitter Buffer Manager. The area of most interest is the light blue area as shown below, which illustrates a spread of jitter values (referenced to the current playout pointer) over the last second. If this area covers a large span, the relative jitter is high. If the light blue section of the graph is small or invisible over a time period, there has been very little jitter present.
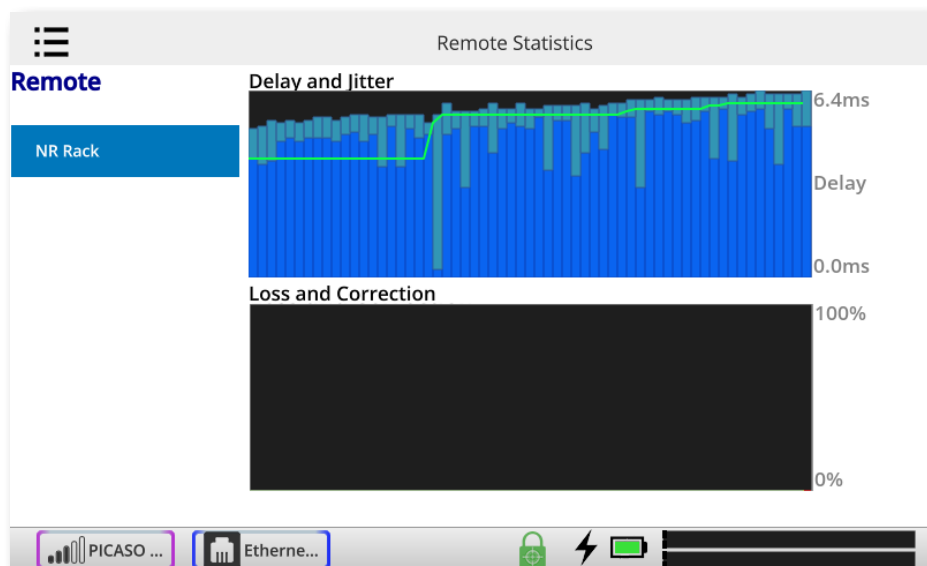
Based on the historical value of this jitter figure, the buffer manager will expand or contract the receive buffer (lengthening and shortening overall delay). The time interval over which this measurement is assessed is called the "jitter window".

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

CHANNEL STATISTICS

The **Channel Statistics** menu provides real-time graphs of outgoing and incoming packets. Each column represents one second of outgoing data, segmented into audio coding data (shown in blue) and overhead, such as IP/UDP headers, RTP headers and similar data (shown in light blue).
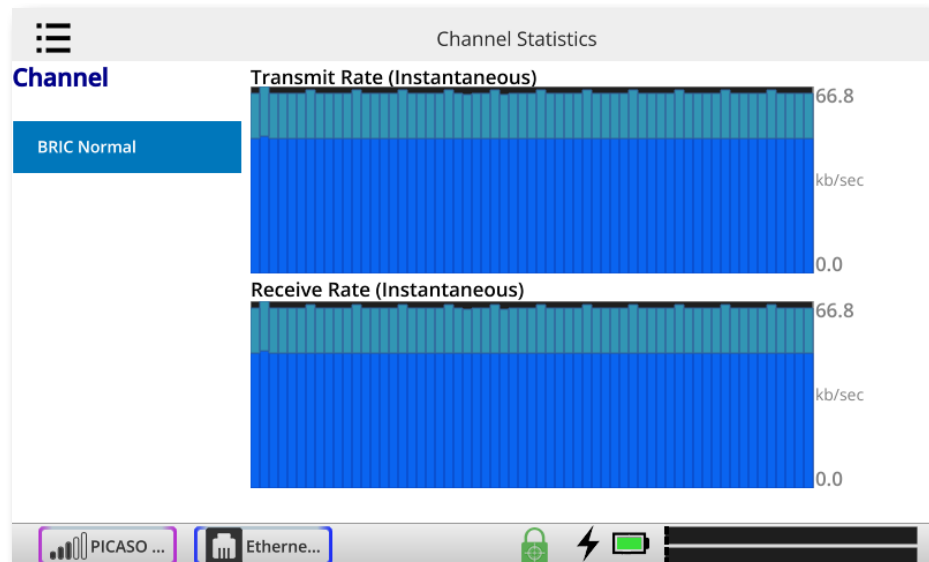
The first screen shows you the rates in real-time. By swiping the screen to the left, it will show you an average of both Transmit Rate and Receive Rate.

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

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

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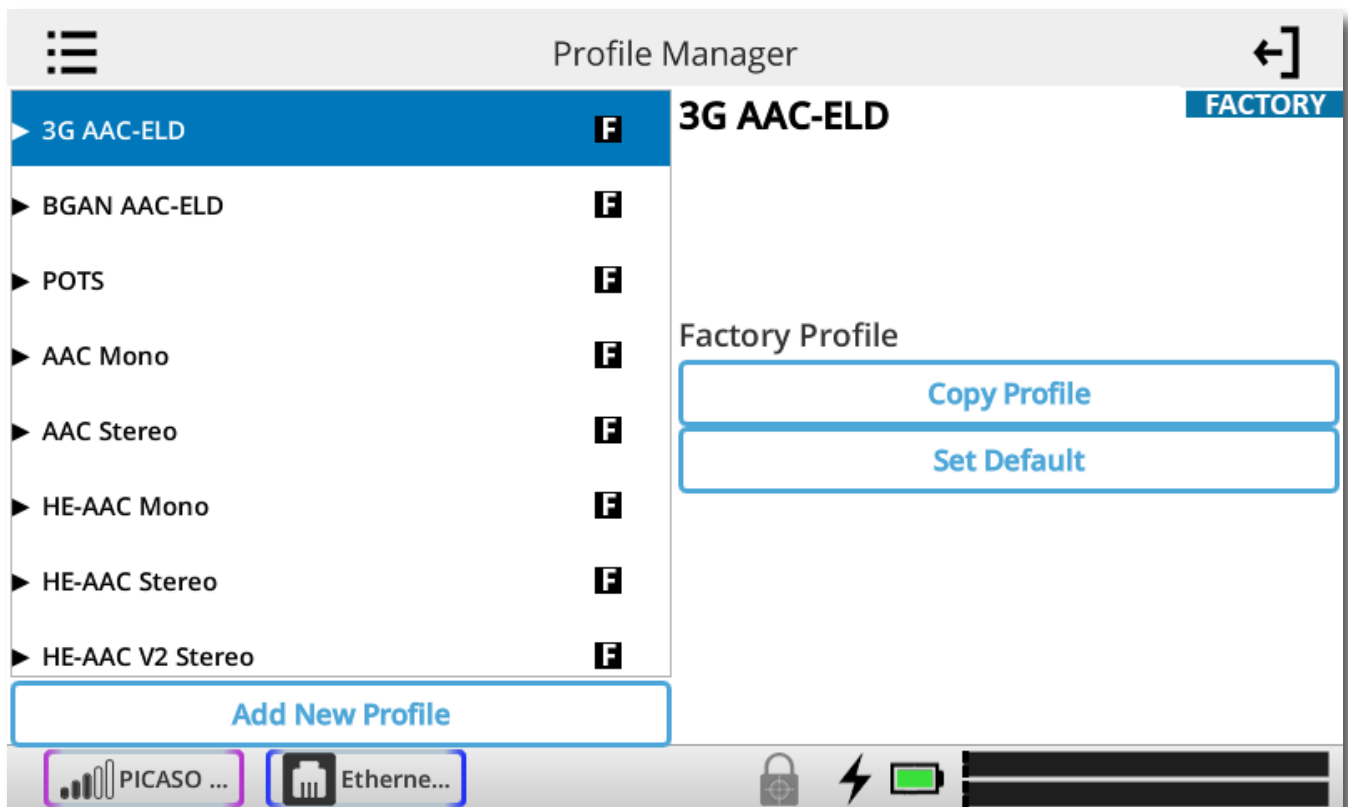
DEFAULT PROFILE

When a new remote connection is created (on the **Remote Connections** screen), a default profile is assigned unless a different profile is selected from the menu on the **Remote Settings** option on the **Remote Connections** menu. The default profile shows a **D** next to it in the list. **OPUS Mono** is the default profile when shipped from the factory. You can change the default profile by selecting it in the list and pressing the **Set Default** button.
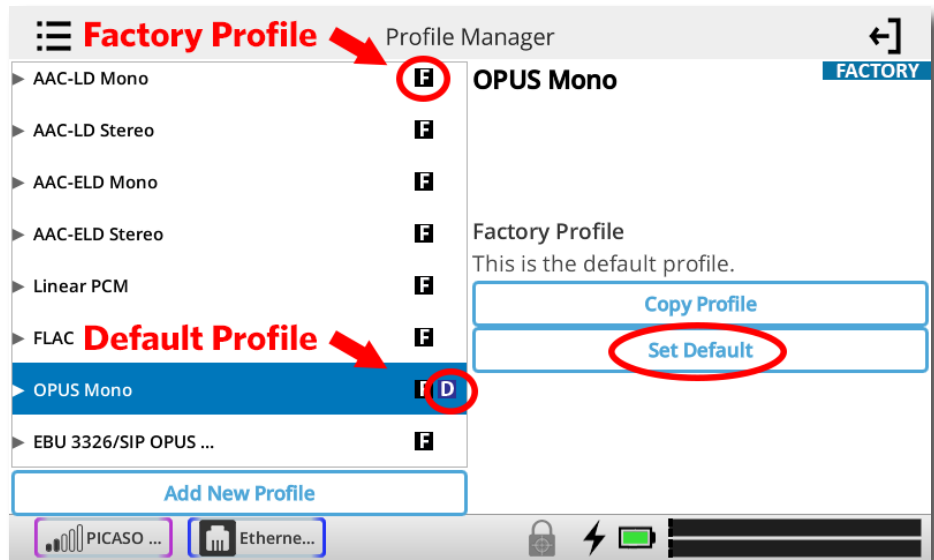
VIEWING PROFILE DETAILS

To view the parameters set for a profile, select the profile in the list and press the right arrow key on the keypad to expand the options. The first two editable entries are **Name** and **Channel**. The default channel type for connecting between ACCESS units is **BRIC Normal**. We do not recommend changing the channel type except for advanced applications.
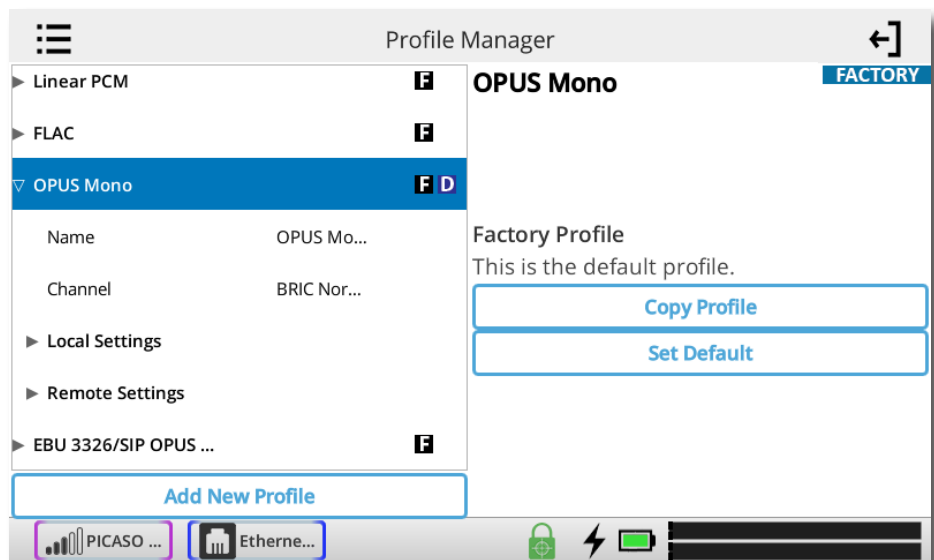
Under the expanded profile, you will also see two additional folders named **Local** and **Remote**.

You'll use the **Local Settings** to determine how your NX behaves, and the **Remote Settings** will determine how the ACCESS on the far end behaves.

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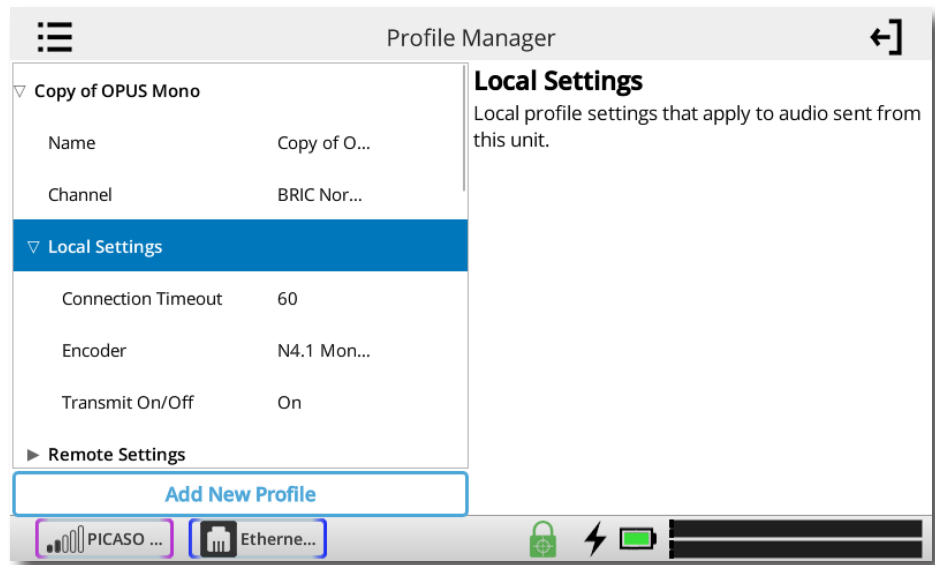
Connection Timeout - Under normal circumstances, a connection will be terminated on one end, and the other end will drop the connection. However, if a network failure occurs, or a connection is ended abruptly for some other reason, the system will drop the connection after a pre-determined time. The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

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

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

EDITING AND ADDING PROFILES
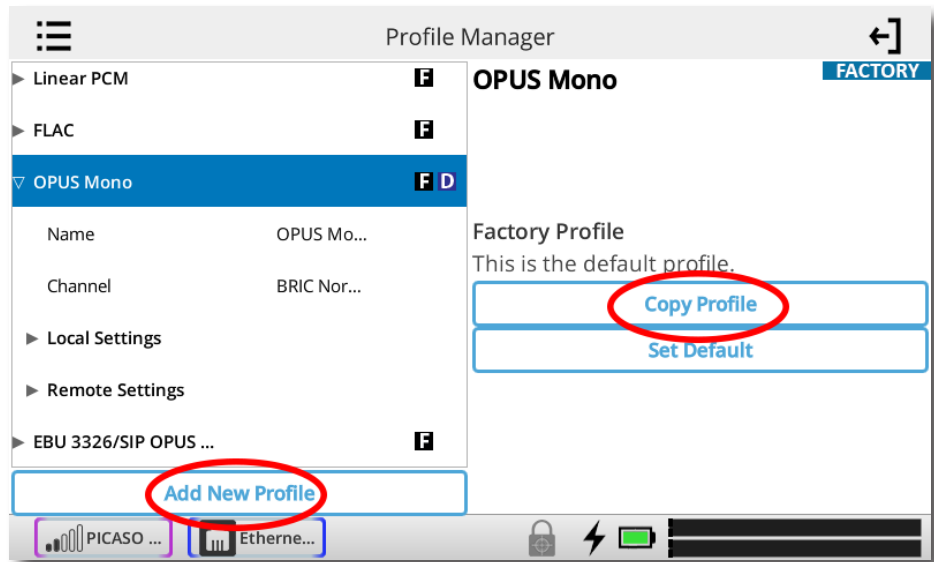
Custom profiles are easy to create on NX. Simply select **Add New Profile** or highlight a profile already in the list and select **Copy Profile.**

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

Profile creation is segmented into commonly used and advanced options. In order to simplify the interface, Advanced options are normally hidden from the user. Once a profile is defined, it will be available from the Profile list.
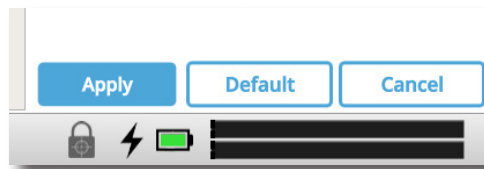
When you make edits to different parameters, you will need to press **Apply** for the changes to be saved. Alternatively, you can **Cancel** to changes or set it back to **Default**.

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

System Settings define parameters that are not specific to a particular remote connection. Examples are how incoming (POTS and IP) calls are handled, global modem settings, and how the contact closures are assigned. Basic options are shown by default. Less used options are hidden until the Advanced option is selected.
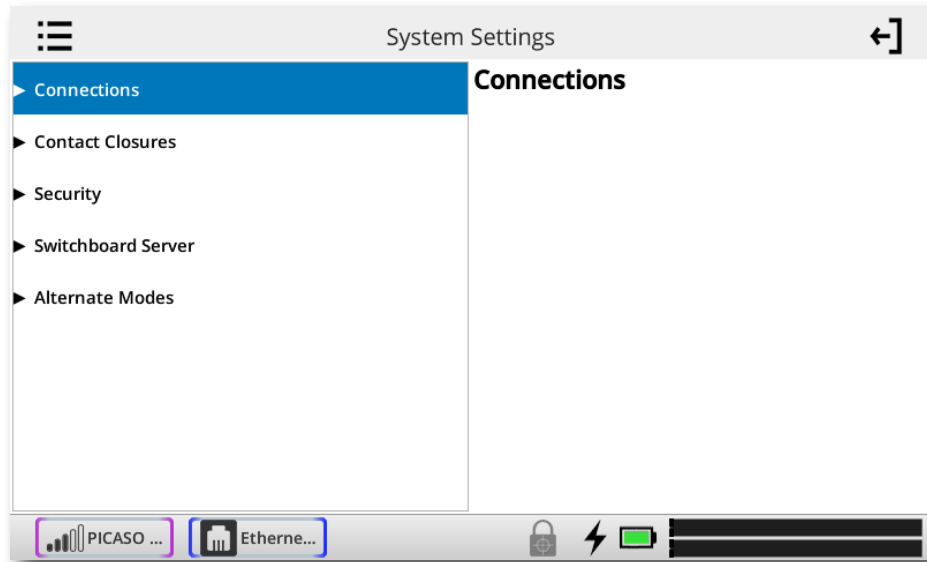
The **System Settings** Menu has the following categories: **Connections, Contact Closures, Security, Switchboard Server** and **Alternate Modes.**
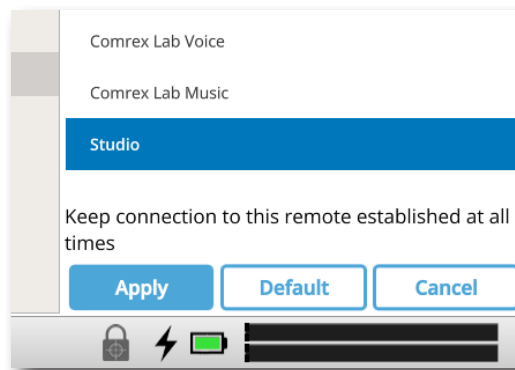
When editing entries on the NX, you have 3 button options: **Apply, Default** and **Cancel**. If you have changed an entry, the **Apply** button will become blue and will start pulsing. You must press this to save your changes. **Default** sets the entry back to default. **Cancel** discards any changes you made.

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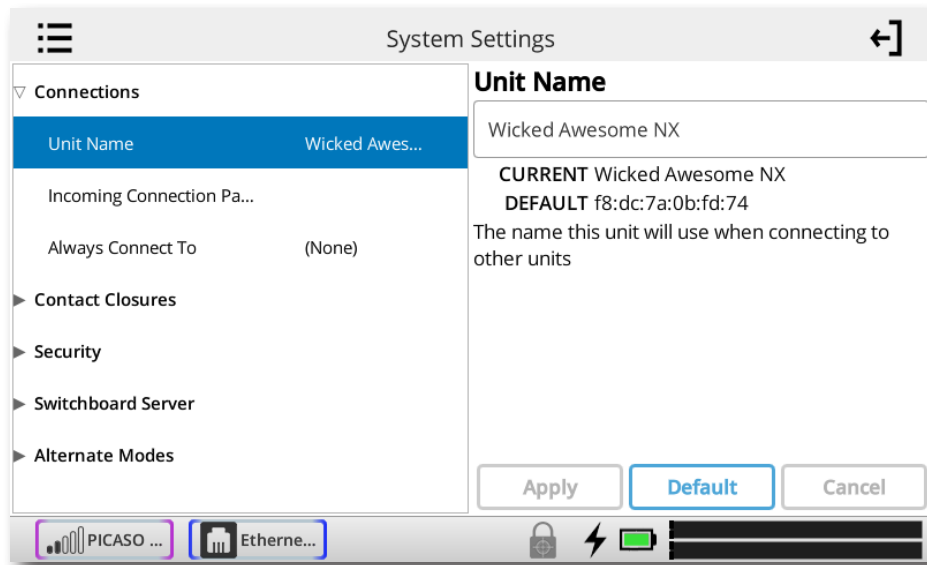
Unit Name - Users are encouraged to name their codecs here. The default name of a codec is the unique MAC address of the Ethernet port. When this is changed to something familiar and unique (such as "Roving reporter", "Weather guy", etc), the new name is reflected in several places:

- In the Web-based Interface
- In Comrex provided utility software such as **Device Manager** and **Codec Commander**
- In Switchboard Contact Lists (See the Switchboard Details section on page 58)
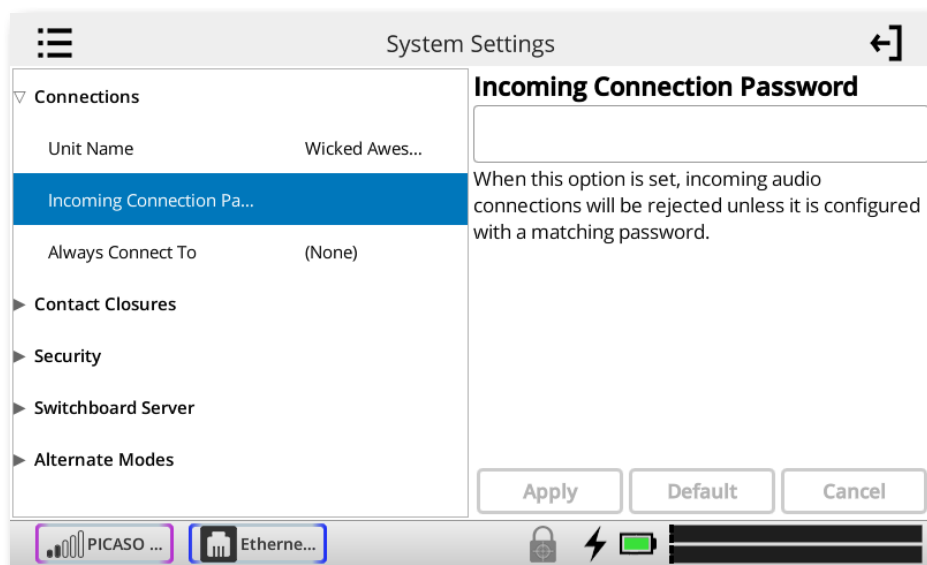
Incoming Connection Password - Allows you to define a password that must be attached to all incoming connections before they are accepted. Units contacting you must know this password and apply it to their outgoing stream, or the connection will not be completed. Leaving the field blank will disable this function.
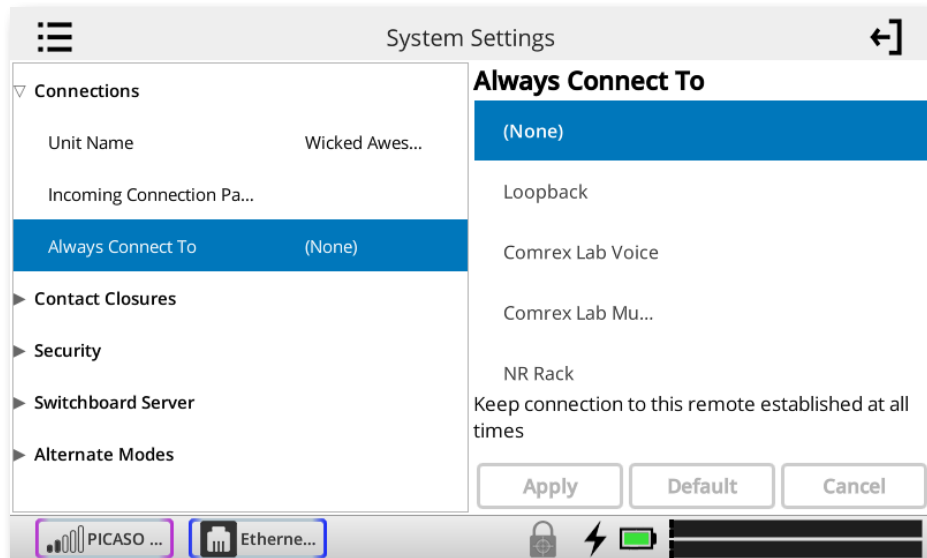
Always Connect To - This setting is available to designate a remote for "always-on" operation. This is useful in environments where a signal is required to be on 24 hours a day. To assign an "always-on" remote, pull down the menu and select which remote to designate as "always-on". A connection will be made and sustained to the chosen remote.

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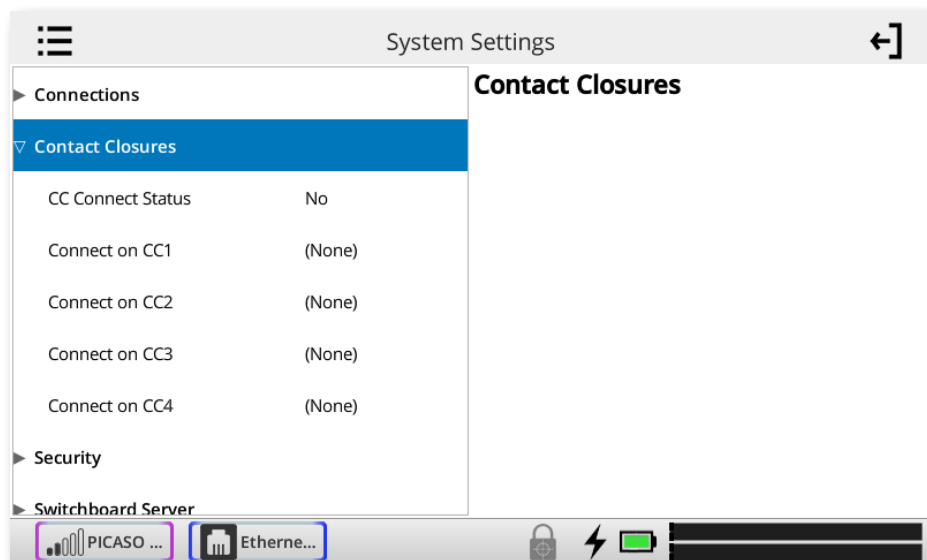
CC Connect Status - Alters the performance of output contact closure #4. Under normal circumstances the contact will close when commanded by the other end of the connection. If this option is enabled, that function is no longer available. This contact will be closed when a valid connection is present,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

Connect on CC (1,2,3,4) - These choices define auto connect rules for remotes to be triggered by the four external input triggers available. **NOTE: These inputs are shared with the end-to-end contact closure signals, so if a remote is designated as auto connect on a closure, that closure signal is not available for use in the direction from this NX.**

To assign a remote connection to a contact closure, pull down the menu box next to the desired closure and select the proper remote. A connection attempt will be made whenever the contact is triggered, and will disconnect whenever the contact is released.

SECURITY SETTINGS
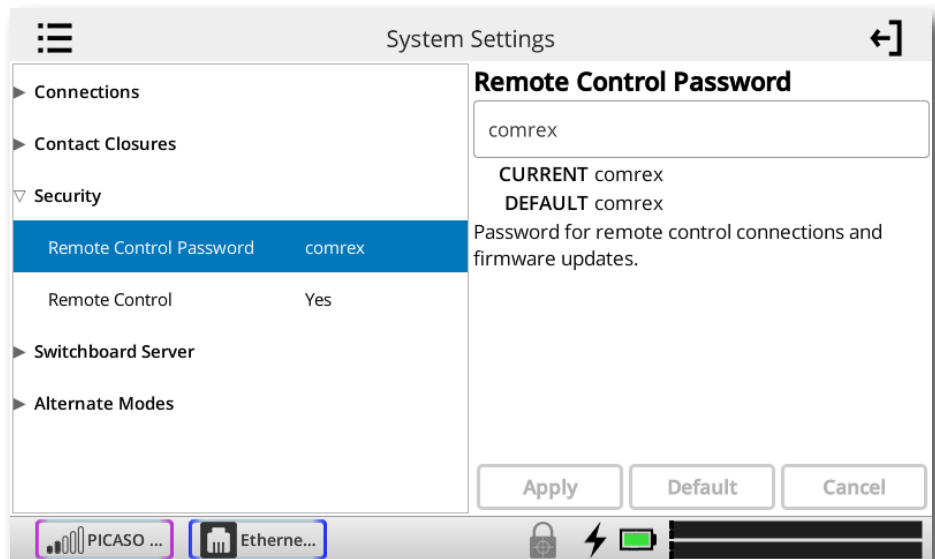
Remote Control Password - Allows you to define a password for the webpage login screen and firmware updater. The default password is **comrex** (lower case). You can disable the remote control and firmware updating functionality completely by disabling the **Remote Control** option.
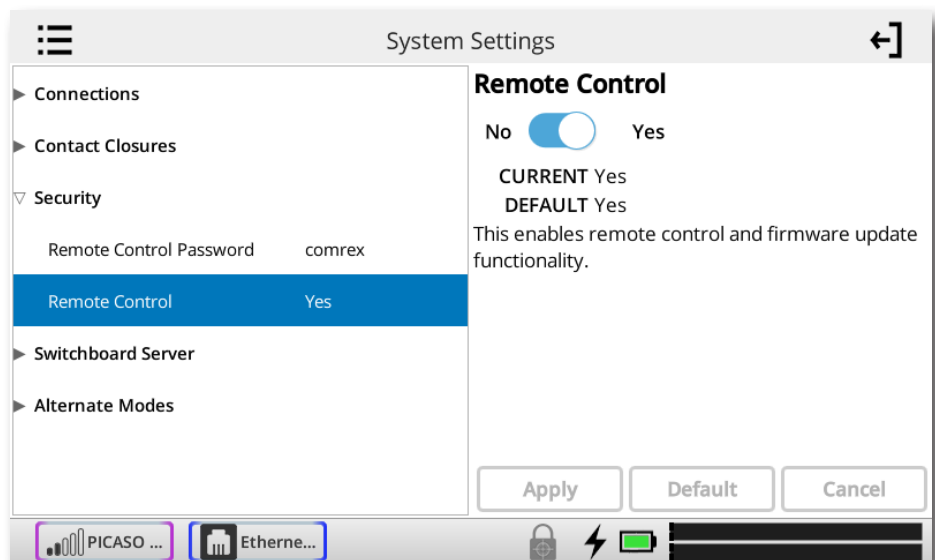
Remote Control - If this function is disabled, the unit will not serve any webpage from its IP address, and the firmware updater will not function. If this option is enabled, you should define a password that will be used to enable both functions.

SWITCHBOARD SETTINGS
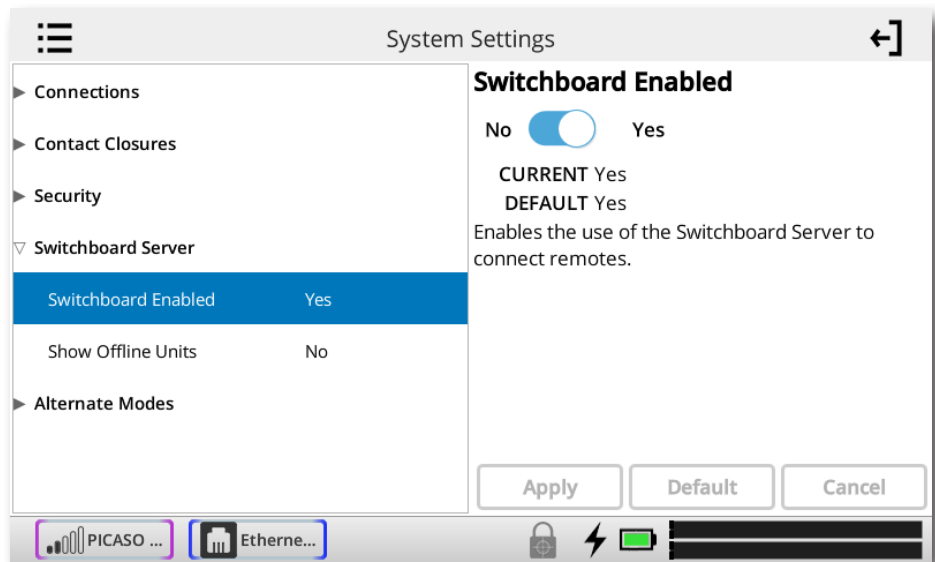
Switchboard Enabled – Allows the use of the Switchboard Server to connect to remotes.
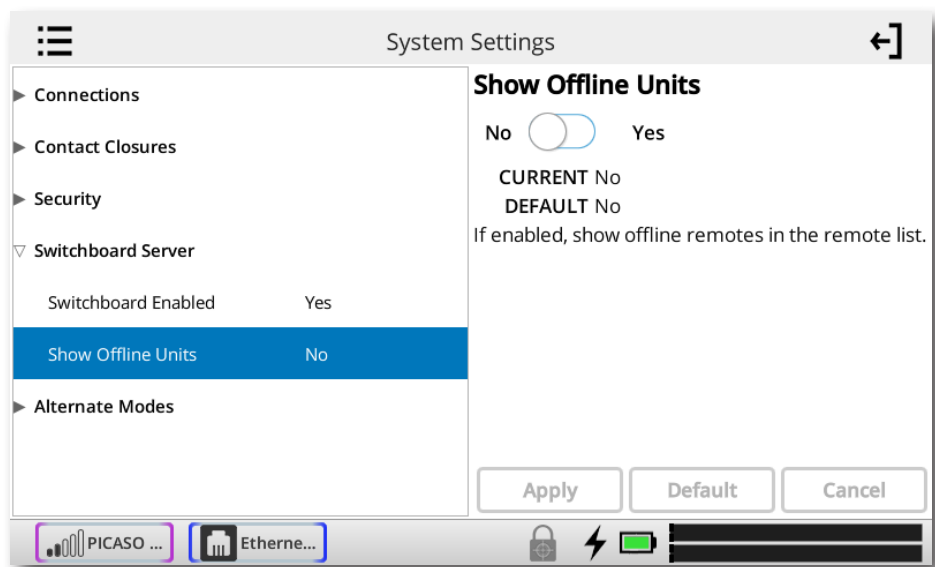
Show Offline Units – When enabled, offline remotes will be shown in the Remotes list.

ALTERNATE MODES
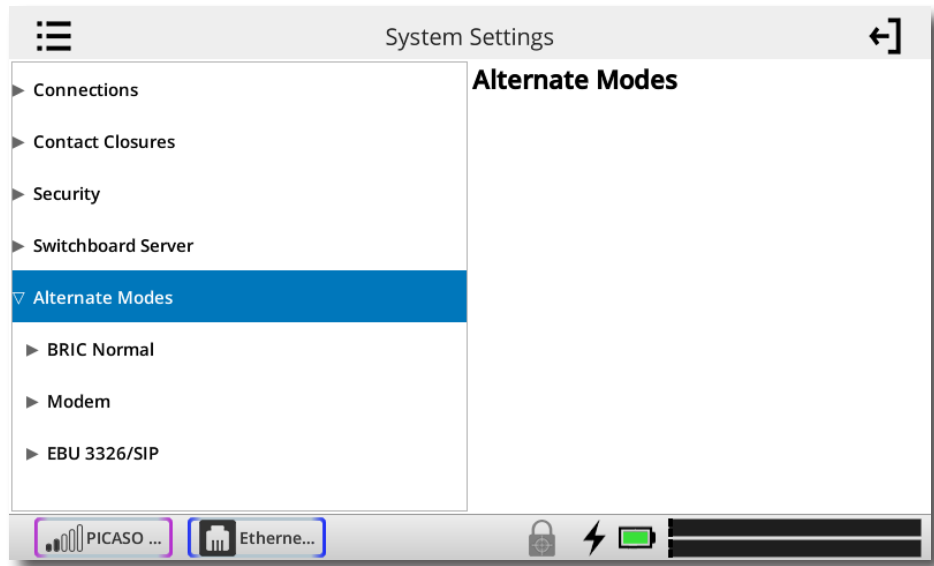
BRIC NORMAL SETTINGS

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

MODEM

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

EBU 3326/SIP

Details for this mode are outlined in the **Making EBU 3326/SIP Connections** section on page 80.
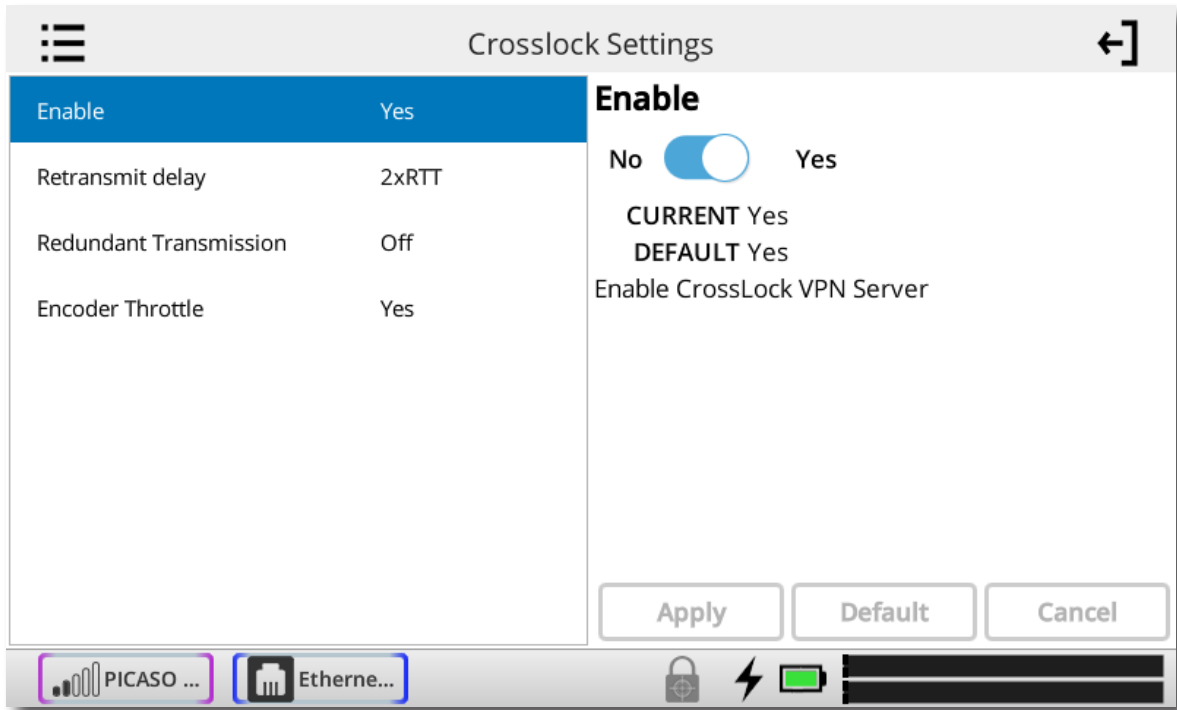
These settings determine how the CrossLock reliability layer behaves. Most users should leave these settings as default

Enable - Allow CrossLock connections in general. Default is yes. Note this does not guarantee connections will be made with CrossLock. Other requirements (CrossLock capable codec on far end, compatible firmware etc) must be met for CrossLock to function.

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

Redundant Transmission - Default is off. Most users of portable codecs will prefer the default "Bonding" mode, which sums the capabilities of networks together. Redundancy disables that feature, and instead puts all network data simultaneously on all available networks. This is the preferred mode if your networks are of known high quality and unmetered. In the case of one network being completely lost, Redundant mode can result in less audio disruption (although in many cases Bonding mode achieves this as well).

Encoder Throttle - Allow CrossLock to signal that the local encoder should reduce data rate. Default is yes.

PINOUTS

PINOUTS - AUDIO

XLR Pinout

Pin 1	Ground
Pin 2	Audio +
Pin 3	Audio –

Line In Pinout

Tip	Left Channel Out
Ring	Right Channel Out
Sleeve	Ground

Line Out Pinout

Tip	Left Channel Out
Ring	Right Channel Out
Sleeve	Ground

PINOUTS - SERIAL PORT

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

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

PINOUTS - CONTACT CLOSURES

Contact closures are available via the 9-pin mini-DIN connector on the top panel of the NX. 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 200mA at a voltage up to 12V. Do not switch AC mains power using these contacts.

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

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

XVIII. ABOUT THE ALGORITHMS

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

1 Do I have lots and lots of bandwidth? If you're running on an entirely unconstrained network like a campus LAN or local Wi-Fi, Mono or Stereo Linear PCM Mode will offer the highest audio quality with lowest delay. If you're hitting the public Internet at any point in the link, however, avoid Linear PCM Mode.

2 Do I require interactivity? If you need to chat back and forth across the link, choose one of our low delay algorithms like AAC-ELD or Opus. The deciding factor between these algorithms is digital bandwidth.

3 Is audio quality the paramount concern? AAC or HE-AAC are the best choices for applications that need excellent audio quality. If delay is also a concern, consider AAC-ELD, which along with Opus, should be the default choices for radio remote broadcasts. If you are running on an unconstrained network, Linear PCM or FLAC would be a good choice.

4 Do I need to deliver two unrelated audio signals to the same location? AAC, HE-AAC and AAC-LD offer Dual Mono options that allow uncorrelated signals (such as dual language broadcasts) to be combined to a single outgoing stream. Note: It isn't possible to send one stream to location A and one to location B. However, it is possible to send the combined stream to locations A and B and have them tap only their respective channels (although this can be a confusing solution subject to operator error).

OPUS

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

LINEAR PCM

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

FLAC

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

G.722

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

AAC

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

HE-AAC

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

HE-AACV2

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

AAC-LD

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

AAC-ELD

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

Algorithm Comparison Chart for ACCESS NX

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**

XIX. SWITCHBOARD TRAVERSAL SERVER (TS)

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

The next section describes how to set up and configure Switchboard. For **Switchboard Theory and Concepts**, go to page 62.

CONFIGURING SWITCHBOARD

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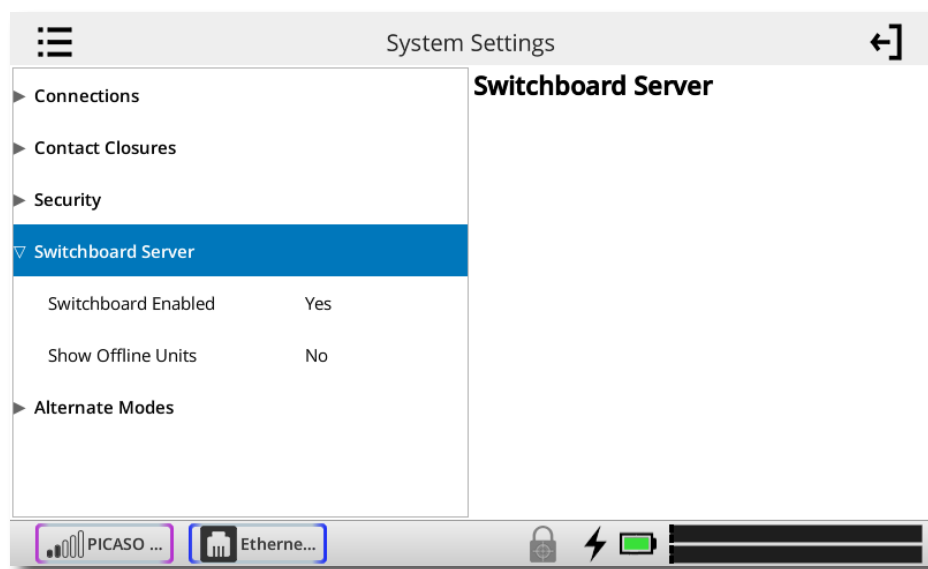
The two choices under the Switchboard Server are **Switchboard Enabled** and **Show Offline Units**. To use Switchboard, the **Switchboard Enabled** must be enabled. Setting the **Show Offline Units** to "enable" will allow you to see the other units on the account, even if they are not currently online.

LOGGING IN AND SETTING UP SWITCHBOARD

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

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

The first time you log in to Switchboard, you will see a notice stating that no units have been added to the account. By clicking on **Add New Unit**, you will be prompted to input the Ethernet MAC address of the NX you wish to add. The MAC

address is available via the touchscreen under **System Settings->Connections->Unit Name**, or you can find it by scanning for the unit via **Device Manager**. The MAC address of the NX must be input in a format with colons between each pair of characters.

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

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

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

CREATING USERS

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

CONTACT LISTS

In some situations, it might not be desirable for every codec in your fleet 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 your codec fleet on your account. You can create multiple Contact Lists that consist of different subsets. With the exception of Shares (discussed next), only units within your Switchboard account may be assigned to Contact Lists.
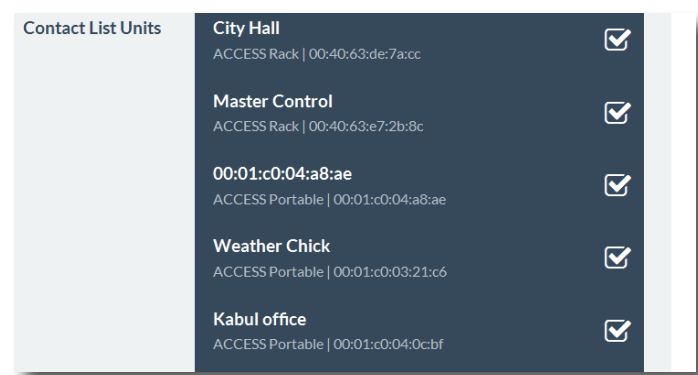
By default, a master Contact List is created that contains all codecs on your account. And by default, every codec in your fleet uses the master list. So if you're not interested in segregating codecs on your account, the default configuration will work fine.
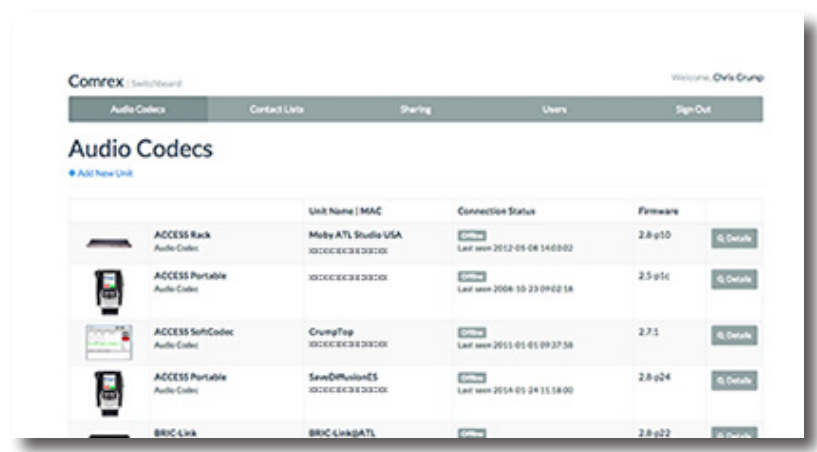
As shown above, you can select one of your individual codecs and change the **Active Contact List**. This will change the list of codecs displayed on that unit.

IMPORTANT: 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.

60

SHARES

If you'd like to allow users outside your account to see the status of some devices in your fleet, Switchboard has implemented **Shares**. Shares are subsets of your codec fleet that you define. Once defined, you can invite other Switchboard accounts to add your Shares, and your codecs become visible to them.

Shares are a one-way transaction. If you invite an external user to share, and he accepts, you don't get any additional status on their codecs. The external user must create a Share and invite you for the Share to be two-way.

Shares are created by clicking the top tab entry labeled **Shares**. A list of your current Shares will appear. You can create a new share by clicking **Add New Share**.

The Share creation screen allows you to choose a subset of your fleet for this Share.

After you make your selection, you'll need to enter either the name of the account you wish to share with, or the email address of the administrator of the account (it must be the one they used to create their Switchboard account). An email will be sent from the server asking the user to confirm your Share(s).

Once the Share(s) is/are confirmed, your shared devices will appear as options in the external user's contact list menu.

IMPORTANT: Shares do nothing until the external user adds them to a contact list. If the user has only a single (default) contact list for his fleet, he must still manually add your codecs to that list in order for them to be visible to his fleet.

Finally, if you want to temporarily deactivate a Share, you can do so by editing the Share entry. A tick-box on the bottom allows activation/deactivation of a share without the need to delete it or re-invite users.

SWITCHBOARD THEORY AND CONCEPTS

Switchboard is useful because it's not always simple to connect two devices over the internet which are essentially "peers". There are two major reasons for this.

First of all, to initiate a stream to a device over the internet requires that you know its IP address. This is the number that gets applied to the destination field of the IP packet, so internet routers can determine how best to send it along its way. Every device that connects directly to the public internet must have one.

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

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

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

We'll cover more about the challenges of connecting codecs behind NAT routers shortly. For now, remember that one of the problems NAT servers add is that the private IP address delivered to the codec (and the only address of which the codec is aware) has no bearing on the public address seen from the internet.

In extreme scenarios, several layers of address locality can be stacked, assuring that the IP address assigned to your device is several degrees removed from the public IP address used for connections. Also, each address in the stack is temporary and able to change at any time.

Internet

The IP address you receive
from the network may be
many layers removed from
the internet IP

Modem
70.22.155.131

Router
192.168.1.1

Router
10.0.0.1

Client Computer
192.168.1.101

ACCESS
10.0.0.49
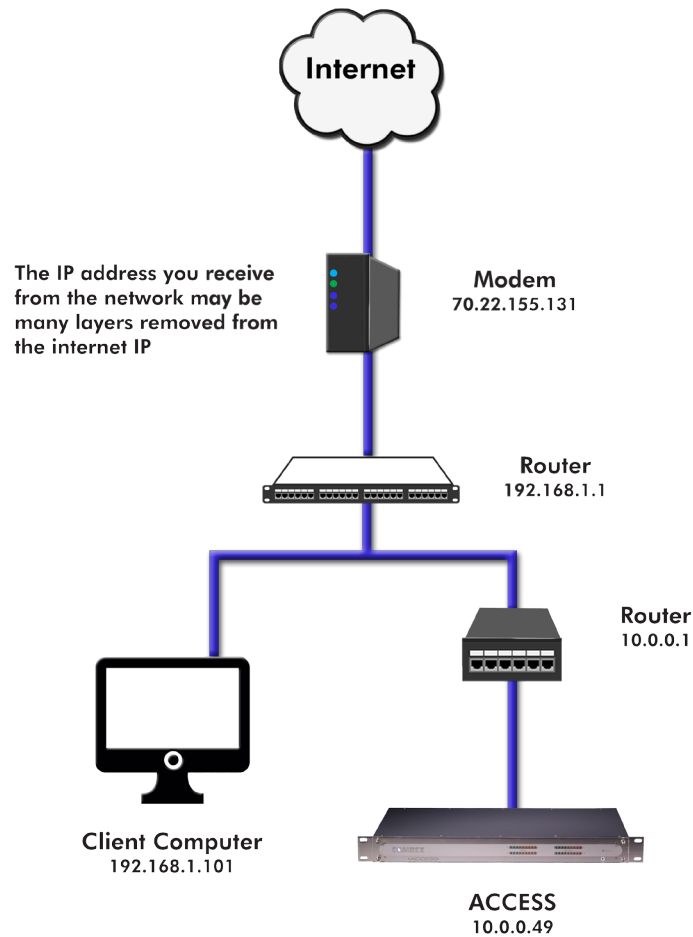
Before deployment of Switchboard, the answer to this dilemma was to assure that the codec located in the studio has a fixed, public IP address. By fixed, we mean that the address is allocated exclusively by the ISP, and that address is entered manually into the configuration of the codec and not subject to change. This scenario works because IP "calls" are usually initiated from the field. As long as the field unit can find the fixed address of the studio unit and send a stream to it, a reverse channel can be created easily and automatically by the studio unit, using the source information contained in the incoming packets. Even in this scenario, the studio IP address must be memorized or input into each codec individually.

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

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

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

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

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

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

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

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

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

NAT routers need directions to correctly forward unsolicited data

Internet

Incoming packet for 70.22.155.130

Where does this go?

Codec A
192.168.1.101

Codec B
192.168.1.102

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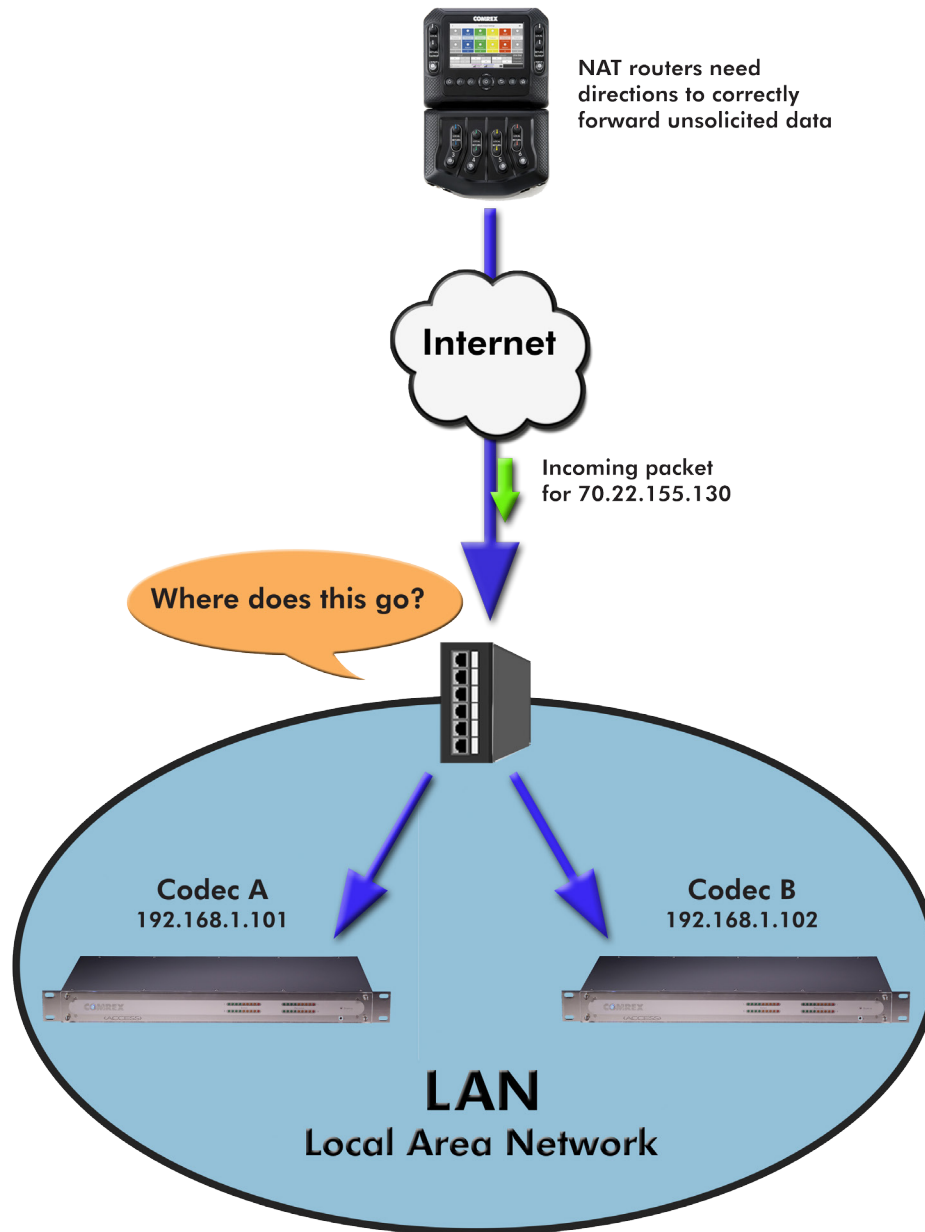
In a typical codec application, Codec X will send a packet from Address A Port B, to Address C Port D on the Destination Codec Y. A codec that has multiple applications running (like streaming audio while simultaneously serving a configuration web page) would deliver these applications from, and to,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

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

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

"Punching a hole"
in a NAT router

1. Codec sends a packet
out through a router

2. Reverse channel stays
open for response packets
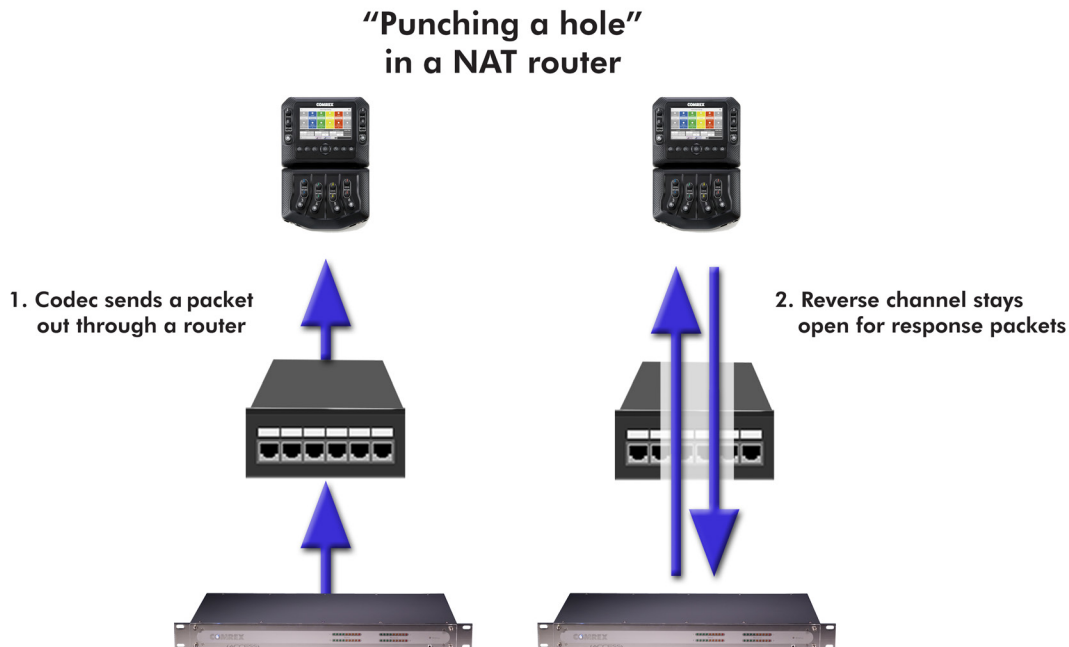
Switchboard aids in breaking through these different types of routers for incoming calls. Because it is in constant contact with all subscribed codecs, it can send and receive test patterns to determine whether one or more NAT routers exist on a link and what type they are. It can then choose a connection 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.

As briefly described in the **Introduction to CrossLock** section**,** CrossLock describes a new reliability layer that gets established between Comrex devices in advance of a connection. This layer takes the form of a Virtual Private network (VPN) between the devices. The ACCESS Media stream is carried within this VPN.
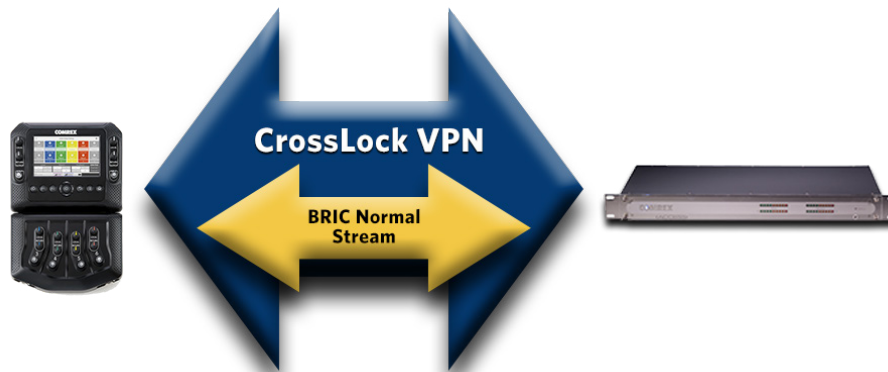
In addition to carrying the audio media, **CrossLock** allows lots of other information to be shared between the endpoint, including information about network quality and far-end delay settings. This provides for much better delay management on both ends of the link.

One or both ends of a **CrossLock** connection can utilize multiple network interfaces. This can take the form of two Ethernet connections, or any mix of wired and wireless networks. A common usage scenario would be attaching two 3G/4G modems to NX. In the case of one network underperforming, the majority (or all) of the data will be sent on the good network.
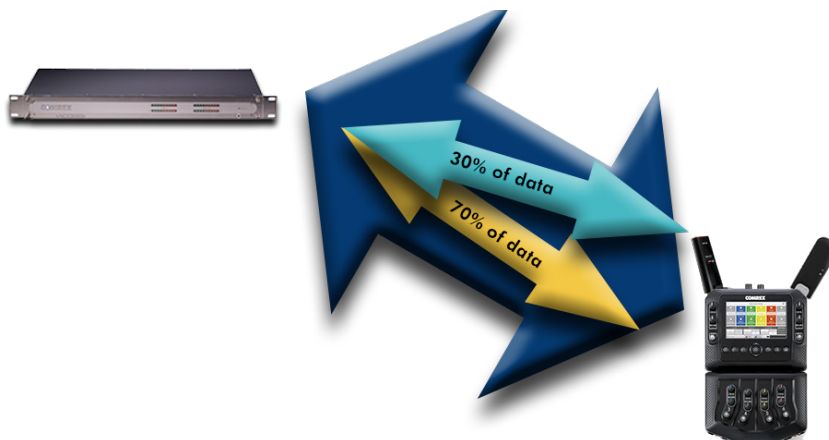
By default, **CrossLock** will utilize any network ACCESS senses as capable of carrying reasonable data. If a network increases in delay and packet loss, ACCESS may decide to remove media data from that network entirely. ACCESS may still use the network for background communications and error correction.

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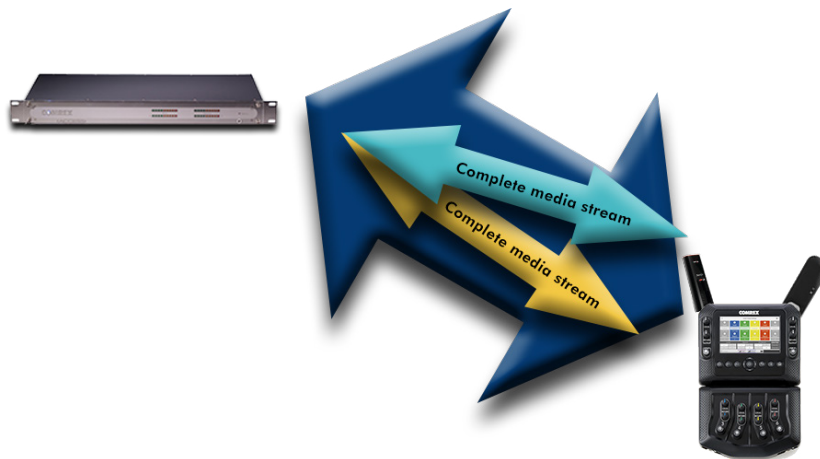
CROSSLOCK AND SWITCHBOARD

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

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

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

Switchboard delivers a "buddy list" to each ACCESS in the fleet. This list appears on the **Remote Connections** menu of the NX.

The connections have a color codec "gear" icon to indicate the status of each other ACCESS or BRIC-Link in the fleet. Items with a green gear are ready for connection. Yellow means busy and red means off-line.
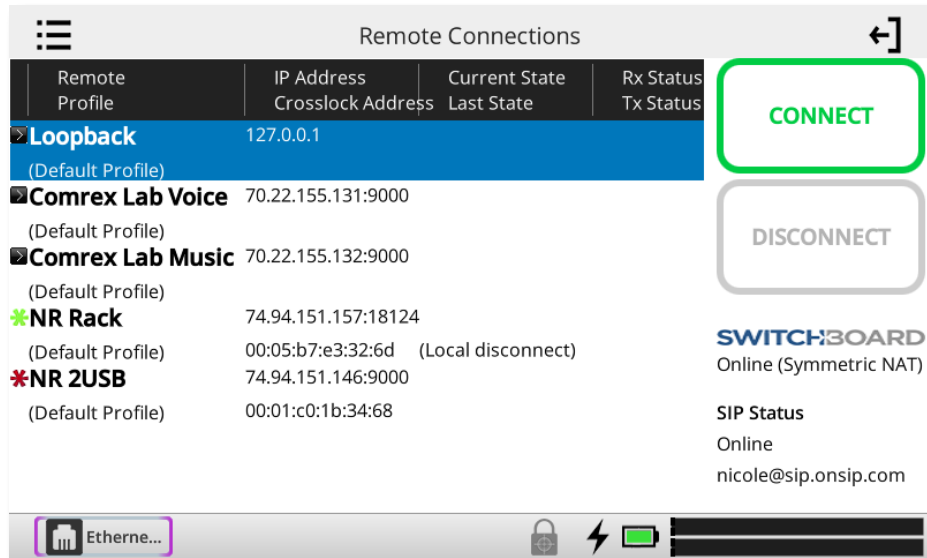
MAKING CROSSLOCK CONNECTIONS VIA SWITCHBOARD

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

1. The ACCESS on the far end is running firmware 4.0 or higher

2. The **CrossLock** port is (UDP **9001**) open to the far end

3. Each ACCESS is aware of the other's Unit ID (Mac address). This is handled behind the scenes in Switchboard.

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

A successful **CrossLock** connection is indicated by a green "Lock" icon in the lower banner. Because **CrossLock** is established before an audio stream, and lingers for some time after, this may stay green even when an audio stream is not active.
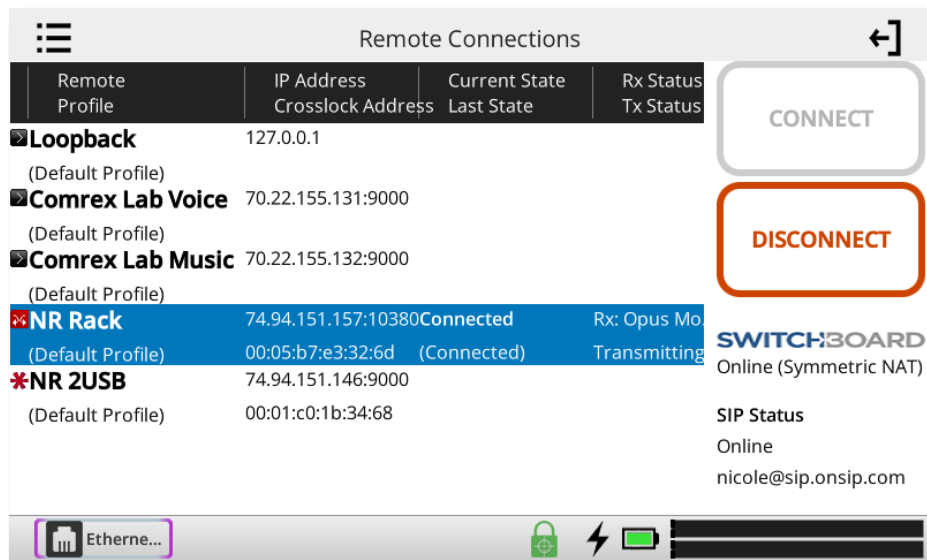
MAKING CROSSLOCK CONNECTIONS WITHOUT SWITCHBOARD

In the case of non-Switchboard based connections (e.g. closed networks or STLs), you will need to know the unit ID (Primary Ethernet MAC address) of the unit to which you wish to connect. This is input to the "**Create New Remote**" pop-up in the "**MAC Address**" field.
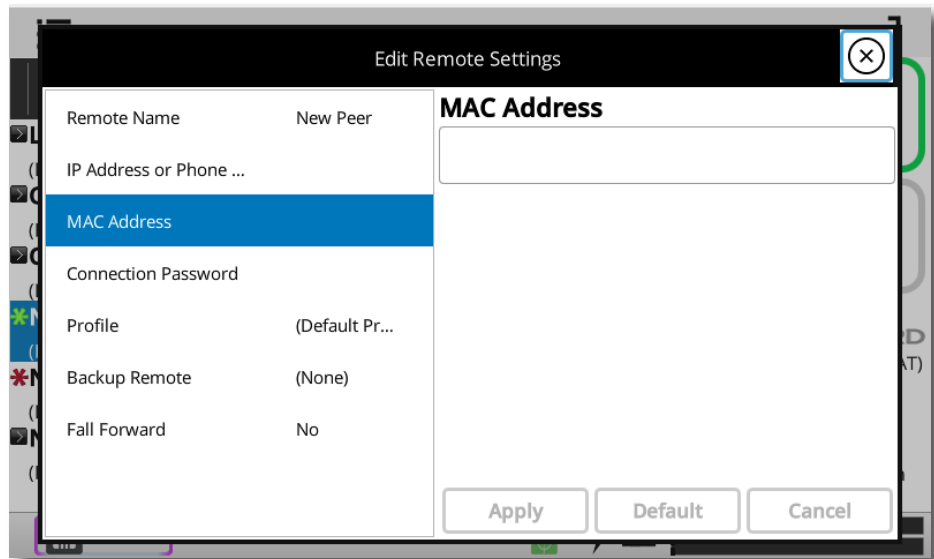
In addition, the codec receiving the connection must have a similar entry made, with the MAC Address of the calling unit populated.

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

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

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

USING DEVICE MANAGER

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

Once a unit is selected, five tabs appear on the right-hand pane.
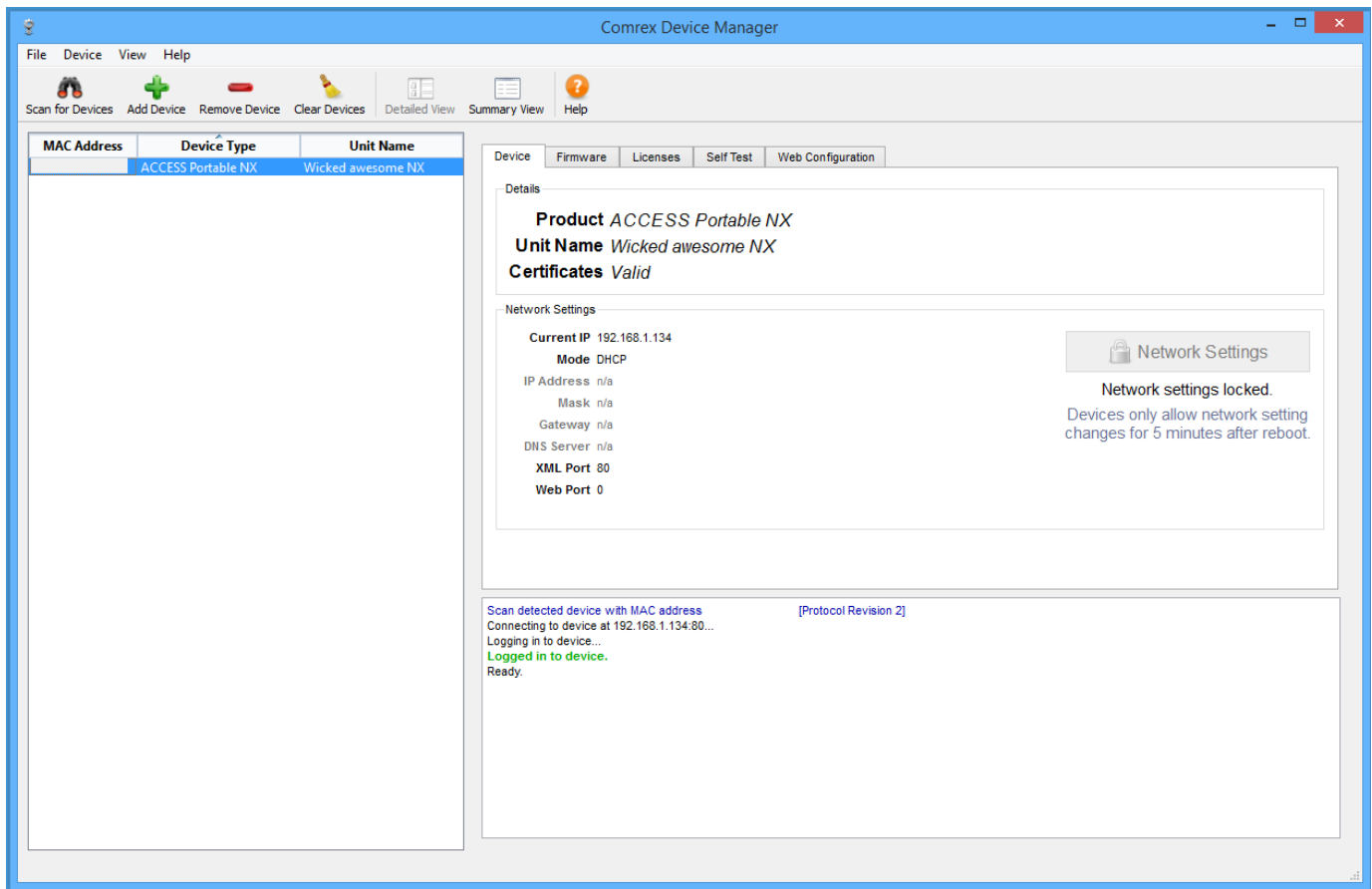
The first tab is the **Device** tab. This tab will give you the current IP address and network settings. As a security measure, network settings may only be changed during the first 5 minutes of your Comrex product operation. If you wish to change your network settings, you will have to reboot your unit and make the changes right away.
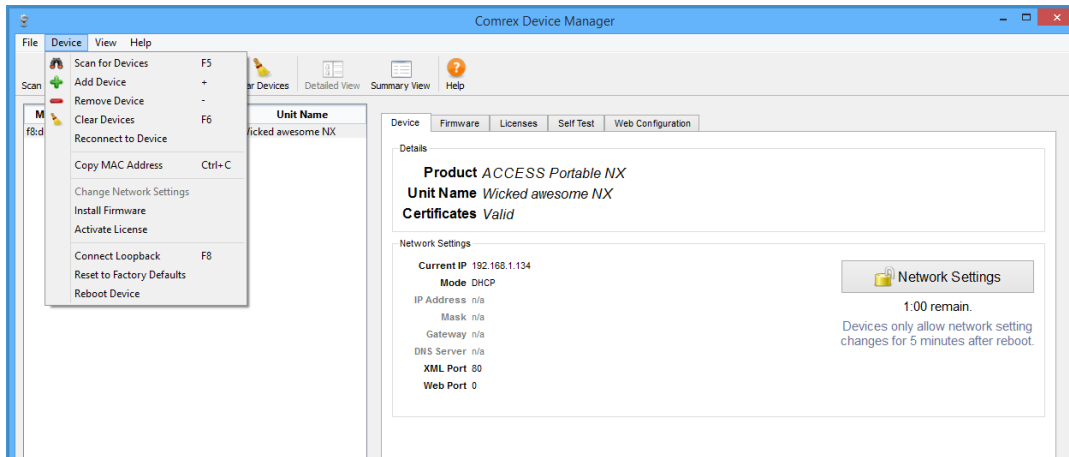
TIP: To reboot your unit, go to the Device menu located at the top left of the window and select Reboot device.
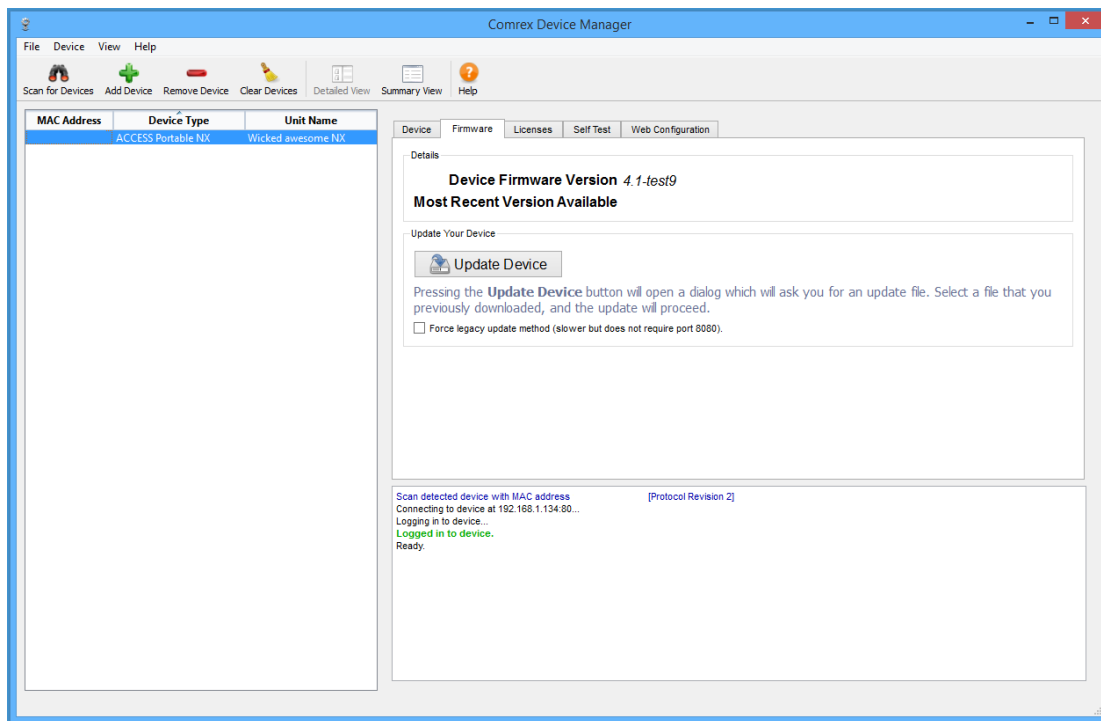
The **Firmware** tab shows you the device firmware version you currently have as well as the most recent version available. If there is a more recent version, it will appear in blue.

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

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

The **License** tab shows you which licenses are currently active to your unit. This is also where you can add and/or remove licenses.
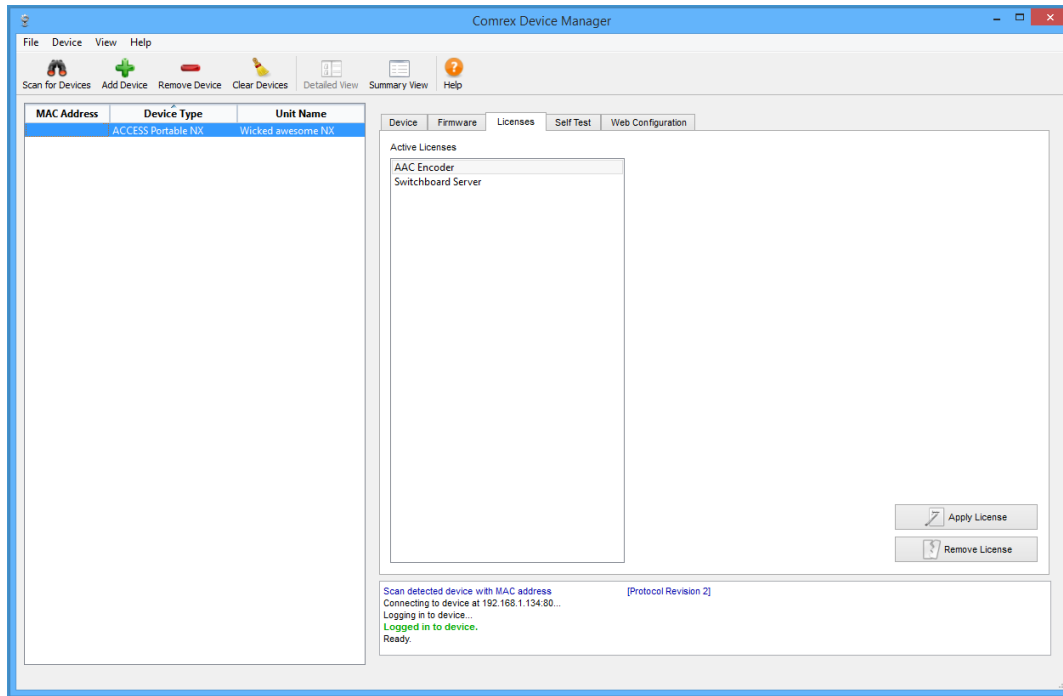
The fifth tab is labeled **Web Configuration**. This will open a simplified setup interface on NX called **Toolbox.** The **Toolbox** interface allows you to configure several options including the Ethernet port. You will need to log in to **Toolbox** separately with a user name (any) and password (default = **comrex**) to enter the **Toolbox**. To learn more about Toolbox, go to the **NX Toolbox** section on page 74.
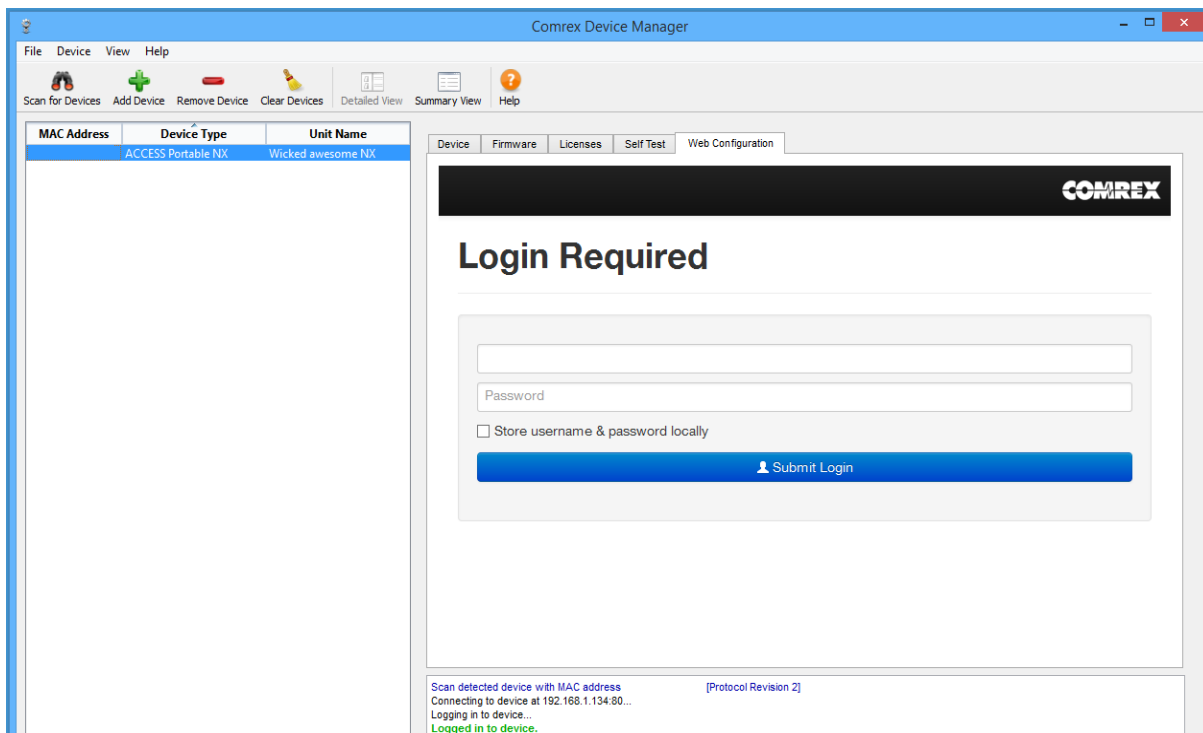
Toolbox is a network manager that allows for easy network configuration. Typically you will be using your NX touchscreen to perform these operations as described in the section **Network Manager** on page 30, but in some cases, it can be much easier to use **Toolbox**.

You can log into Toolbox either via **Device Manager** or through the IP address of the unit with a **/cfg** appended to it (e.g. **192.168.0.34/cfg**).
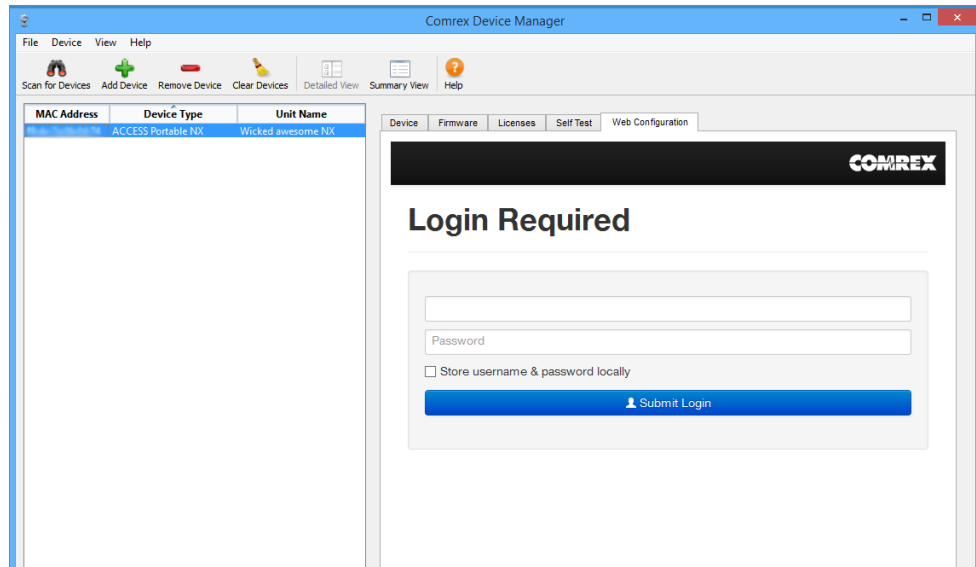
Once logged into **Toolbox**, choose the **Network/Admin/CrossLock** option and then choose **Set up Ethernet and Wireless**.
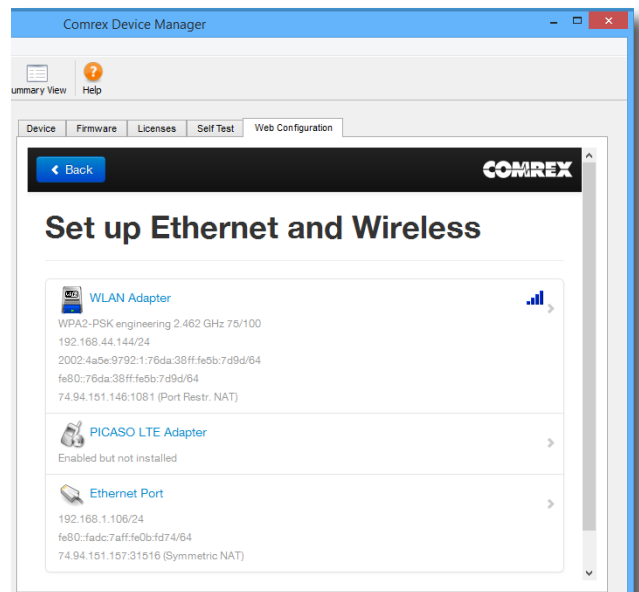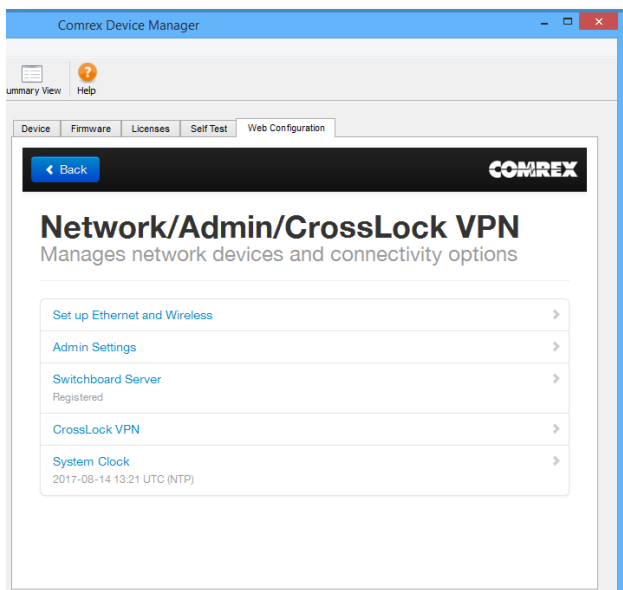
From here, you can select the device you would like to configure and then adjust the parameters for that device. You can edit the **Name**, if it is enabled or not, and the **Active Network Location**.
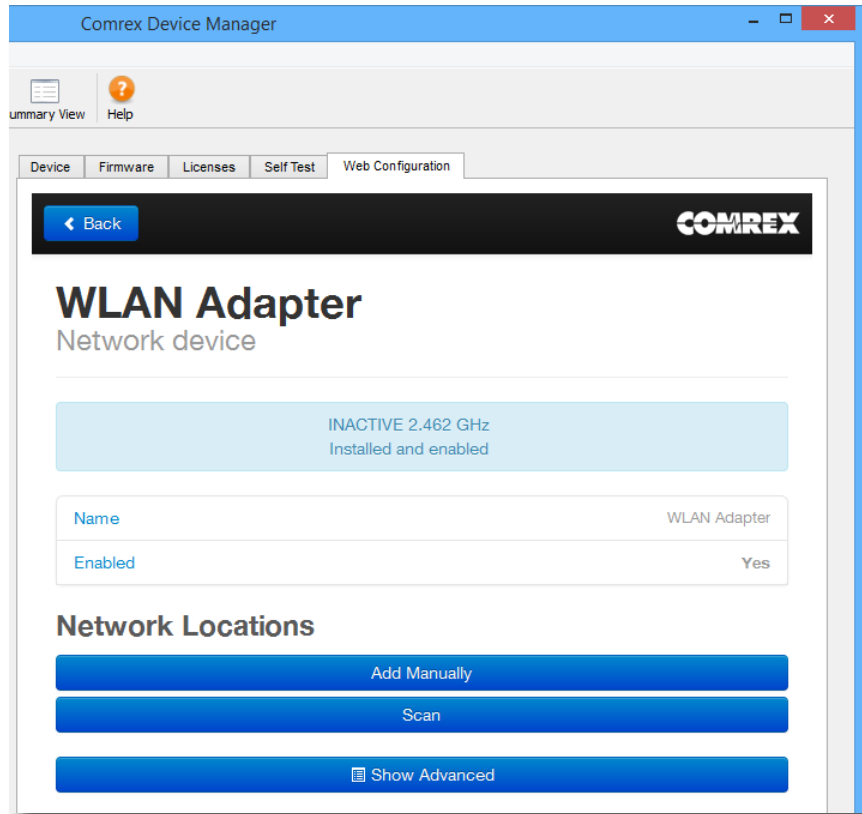
LOCATIONS

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

CONFIGURING WI-FI

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

Once selected, you can enter in the details for that network, including the network key, if needed.
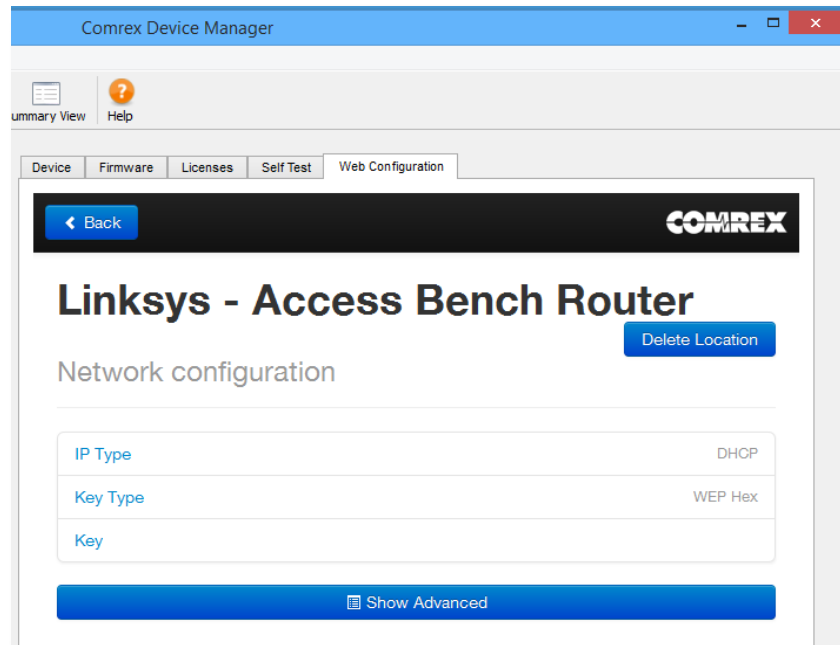
Once created, you can assign that network to the adapter by selecting **Active Network Location** and selecting the network from the drop-down list.
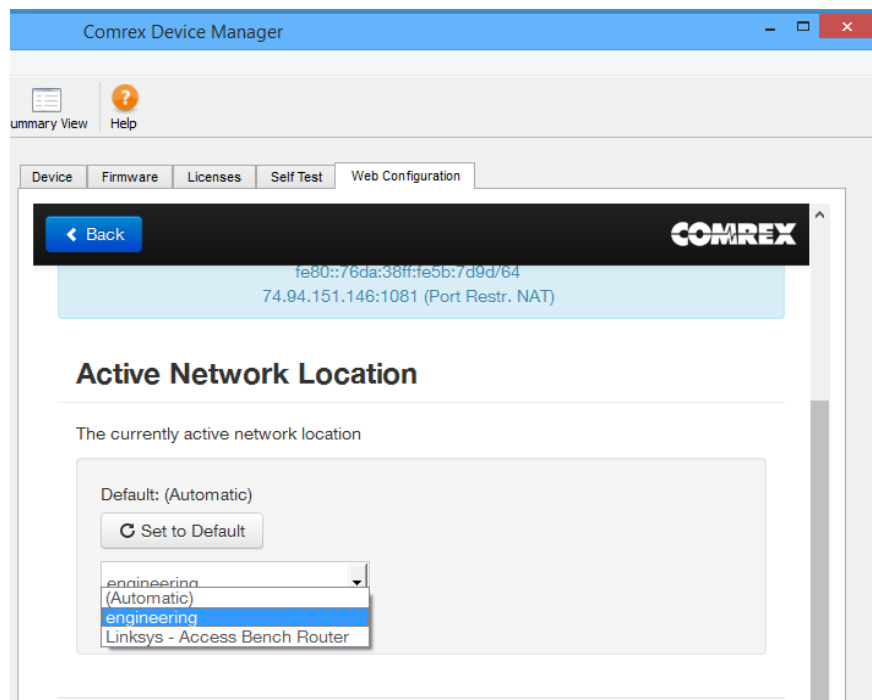
If the Wi-Fi adapter's location is set to **Automatic**, it will check all location settings when the Wi-Fi adapter is installed and enabled, and choose the first location "match" it finds.

ADVANCED NETWORK SETTINGS IN TOOLBOX

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

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

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

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

XXIII. OPERATING NX IN A 24/7 ENVIRONMENT

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

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

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

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

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

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

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

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

1. The timeout value is set to infinity - the connection will never be torn down regardless of data.

2. NX is configured to re-establish the connection in the event of a power re-cycling.

3. The local **Disconnect** control is disabled. The **Disconnect** function on the receiving side is still enabled, but will result in an immediate reconnection by the initiating side.

SETTING NX FOR 24/7 OPERATION

On the NX, go to Connections under the **System Settings** menu.

Select the **Always Connect To Remote** entry and all available connections will appear on the right. Setting this value to one of your pre-defined connections results in configuring the unit for 24/7 operation to that remote. No configuration is necessary on the remote side.
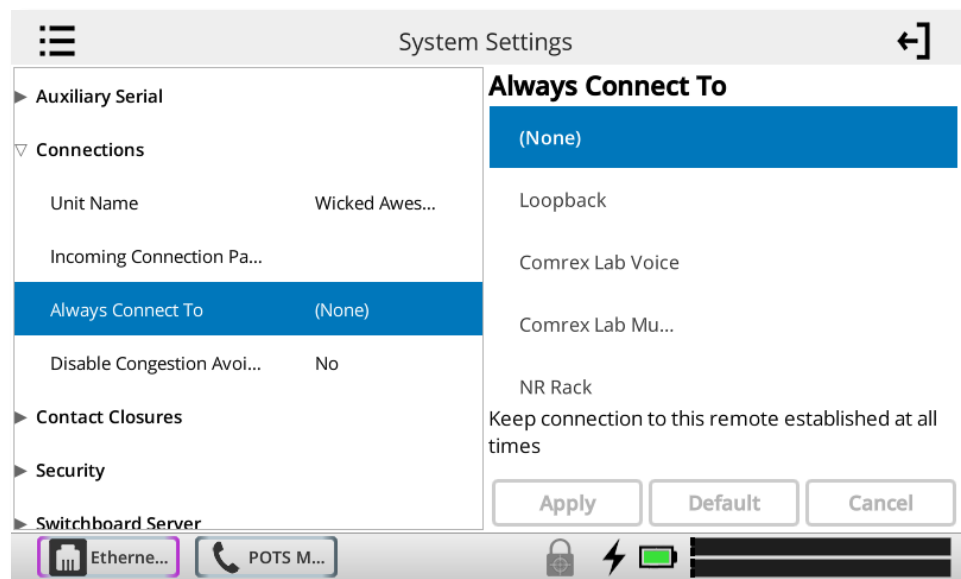
NX has another option for continuous connections. When building a new remote on the Remote Connections menu, there is a field for backup options. One of those options is called "**Keep Retrying This Remote**".
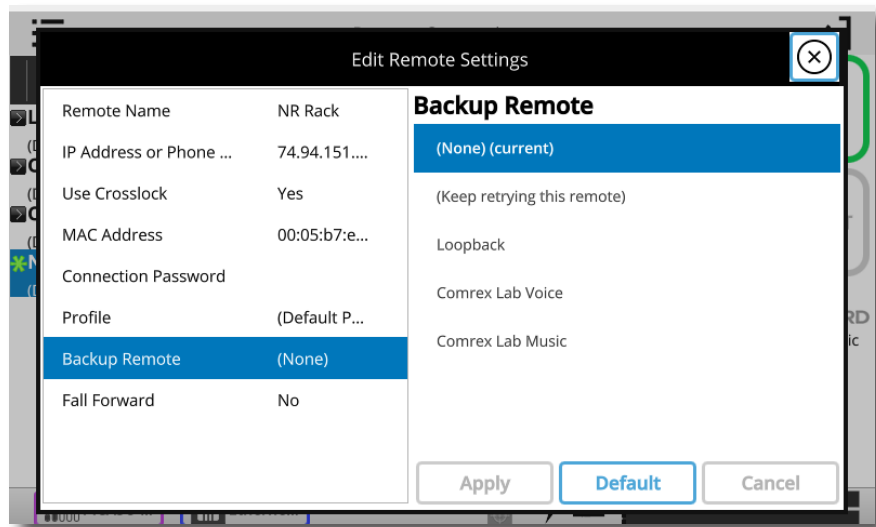
Using this mode will allow the unit to disregard the timeout value and keep a persistent connection. The difference is that the **Disconnect** function still works and the connection will not be reinitiated on a power re-cycle. This mode is meant for users who are making temporary connections, but do not want the system to time out and disconnect in the event of network failure.

XXIV. MAKING EBU 3326/SIP COMPATIBLE CONNECTIONS

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

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

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

MORE ABOUT EBU 3326

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

EBU 3326 IN NX

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

EBU 3326/SIP MODES

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

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

UNREGISTERED MODE

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

REGISTERED MODE

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

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

SIP SERVERS

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

SIP URIS

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

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

REGISTERING WITH A SERVER

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

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

Below shows where this information can be applied in the **System Settings** section. You will also need to enable the **Use SIP Proxy** option in that menu.
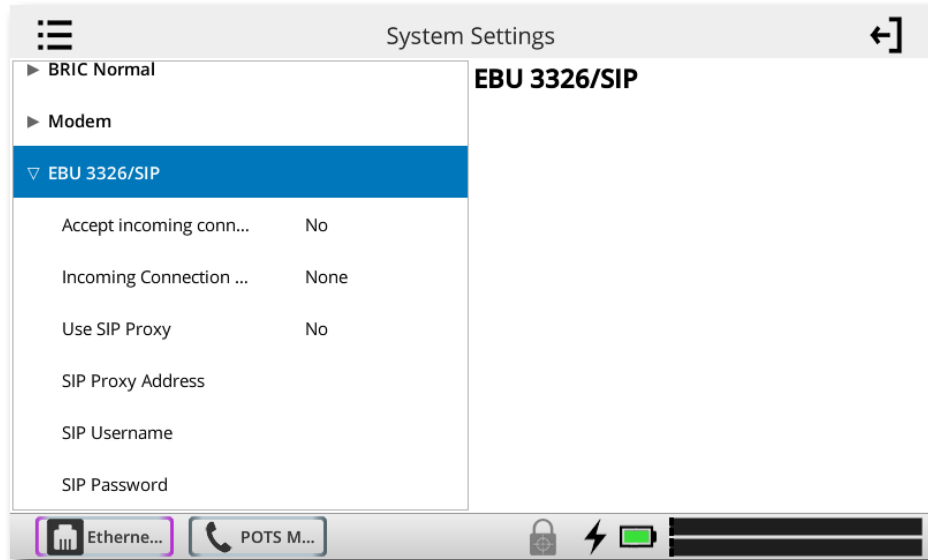
Once this information is correctly entered, a new status line appears on the NX Remote Connections menu.
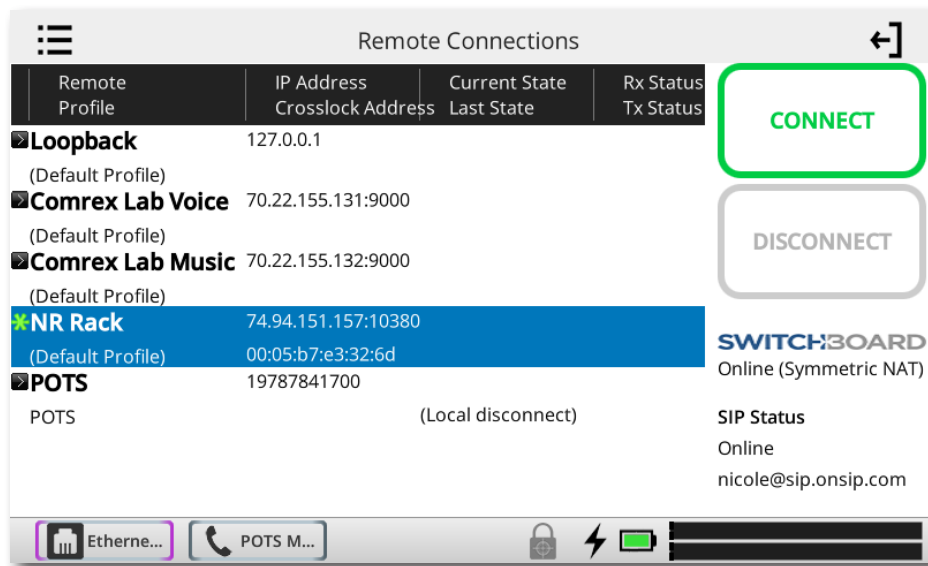
The status will reflect the progress of the registration process. When complete, this will display **Online**. If the box does not display Online after a short time, it usually means that registration attempt failed. It's best to go back and carefully check the registration info. It might also be useful to check that your registration information is valid by using it to configure a VoIP phone or softphone.

SIP registration can be very simple with some servers, and others can require more advanced settings.

MAKING SIP REGISTERED CALLS

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

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

1   The server does not support direct connection to IP addresses (if the address is in this format)

2   The server does not recognize the address

3   The server does not forward calls beyond it's own domain

4   The server does not support the chosen codec

5   The called device does not support the chosen codec

6   The address is a POTS telephone number, and POTS interworking is not supported

7   The address is a POTS telephone number, and no credit is available (most services charge for this)

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

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

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

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

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

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

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

SIP TROUBLESHOOTING

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

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

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

OUTGOING CALL ISSUES

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

INCOMING CALL ISSUES

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

SOLUTIONS

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

In point-to-point connections, this isn't possible. All is not lost here, since we can find some hacks to make this work. The first place to look is your router, since many modern routers are aware of this issue and have taken steps to relieve the pain. If your router supports a SIP Application Layer Gateway (ALG), then enabling this option can fix the issue.

Essentially, the router will get smart enough to read your SIP handshake, find the outgoing address field, and replace it with your public IP. This is a pretty slick solution, but there may be environments when you are not aware whether this option is supported on your router, or have the ability to enable it. So on to solution two:

STUNNING SUCCESS

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

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

FIX OF LAST RESORT

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

xxv.   MULTI-STREAMING

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

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

Multi-streaming should not be confused with IP Multicast, which is described in the IP Multicast section on page 88.

Note: Multi-streaming is unsupported with CrossLock connections.

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

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

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

86
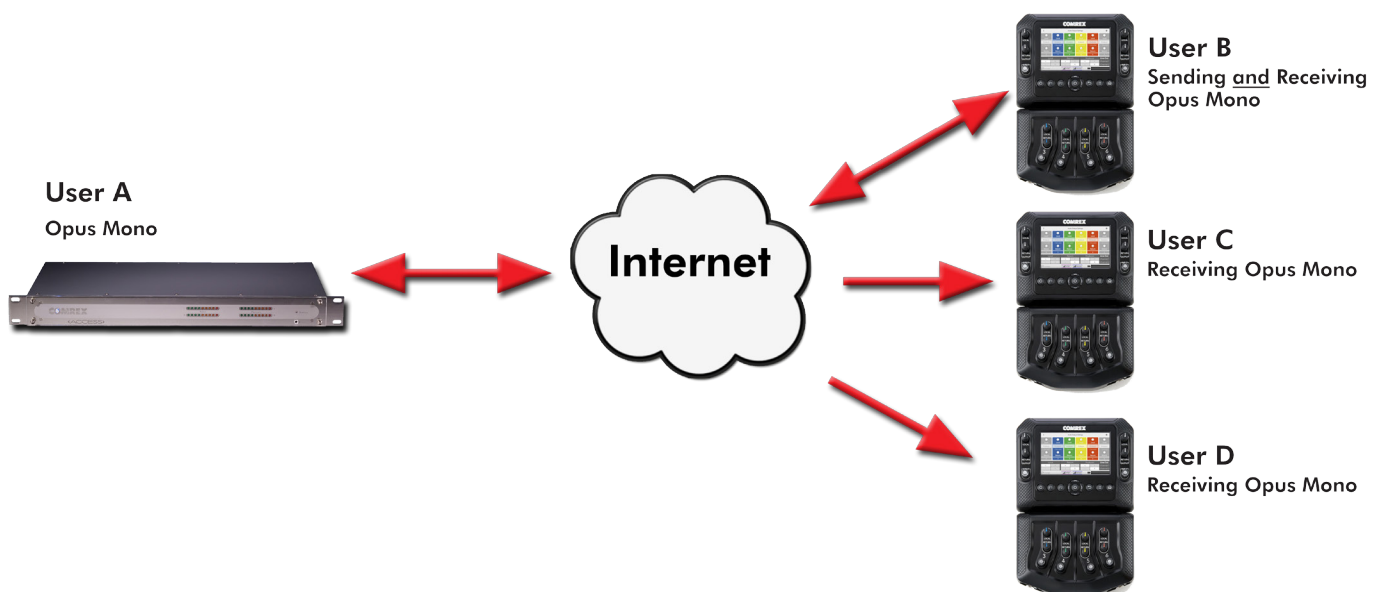
To turn the encoder off, expand the profile you will be using in the **Profile Manager** menu. Under each folder, both **Local** and **Remote**, there is a **Transmit On/Off** option. By selecting this, you can then turn the transmit to Off.
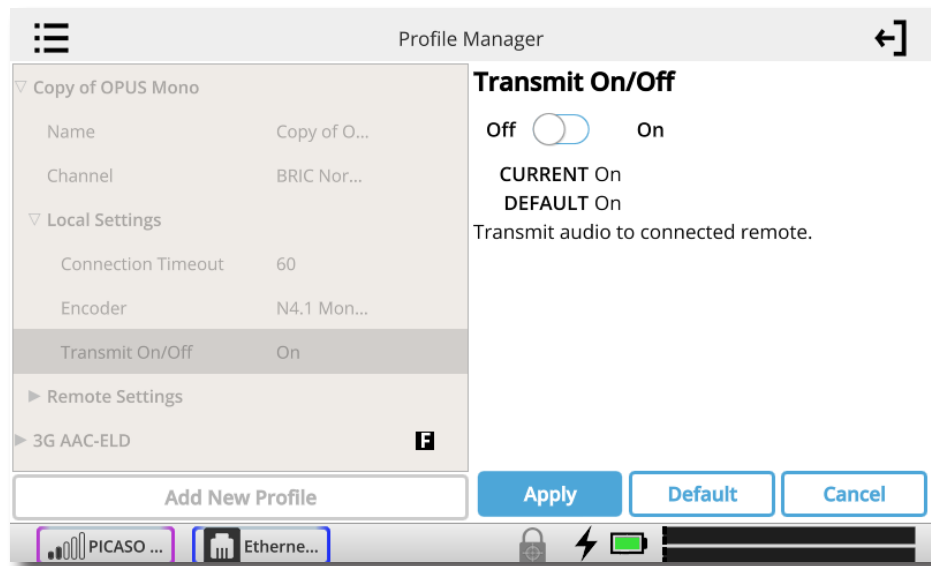
We'll give two examples of multi-streaming scenarios. The first is an environment where the user that is serving the multi-stream initiates the calls, and in the second the serving user accepts all its incoming connections.

In the "multi-streamer as caller" model, two different profiles will be built on User A. The first profile, labeled "Multi-Duplex," will be defined as a normal, full-duplex 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 Transmitte**r is turned **Off**. Most other selections in this profile are irrelevant.

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

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

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

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

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

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

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

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

MULTICAST PROFILES

To set any remotes to Multicast, you must first create a profile for either a Multicast Sender or a Multicast Receiver on the **Profile Manager** menu.
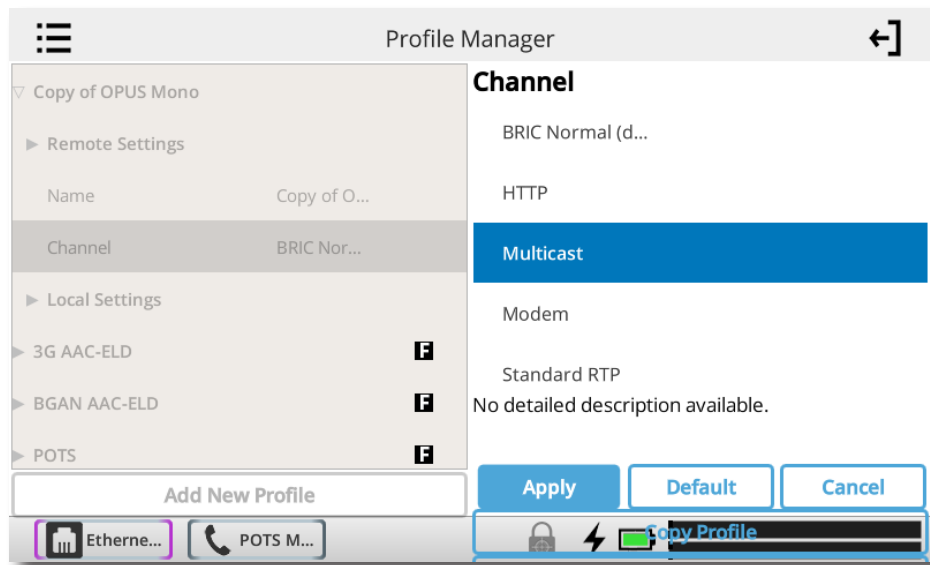
When you define a new profile, you have the option to choose **Multicast** as the profile type. Multicast profiles have fewer options than other profile types, and some of the available options will have no effect.

The important settings for Multicast are:

- **Sender/Receiver** – Determines whether this particular ACCESS is designed to generate the IP Multicast stream (send) or decode one (receive).

- **Encoder Type** – Determines the type of stream to be used by the Multicast Encoder (not relevant for decoders).

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

SETTING UP A MULTICAST REMOTE

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

TIME-TO-LIVE

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

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

CHANGING PORT NUMBERS FOR MULTICAST

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

224.0.2.4:443/100

XXVII. STREAMING SERVER FUNCTION

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

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

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

Keep in mind 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 AN HTTP STREAM

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

http://192.168.0.75:8000
(insert the real IP address, but always use port **8000**)

In Windows media, input the address like this:

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

SIMULTANEOUSLY CONNECTING NX AND STREAMING

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

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

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

POTS CODEC SET-UP FOR NX COMPATIBILITY

The legacy codecs (Matrix, Vector or BlueBox) must be configured for operation in **Music Mode**, which will allow full-fidelity (up to 15 KHz) connections. Voice Mode is not supported by NX. All 4 Contact closures and ancillary data supported by legacy codecs are not supported by NX.

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

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

USING NX WITH POTS

To use NX on POTS, insert the Zoom USB POTS modem into one of the USB ports. Connect the phone cord to a normal, analog telephone jack.

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

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

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

RATE VS. RETRAIN

When incoming or outgoing POTS calls are active, the **Remote Connections** menu changes slightly. You will see two additional buttons appear; **POTS Retrain** and **POTS Rate Drop**. These are special functions applicable only to POTS calls, so they are not visible during IP connections.
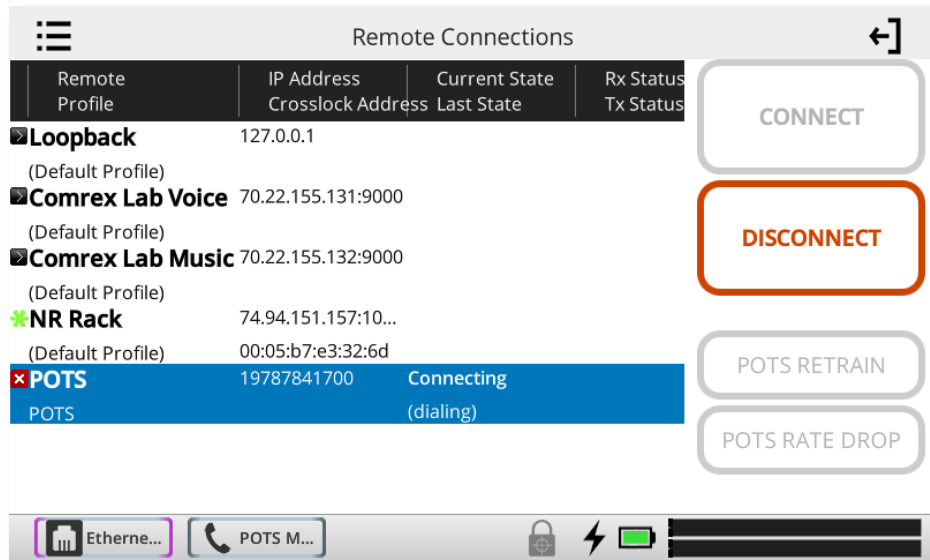
These controls are similar in function to those provided on POTS codecs. NX will initially connect at the best data rate supported by the telephone line, and will display that connect rate on the **Remote Connections** menu**.** This value may be viewed by pressing the + next to the active connection. You can force the system to drop to the next lowest connect rate by clicking the **Rate Drop** button at any time. Audio transfer will be interrupted momentarily while the units negotiate the new connect rate. Alternately, you can force the system to initiate the entire training sequence again (the "chat" sounds heard at the beginning of a call) by clicking the **POTS Retrain** button. You will lose audio for a longer time (approx. 7 seconds) but the modems will completely re-equalize the connection and audio will begin again once the retraining is finished.

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

TROUBLESHOOTING POTS CONNECTION

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

1. Use the POTS codec on a direct telephone company line and avoid in-house phone systems. A line used by a fax machine usually provides this direct access. (Be sure to disconnect the fax machine before connecting the codec!)

2. Check to see that there are no extensions or modems on the line you are using — or at least arrange that no one uses these during your broadcast.

3. If there is call-waiting on your line, disable it by entering "*70" in front of the number you are dialing.

4. If possible, try the POTS codec out at the remote site before your actual broadcast at about the same time of day that you plan to use it. This will give you a good idea of expected connect rates and possible line problems.

5. At minimum, connect a few minutes before airtime to assess the connection quality. Setting a MaxRate on the POTS codec, based on your findings, is highly recommended. MaxRate usually should be set at a level or two below the maximum unrestricted rate. This will provide a "guard band" of sorts against noise and corruption which may cause errors on the line.

6. If operation starts to degrade after a long period of connection, it may be that the phone line parameters have changed. These parameters are affected by factors such as time of day, weather and geographic location. The modems should be given the opportunity to renegotiate for these new parameters.

7. If you experience low connection rates or errors, try redialing. If that does not help, dial from the other end. If the call is long distance, try forcing the call to another carrier. If a good connection is found, keep that line up.

XXIX. GATEWAY OPERATION

ABOUT GATEWAY OPERATION

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

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

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

CONNECTING AS A GATEWAY

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

As shown below, NX is using a 4G adapter to connect to the internet and using its Ethernet port to share 4G data with a laptop computer via a crossover cable.

ACCESS NX Connection
to the Internet via 4G

Connection from Computer to ACCESS NX
Ethernet Jack using an Ethernet Crossover Cable
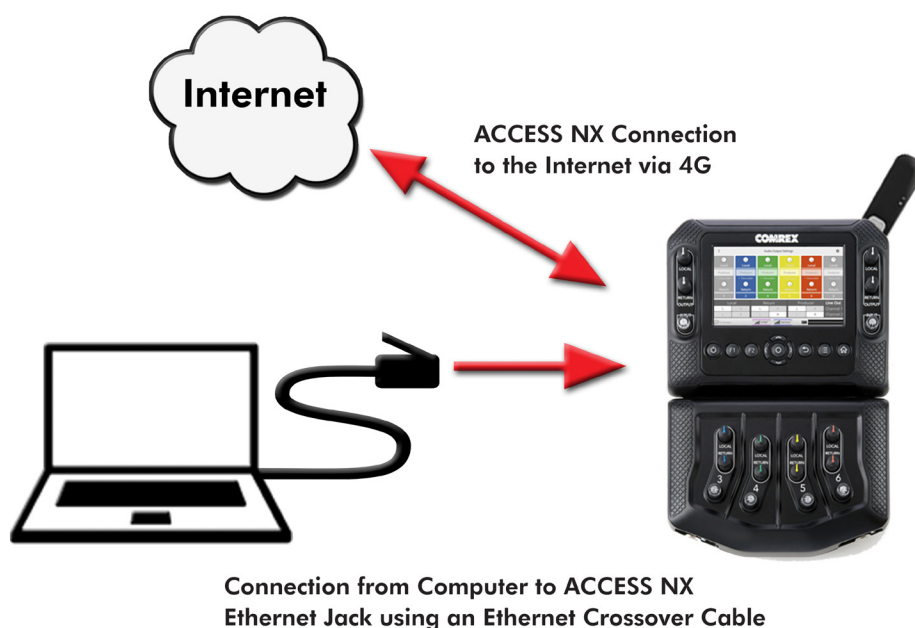
GATEWAY SETUP

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

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

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

xxx. ADVANCED SETTINGS

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

In many of the menus, you can access advanced settings by selecting the Options icon in the top right and pressing the Advanced box. If the advanced items are turned off, the box will show a red line. If they are turned on, you will see a green line.

In some menus, there is also an option to view only the items that changes have been made. This also reflects if it is on/off with the red or green line.
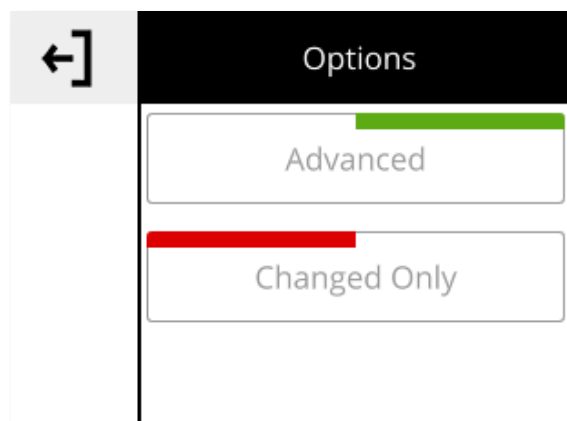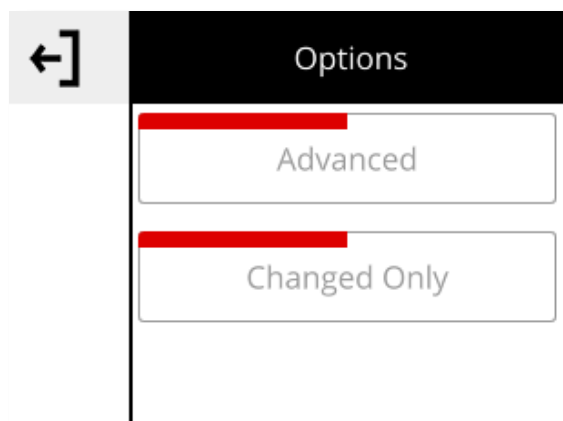
ADVANCED REMOTE SETTINGS

BACKING UP A CONNECTION

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

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

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

To enable an automatic backup, both the primary and secondary remote connections must first be defined and assigned profiles. Next, select the primary remote and select **Backup Remote.** Choose from the list the remote to be used for the backup.
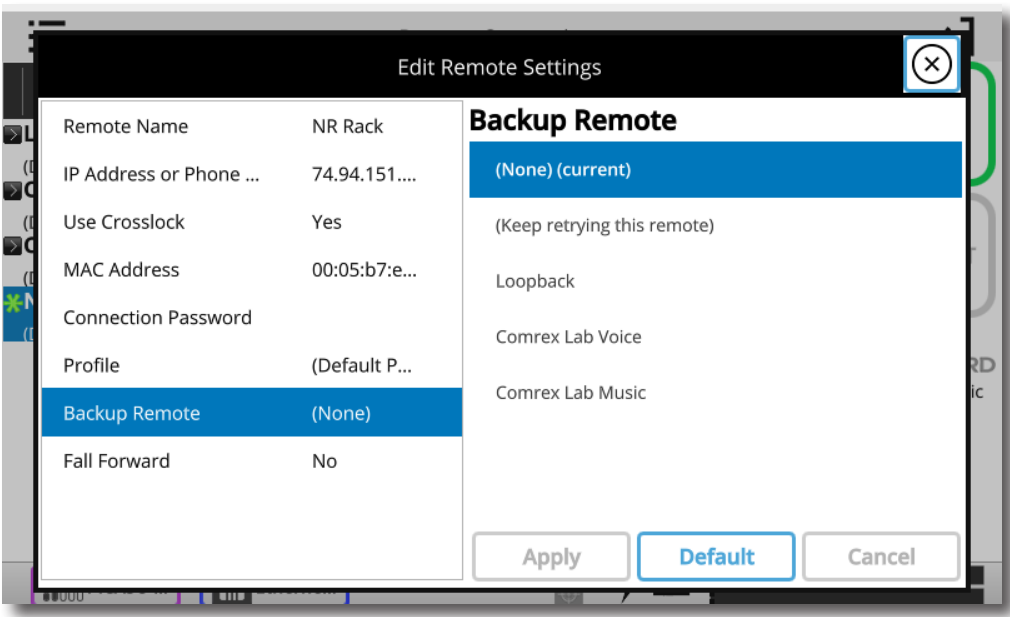
"AUTO FALL-FORWARD" FUNCTION

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

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

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

PROFILE SETTINGS

GLOBAL PROFILE SETTINGS
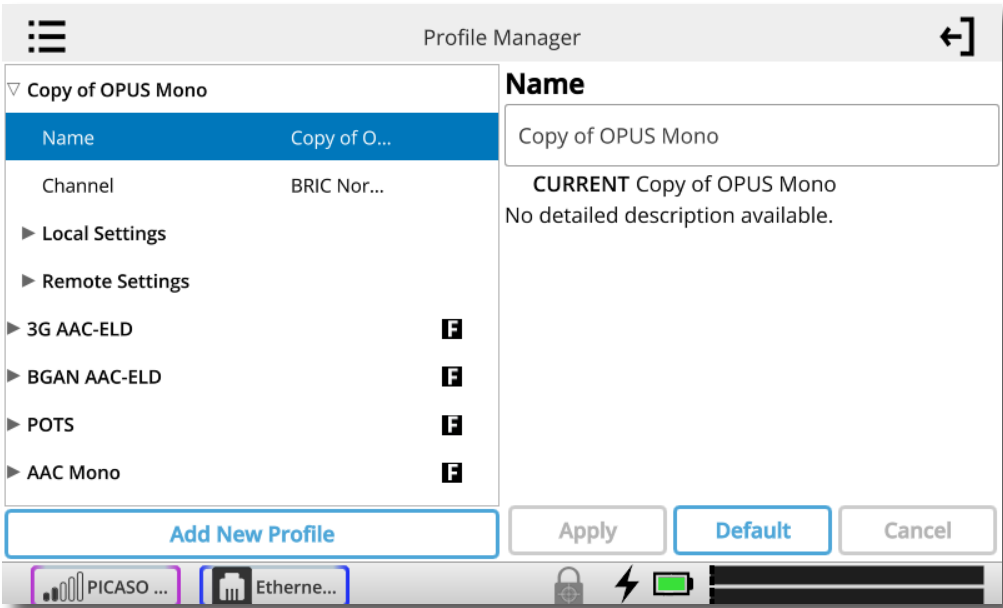
Profile Name - Allows you to name the new profile.
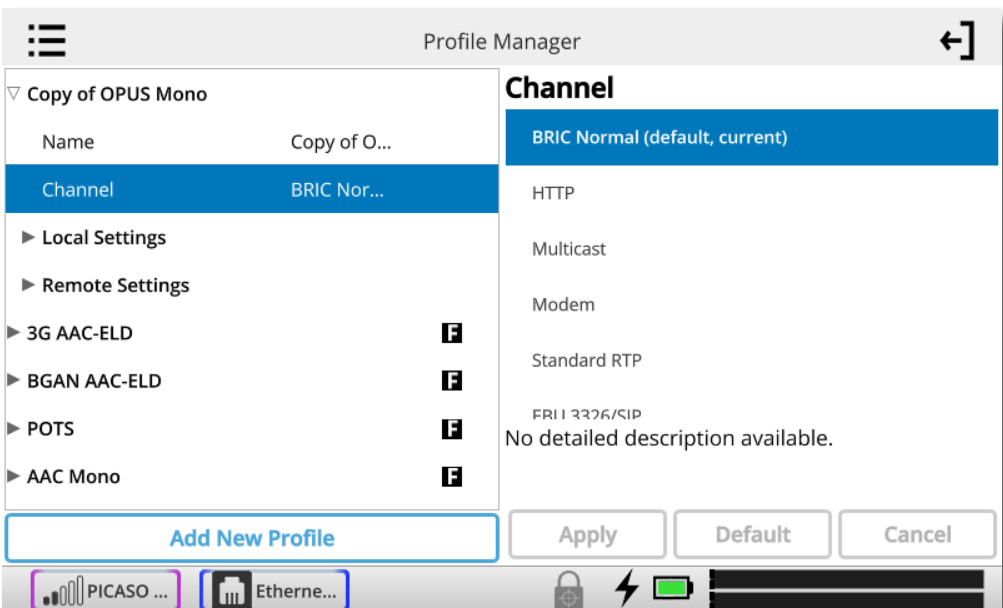
Channel - Here you can select whether this will be used as an IP connection (BRIC Normal), HTTP, Multicast, Modem (POTS connection) Standard RTP, TCP or an EBU 3326/SIP connection.

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

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

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

These compatibility modes are provided on a "best effort" basis. They are not guaranteed to be compatible with other manufacturer's implementations. ACCESS is not strictly compatible with Tech3326, because it does not support all mandatory encoders. For more information on EBU 3326/SIP, please see **"MAKING EBU 3326/SIP COMPATIBLE CONNECTIONS" on page 80**.

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

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

LOCAL & REMOTE SETTINGS

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

Each category lists identical options, so we'll cover only the **Local Settings**:
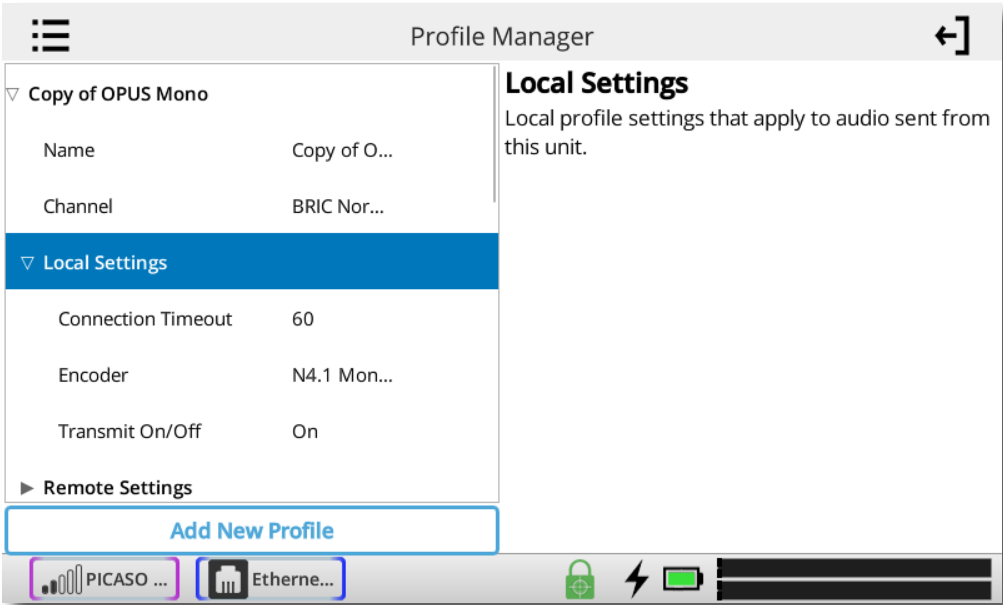
Connection Timeout - Under normal circumstances, a connection will be terminated on one end, and the other end will drop the connection. However, if a network failure occurs, or a connection is ended abruptly for some other reason, the system will drop the connection after a pre-determined time. The default is 60 seconds, but this can be shortened or lengthened here.

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

Transmit On/Off - This option determines whether the selected encoder (local or remote) is actually sending any data. By default, all encoders are turned on, but there may be circumstances where one-way operation is desired, such as multi-streaming **"MULTI-STREAMING" on page 86**. Selecting **Off** under **Transmit On/Off** under the **Local Settings** folder disables outgoing audio streaming. In the same way, selecting **Off** under the **Remote Settings** folder disables the incoming audio streaming from the remote encoder.

ADVANCED PROFILE SETTINGS

The options available in the default mode should provide good performance for most users. However, in some circumstances, it may be important to fine-tune some of the more obscure parameters that make NX work. In addition to the information printed below, most of these choices also have "help" information built into the selection on NX to remind users of what each function does.
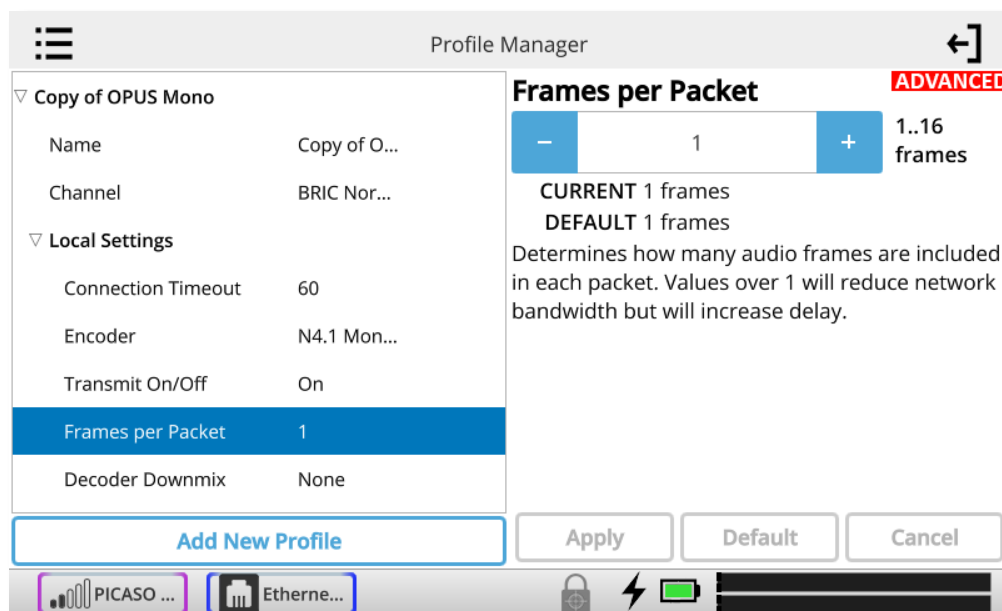
Frames per Packet - Allows the encoder to wait for X number of frames to exist before sending a packet. This option differs from FEC because each frame is only sent once. Setting this value to a number higher than one can reduce network usage, at the expense of delay. This is because this setting reduces the frequency with which packet overhead bits like IP and UDP headers are sent.

Decoder Downmix - This allows the decoded "stereo" (two-channel) audio that arrives at the receive end to be downmixed to a mono signal. The choices are **None**, **Mono Left Only**, **Mono Right Only**, and **Mono Full**. Except for **None**, these are mainly used for sending two different mono streams to two different destinations at the same time. For more information on these choices, see **"APPENDIX D - USING THE COMREX ACCESS DECODER DOWNMIX FUNCTION" on page 121**.

Loss Cushion - This choice instructs the buffer manager to ignore a certain percentage of late packets in its calculation. The default value is 5%. Applications that are not at all delay sensitive may wish to reduce this value to zero, while extremely delay sensitive applications may prefer to have this closer to 25%. By eliminating packets that arrive extremely late, delays can be reduced greatly. The decoder error concealment does a very good job of hiding any losses that may result.

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

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

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

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

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

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

Delay Cushion - The **Delay Cushion** setting instructs the jitter buffer manager to not attempt to drive the delay below a certain value. For example, if the delay cushion is set to 500mS, that amount of fixed delay will be added to the buffer. If the jitter manager needs to increase the buffer it will do so, but will not fall below the ½ second level.
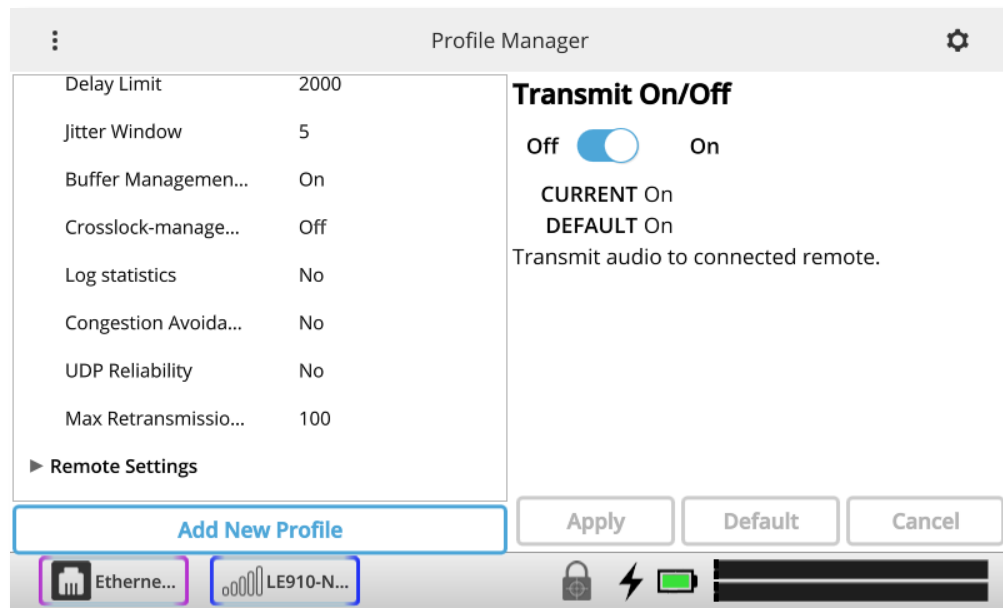
Delay Limit - The **Delay Limit** instruct the jitter buffer manager to not "wind" the buffer out beyond a certain delay value, regardless of how many packets are lost. This is useful in applications where staying below a certain delay figure is essential. However, use of the delay limit can result in very poor performance if the network jitter dramatically exceeds the set limit.

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

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

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

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

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

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

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

ADVANCED SYSTEM SETTINGS

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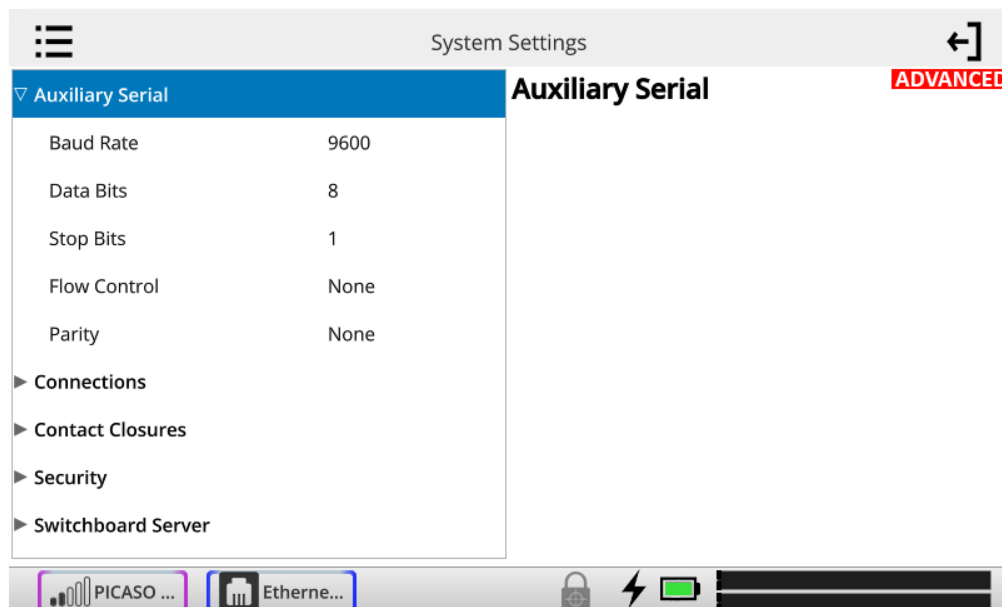
This allows you to set the parameters of the auxiliary serial data port. This port is always active during an IP connection and allows serial data transfer along the same path used for the audio data. It does not remove any audio data; the serial data is added to the packets and bandwidth is increased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

CONNECTIONS

Disable Congestion Avoidance – Turns "**Avoidance Congestion**" feature off.
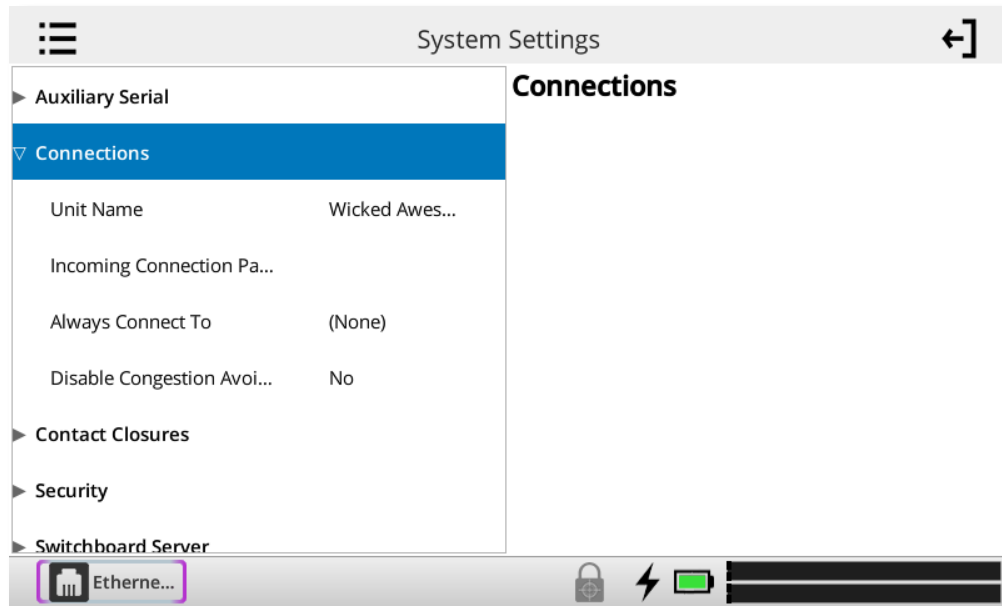
SECURITY
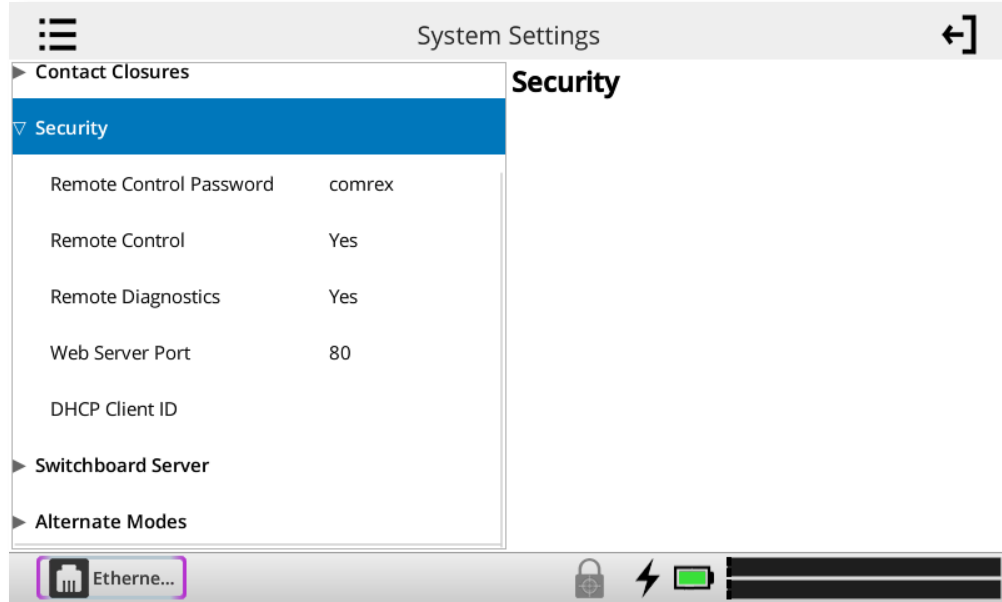
Remote Diagnostics - Enables Comrex support to connect to this unit using the SSH protocol for troubleshooting purposes. We recommend leaving this option enabled. Since SSH access requires a key value that is not disclosed by Comrex, generic SSH requests are rejected.

Web Server Port - In order to deliver the remote control web page, NX must "listen" on a certain internet port number for a request from a web browser. By default, web page servers listen on port 80 for incoming requests.

In some environments, you may wish to remotely control NX through your router, and port 80 may already be utilized by another device. This setting gives you the ability to change the port where the system listens for and delivers web pages from. **NOTE: you will now need to enter this new port number into your browser in order to see the unit. As an example, if the Web Server Port is changed from 80 to 84, the address of the unit must be entered in a browser in the following manner: http://192.168.1.142:84**

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

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

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

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

SWITCHBOARD SERVER
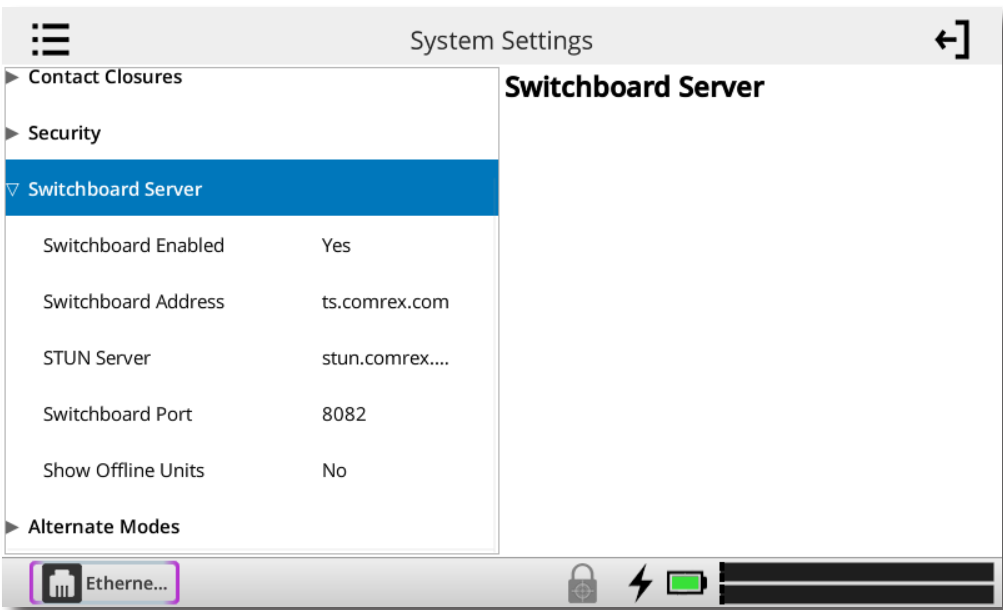
Switchboard Add (Address) – shows the IP address of Switchboard.

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

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

BRIC NORMAL SETTINGS

IP connections use a concept known as ports to differentiate between different applications on the same computer. A port is simply a number contained in the IP header, but it can be thought of as a physical opening in and out of your computer. Most firewalls function by opening the network to traffic with only specific port numbers.

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

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

Changing the port for incoming connections is done under **System Settings**.
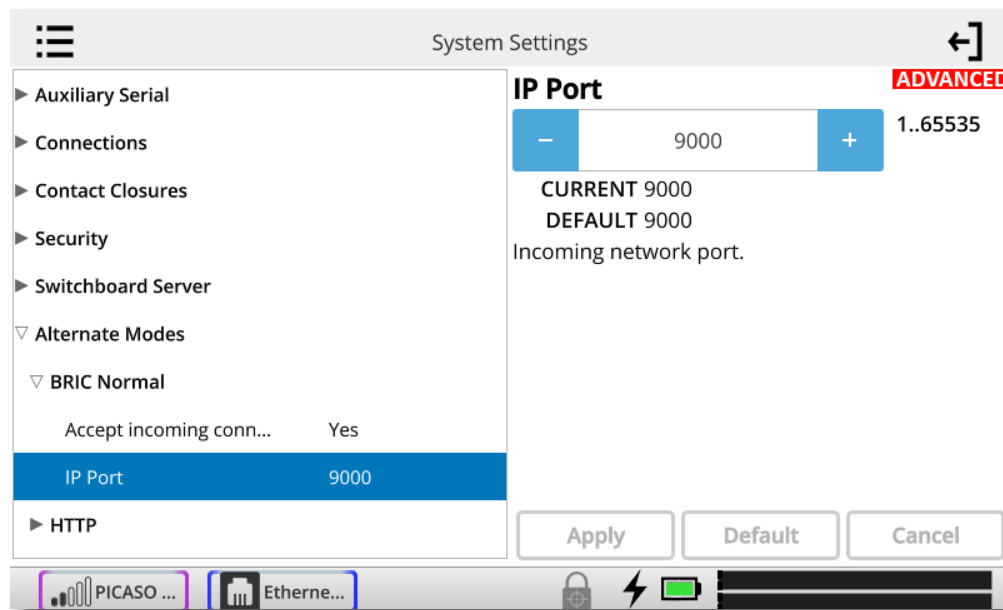
To change the destination port of an outgoing call, you must add the port number to the IP address in the correct format. For example, to initiate a connection to the Comrex test line at port number 5004, enter the following into the IP address field:

70.22.155.131:5004

Note that the last four digits of the IP address are the numbers corresponding to the port at the receive point.

Be aware that the call will fail unless the ACCESS on the far end is set to receive data on that port.

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

106

EBU 3326/SIP SETTINGS

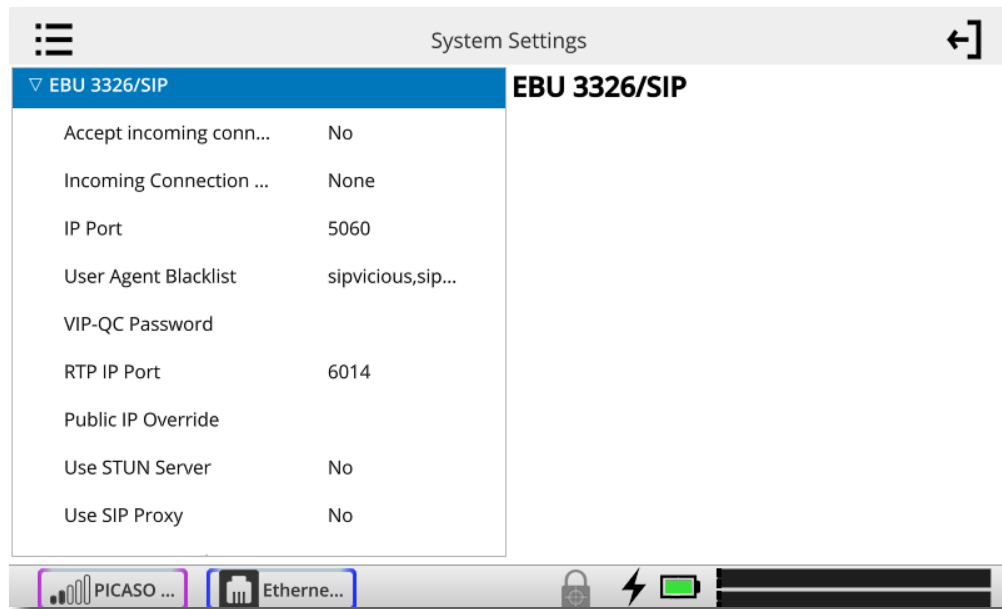**Accept incoming connections -** EBU 3326/SIP calls must be answered automatically on NX. If this option is disabled, no EBU 3326/SIP calls will be answered and only outgoing EBU 3326/SIP connections can be made.

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

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

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

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

RTP IP Port – Allows setting of RTP network port.

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

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

Use SIP Proxy – Enables/disables registration with the SIP proxy to use for inbound and outbound calls.
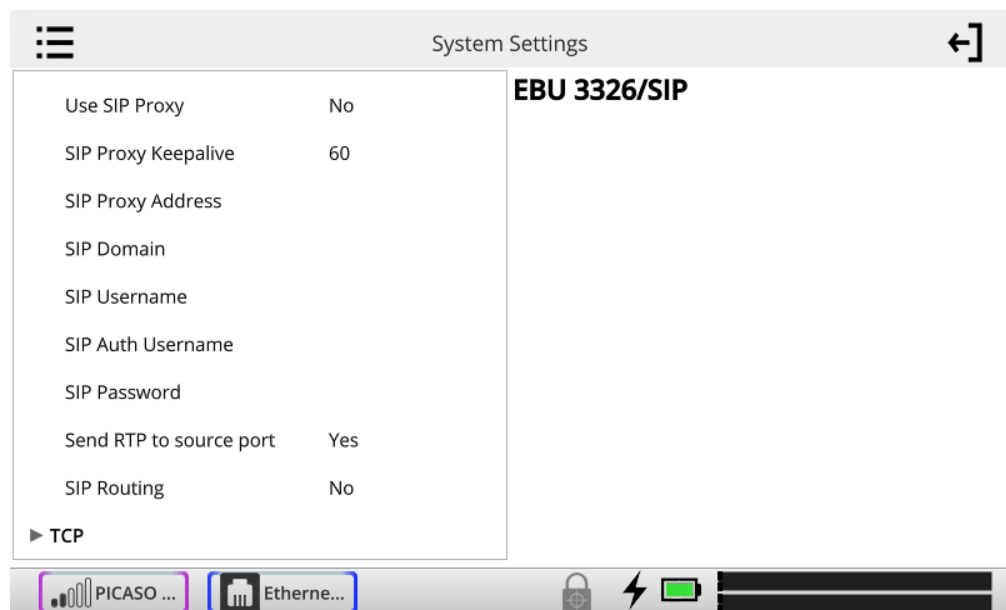
SIP proxy Keepalive - Sets "keepalive" interval time for SIP connections.

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

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

SIP Username – Allows entry of SIP username.

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

SIP Password - Allows entry of password for authentication.

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

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

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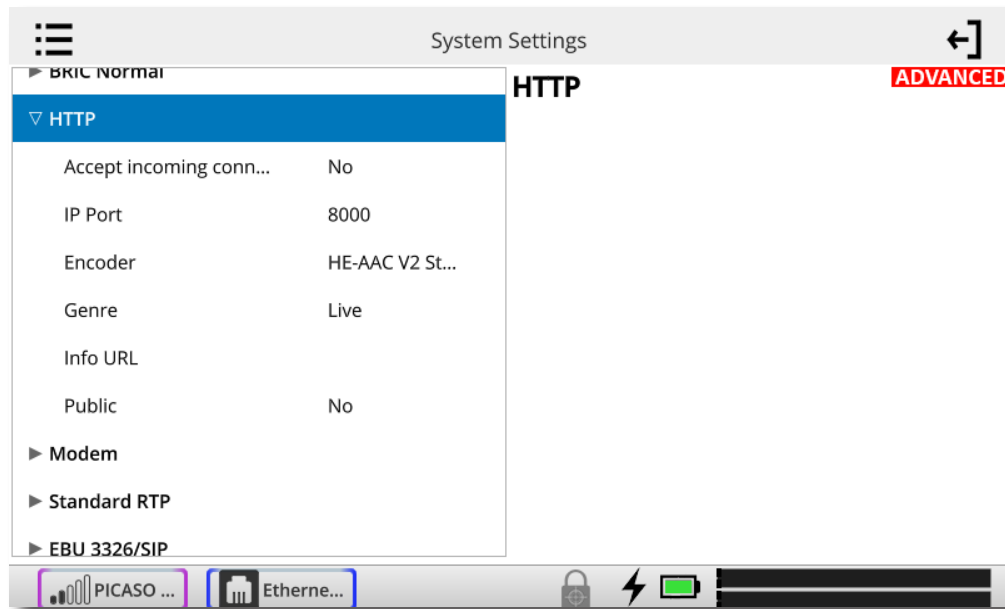
Accept incoming connections - Enables/disables the HTTP streaming function.

IP Port – Sets incoming network port.

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

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

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

Public - Enables/disables setting of the public stream.

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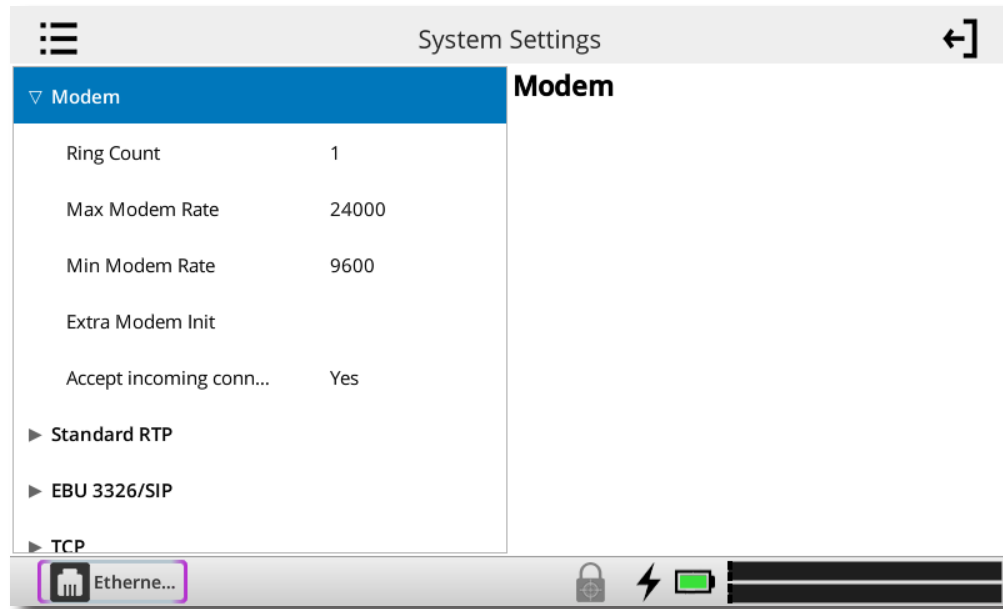
Ring Count – If auto-answer is enabled for incoming calls, sets the number of rings before line is answered.

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

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

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

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

STANDARD RTP SETTINGS

ACCESS NX uses the term "channel types" to differentiate between audio streaming modes that are incompatible with each other. One alternate mode is called "Standard RTP", and is a term used to describe a very simple streaming protocol, with no real handshake or setup requirements.
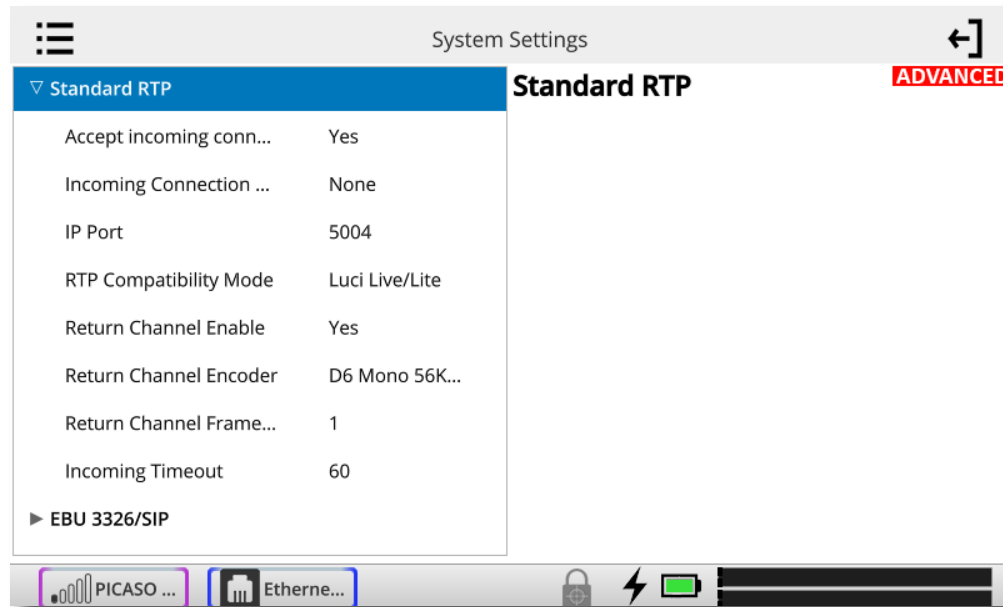
Accept incoming connections - RTP calls must be answered automatically on NX. If this option is disabled, no RTP calls will be answered and only outgoing RTP connections can be made.

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

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

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

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

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

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

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

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

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

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

TCP SETTINGS
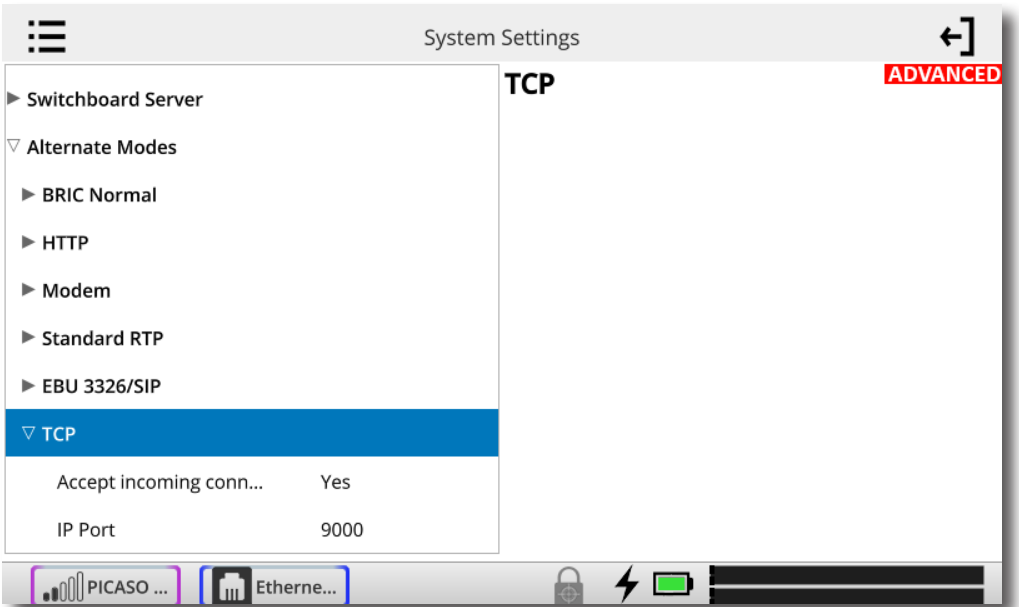
Accept incoming connections - Enables/disables the ability for TCP connections to be accepted by the A.

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

CROSSLOCK SETTINGS

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

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

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

Authentication - ACCESS NX uses security certificates assigned to the codec hardware to authenticate it as a Comrex product. This option determines whether connections will be made to codecs without these certificates. Certificates are assigned to codecs by the Switchboard server. This option is defaulted **Off**.

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

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

FEC - **CrossLock** has a powerful Forward Error Correction algorithm that is enabled in the presence of multiple networks, using any excess network bandwidth to add in the parity required. Use of FEC is recommended, but it can be disabled here.

FEC Delay - Controls both how much delay is introduced into the system by FEC , and also to an extent how effective the recovery is (which is dependent greatly on the packet rate). The default of 100mS should only be altered on recommendation of Comrex support.

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

Retransmit Delay - **CrossLock** automatically provides an extra "Retransmit Cushion" that provides some time to make ARQ error correction effective. The default amount of time is twice the measured round trip delay of the network (2xRTT). This has been shown to be most effective on most networks, but can be altered lower (1xRTT, none) or higher (3xRTT) using this menu.
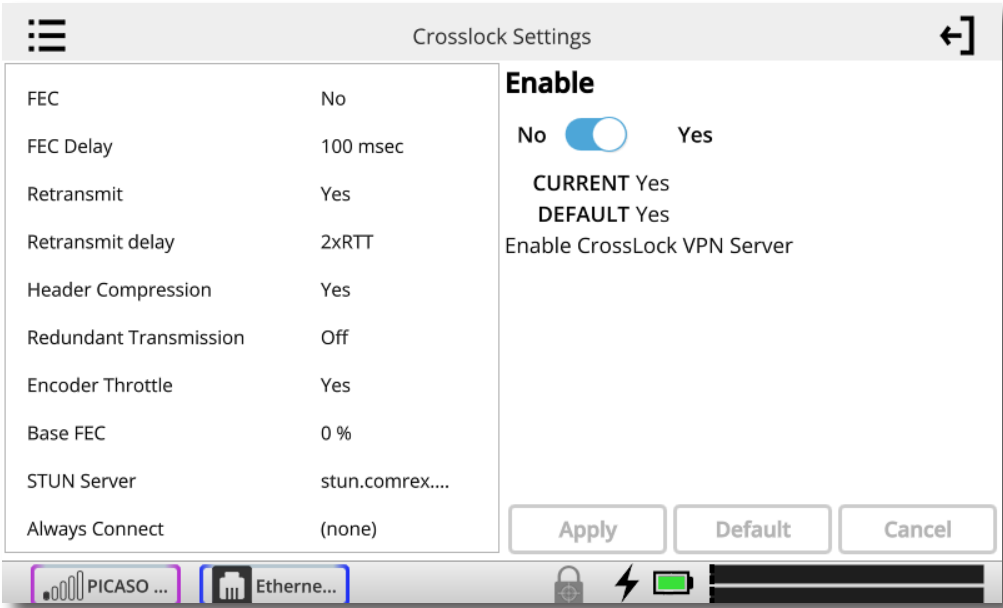
Header Compression - The nature of Internet packets sometimes results in IP overhead (RTP headers and other info) actually using nearly as much bandwidth as the payload. **CrossLock**, by default, compresses some of these headers to conserve network bandwidth. In instances where the network rejects this, or packet inspection is required, this compression can be disabled.

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

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

Base FEC - This parameter applies a constant rate of FEC targeting recovery of the specified expected loss rate. It is measured in percent packet loss to be corrected. This is useful when retransmission is not effective (e.g., high delay network) and auto-FEC is not working as desired. It should be used on recommendation of Comrex support.

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

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

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

XXXI. ADVANCED 3G/4G NETWORK SETTINGS

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

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

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

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

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

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

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

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

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

To communicate with a Luci Live device:

   a. **Initial Setup** - This will define all Standard RTP connections to be Luci Compatible

   - ACCESS Rack - On the **System Settings Tab**, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, choose **Luci Live**.

   - NX - Choose **System Settings** on the display. Enable Advanced options and under Alternate Modes select **Standard RTP Settings.** Select **RTP Compatibility Mode** and choose **Luci Live**.

   b. **Incoming Connections** - Luci Live sends either an AAC or HE-AAC stream to the ACCESS on UDP port 5004. These streams will be automatically decoded. By default, a return channel of AAC 56kb/s mono is returned to the Luci Live product. The return channel may be altered to any Luci-compatible mode in the **Systems Setting** section. ACCESS that do not have the AAC upgrade applied will not create a return channel.

   c. **Outgoing Connections** - Build a profile using the **Profile Manager** on either the ACCESS Rack or NX and select a Channel Mode of **Standard RTP**. Then choose a Luci-compatible encoder for the outgoing call. The Luci software will control what type of stream, if any, is returned to the ACCESS.

2. **Zephyr Xstream** - Xstream Firmware version 3.2.0 and higher support an "RTP Push" function that is compatible with ACCESS in some modes. ACCESS products are not currently compatible with the Xstream's HTTP and SIP streaming functions. There are several limitations imposed by the Xstream when using the RTP Push function:

   - On the Xstream, only AAC and MP3 coding are available in this mode, and ACCESS is only compatible with the AAC mode

   - The Xstream uses downsampling in modes below 96Kb/s, which is not supported by ACCESS.

   - In order for an Xstream to decode an ACCESS stream, the default decoder setting must be changed from <Auto> to <AAC> in the codec menu of the Xstream.

To communicate with a Zephyr Xstream:

> a Initial Setup - This will define all Standard RTP connections to be Xstream Compatible.
>
> - ACCESS Rack - On the **System Settings Tab**, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, select **Zephyr Xstream**.
>
> - ACCESS NX - Choose **System Settings** on the display. Enable Advanced options and under Alternate Modes select **Standard RTP Settings.** Select **RTP Compatibility Mode** and choose **Zephyr Xstream**.
>
> b **Incoming Connections** - Zephyr Xstream sends an AAC stream to the ACCESS on UDP port 9150. These streams will be automatically decoded. By default, a return channel of AAC 96kb/s mono is returned to the Xstream. The return channel may be altered to any Xstream-compatible mode in the **Systems Setting** section. ACCESS that do not have the AAC upgrade applied will not create a return channel.
>
> c **Outgoing Connections** (ACCESS AAC Option required) - Build a profile using the **Profile Manager** on either the ACCESS Rack or Portable and select a Channel Mode of **Standard RTP**. Then choose an Xstream-compatible encoder for the outgoing call. The Xstream will control what type of stream, if any, is returned to the ACCESS.

3 **Standard RTP** - This mode is set to receive a basic, unformatted AAC stream within a standard RTP/UDP structure. At present, this mode does not offer compatibility with other industry devices.

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

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

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

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

INCOMING SERVICES

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

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

OUTGOING SERVICES

Service	Destination
NTP	0.comrex.pool.ntp.org:123 (UDP)
Switchboard	switchboard.comrex.com:8090, switchboard.comrex.com:8081 (secondary) (TCP)
STUN	stun.comrex.com:3478 (UDP)

Under most circumstances, NX 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 following setting applies to both codecs in the link (encoder and decoder):

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

1   On the ACCESS Rack, enter the Web-based Interface and choose the **System Settings** tab. On the ACCESS NX, navigate to **System Settings.**

2   Turn advanced options on for both units.

3   Find **Standard RTP Settings** and choose to edit the **RTP Compatibility mode**.

4   Change this setting to **Standard** and click **Apply**.

DECODE SIDE SETTINGS ONLY

Also under **Advanced Standard RTP Settings**, find the **Return Channel Enable** entry. Disable the return channel and click **Apply**. This will make sure that no channel will be set up in the direction to the encoder.

ENCODE SIDE SETTINGS ONLY

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

Next, create your outgoing remote on the **Remote Connections** menu. 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** menu.

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

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

Use of the decoder downmix function has two drawbacks: As with all multi-streams in ACCESS, full duplex operation is only supported to one destination. Also, both channels of the stream are actually delivered to both destinations over the network, utilizing more incoming network bandwidth to the decoder than necessary.
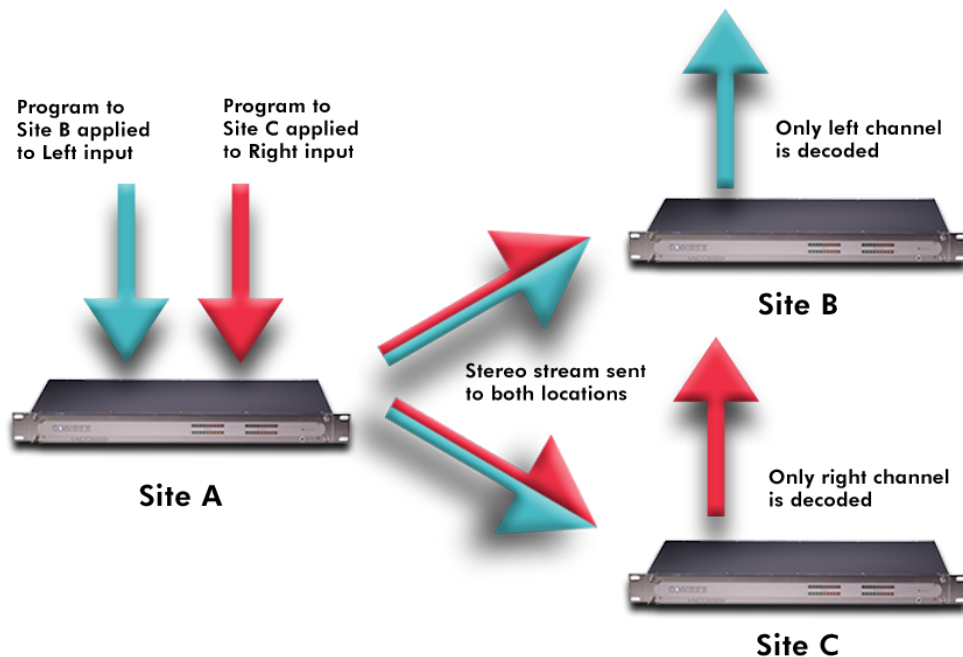
The figure above shows a typical connection using the Decoder Downmix function from the encode site (A) to two decode sites (B and C). For clarity, no return audio channel is shown from either B or C (although one could exist from either but not both).

The user at site A builds two separate connection profiles, each using the same local stereo encode option. He will turn off the remote encoder on both profiles. On the profile labeled "**Downmix L**", under advanced options, he will go to the remote connection side and select "**downmix**". Here he will instruct the remote decoder to output only "**Mono Left Only**" through both Left and Right audio outputs.
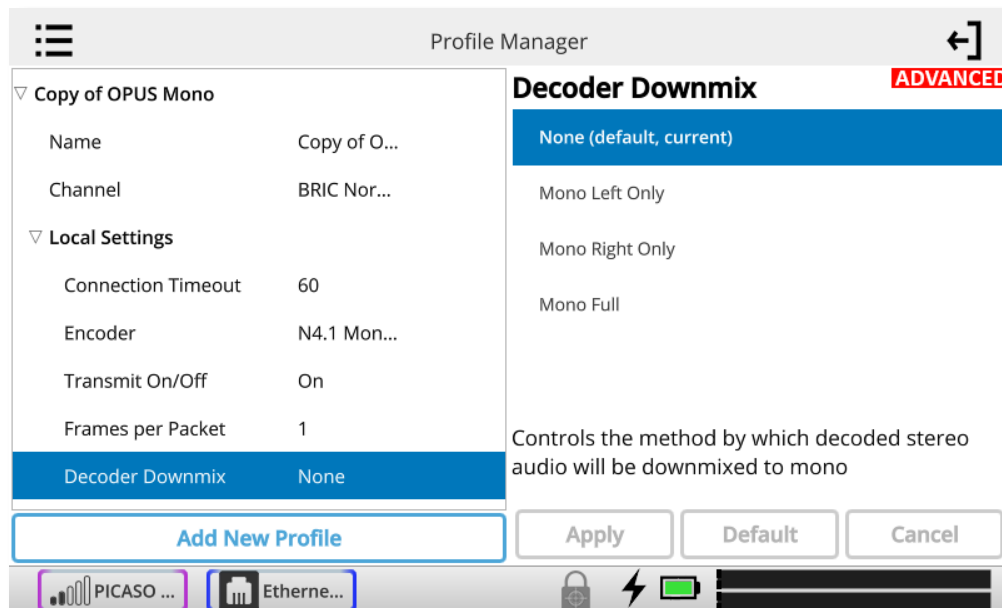
He will build corresponding "**Downmix R**" profile, selecting the "**Mono Right Only**" option in the same location.

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

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

CONNECTIONS

- Power: 4-pin mini-DIN female, pins 1+3 +24V, pins 2+4 ground
- XLR In: 3-pin female, pin 1 ground, pin 2 +, pin 3 –
- Stereo Line In: 3.5mm female, tip=left, ring=right, sleeve=gnd
- Line Out: 3.5mm female, tip=left, ring=right, sleeve=gnd
- Headphone Out: 1/4" female, tip=left, ring=right, sleeve=gnd
- Serial: 8-pin DIN female, pinout in Section 2
- Contact Closures: 9-pin DIN female, pinout in Section 2
- USB: USB Type A x 2
- Ethernet: 8-pin modular, 1000Base-T wiring

AUDIO SPECIFICATIONS

XLR Input
    Type: Balanced
    Impedance: 20k Ohms (pins 2-3)
    Level: Line, Mic HI, and Mic LO

Stereo Line Input
    Type: Unbalanced
    Impedance: 20k Ohms (tip to sleeve, or ring to sleeve)
    Level: -10 dBu nominal, +10 dBu max

Line Output
    Type: Unbalanced
    Impedance: 47 Ohms
    Level: -10 dBu nominal

POWER

Voltage: AC: 100-240 VAC, 50-60 Hz
         DC: 24V

Power: 24 Watts with all peripherals

PHYSICAL

Dimensions: 7.5" W (19.05 cm), 6" D (15.24 cm), 4" H (10.16 cm)
Weight: 3.16 lbs (1.43 kg)
Shipping: 6 lb (2.7 kg) with all peripherals and packing

COMREX SWITCHBOARD TRAVERSAL SERVER USE

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

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

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

XXXVIII. LICENSE AND WARRANTY DISCLOSURES

FOR COMREX ACCESS NX

LICENSES

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

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

ncurses
Copyright (c) 1998,1999,2000,2001 Free Software Foundation, Inc.
See further Copyright notice below

dropbear
Copyright (c) 2002-2004 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.
See further Copyright notice below

libxml2
Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.
See Further Copyright notice below

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

PuTTY is copyright 1997-2003 Simon Tatham

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

Further copyright notice for ncurses, dropbear PuTTY and libxml2

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

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

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
Libpcap
tcpdump
Copyright © 1988, 1989, 1991, 1994, 1995, 1996, 1997
The Regents of the University of California. All rights reserved.

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

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

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

WARRANTY

All Equipment manufactured by Comrex Corporation is warranted by Comrex against defects in material and workmanship for one year from the date of original purchase, as verified by the return of the warranty registration card. During the warranty period, we will repair or, at our option, replace at no charge a product that proves to be defective, provided you obtain a return authorization from Comrex and return the product, shipping prepaid to Comrex Corporation, 19 Pine Rd, Devens MA 01434 USA. For return authorization, contact Comrex at 800-237-1776 or 978-784-1776 or email techies@comrex.com.
This warranty does not apply if the product has been damaged by accident or misuse or as a result of service or modification performed by anyone other than Comrex Corporation.

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

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