
ACCESS 4.0

Addendum

Product Manual

**COM
MREX**

ACCESS 4.0 FIRMWARE ADDENDUM

The ACCESS manual describes operation of firmware 3.x. Firmware 4.x adds significant new features and changes the default behavior of the product in many ways. This addendum describes those changes.

INTRODUCTION

MAJOR CHANGES IN FIRMWARE 4.0

If you are familiar with ACCESS 3.0 firmware, or if updating an ACCESS from a previous firmware to 4.0 or higher, here are the major differences:

- 1 **CrossLock*** - This is a new, optional reliability layer available for connection to other Comrex devices running compatible firmware. **CrossLock** allows the use of two simultaneous networks for added reliability
- 2 **Switchboard**** - Previously referred to as BRIC-TS, Switchboard server takes a bigger role in making connections using **CrossLock**. It is highly recommended (but not required) for all **CrossLock** connections.
- 3 **Ports** - **CrossLock** makes connections on UDP port **9001**. Legacy Comrex audio codec connections are made on UDP port **9000**. This may require that you open additional ports in your router or firewall settings.
- 4 **Encoders** - Version 4.0 has removed the ability to choose several of the more dated encoder offerings like HQ1, HQ2 and ULB. This is because the existing high-quality compression choices (AAC family and Opus) are superior for virtually all uses. The default profile used in 4.x (for connections that haven't been assigned a profile) is now Opus mono (this is adjustable in the User Interface). Connections made to 3.x and lower units will still work with these legacy encoders—they just are not available to choose for outgoing profiles.
- 5 Previous versions of firmware used TCP port **8080** for XML commands used by the web interface and the **Device Manager**. These connections are now made on TCP port **80** (along with all other web traffic). In some instances, you may need to change the settings of **Device Manager** to properly interface with your ACCESS.
- 6 Using **CrossLock**, the decode jitter buffer (and therefore the end-to-end delay) is visually represented on a bar graph, and can be manually manipulated by means of a slider on the user interface.
- 7 Stereo POTS mode and POTS PPP mode are no longer supported.

*CrossLock is not supported when using Linear PCM or FLAC algorithms.

If you are utilizing Switchboard with a unit that was updated to 4.0 firmware and is in a heavily firewalled network, TCP port **8082 and TCP port **8090** must be open for communicating with Switchboard. After ten minutes of your updated unit being online, it will receive a certificate from Switchboard and will then connect through TCP port **8090**. At this point, you can close TCP port **8082** if desired.

INTRODUCTION TO CROSSLICK

CrossLock describes a new reliability layer that gets established between Comrex devices in advance of a connection. This layer takes the form of a Virtual Private network (VPN) between the devices. The ACCESS Media stream is carried within this VPN. This is shown in Figure 1.

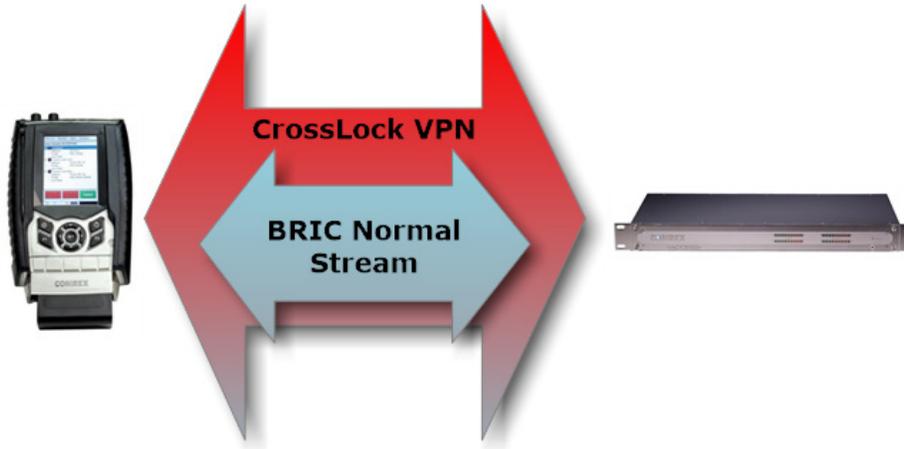


FIGURE 1

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 either end of the link.

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

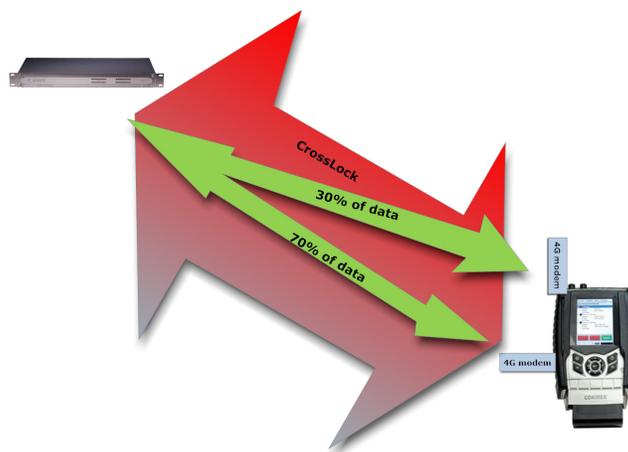


FIGURE 2

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 has redundant and fast recovery capability, it is preferred for wireless networks.

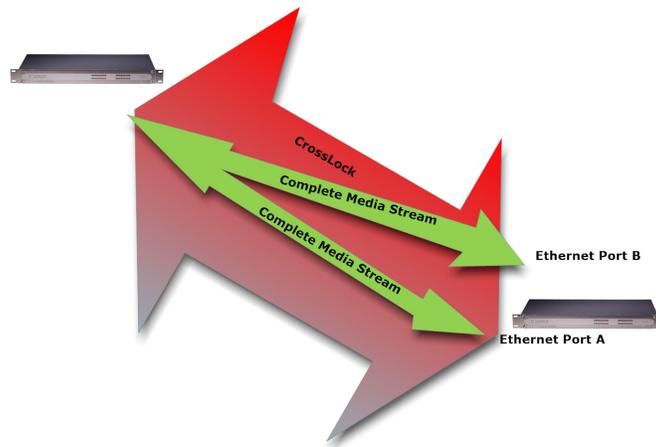


FIGURE 3

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

CROSSLOCK AND SWITCHBOARD

It is recommended that **CrossLock** connections be made in conjunction with the Switchboard Traversal Server. ACCESS users can get a Switchboard account for their codecs by contacting Comrex. For configuration and operation of Switchboard Server for ACCESS, see the technote on the Comrex web site.

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 or BRIC-Link codec in the fleet. This list appears on the **Connections** tab of the ACCESS, both in the Web-based user interface and (in the case of ACCESS Portable) on the display.

Connections				Media Statistics	CrossLock	Audio Metering	Profiles
REMOTE ACCESS UNITS							
Name	IP Address	Current State	Receive Status				
Profile	Crosslock Address	Last State	Transmit Status				
Omaha beach	[74.94.151.145:1132] 3000	connected (Connected)	Rx: Opus Mono Tx: N4.1 Opus Mono 48kbps				
Nags Head	74.94.151.145:1132	not connected					
My BL2	0.0.0.0	not connected					
Master Blaster	0.0.0.0	not connected					
Kabul office	00.21.2b.0f.00.36	not connected					
Admiral Halsey	74.94.151.145:1134	not connected					
00.21.2b.0f.00.36	00.21.2b.0f.00.36	not connected					

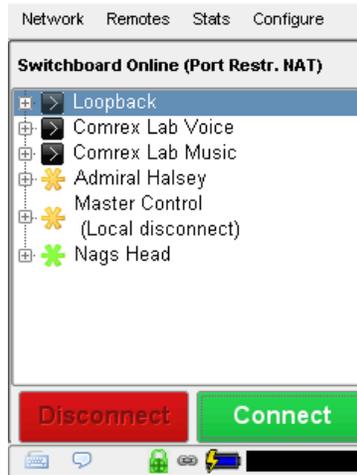


FIGURE 4

On ACCESS Portable, 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 CROSSLINK 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 or BRIC-Link 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 as shown in Figure 5. Note the "Lock" icon in the lower banner is lit green during a successful **CrossLock** connection. 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.

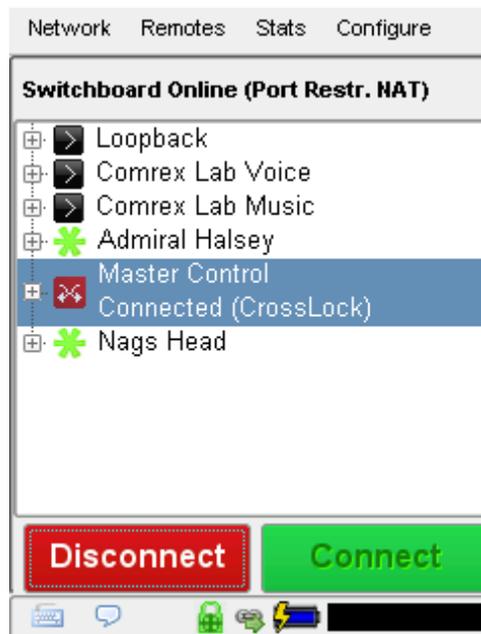


FIGURE 5

MAKING NON-CROSSLINK CONNECTIONS IN FIRMWARE 4.0

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

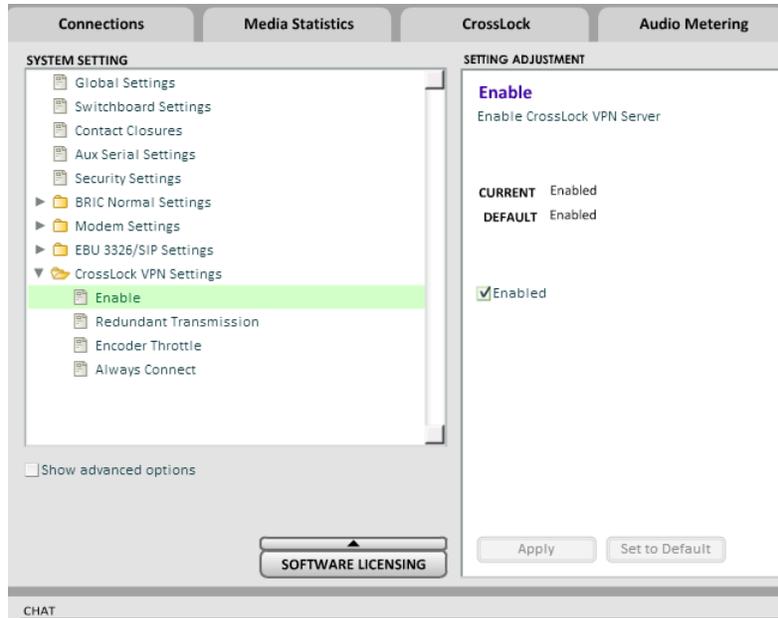


FIGURE 6

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

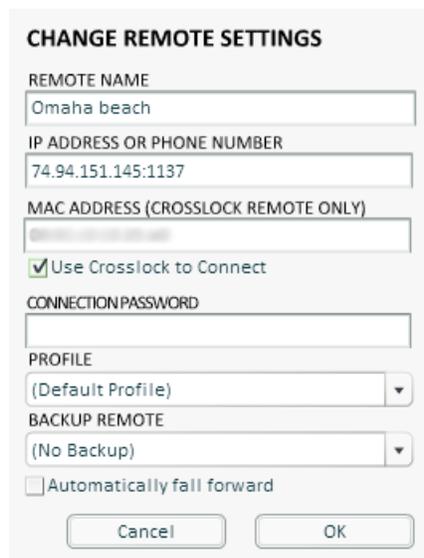


FIGURE 7

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. As shown in Figure 8, this is input to the “Create New Remote” pop-up in the “MAC Address” field.

The image shows a 'STORE NEW REMOTE' dialog box with the following fields and controls:

- REMOTE NAME: [Text Input]
- IP ADDRESS OR PHONE NUMBER: [Text Input]
- MAC ADDRESS (CROSSLOCK REMOTE ONLY): [Text Input]
- CONNECTION PASSWORD: [Text Input]
- PROFILE: (Default Profile) [Dropdown]
- Buttons: Cancel, OK

Below the dialog, a 'Store New Remote' button is highlighted with a green border, and a 'Remove Stored R' button is partially visible.

FIGURE 8

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.

CROSSLOCK STATS

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

The **CrossLock** stats are available on ACCESS Portable under **Stats->CrossLock stats**. On the Web-based interface, the **CrossLock** tab becomes active.

The **CrossLock** tab is similar to the information available on the **Statistics** tab, which shows streaming performance without regard to the **CrossLock** layer. The **CrossLock** tab shows finer details about network performance in both directions than can be obtained through the **Statistics** tab.

In addition, the **CrossLock** tab contains the **Delay Slider Bar**. This bar gives a visual indication of the target (delay the system thinks is required) and actual delay of the link. The default of the slider bar is “automatic” operation, but manual mode can be engaged in circumstances where desired.

As shown in Figure 9 you can choose between seeing graphs for the transmit (outgoing) or receive (incoming) side of the link using the pull down option in the upper left side.

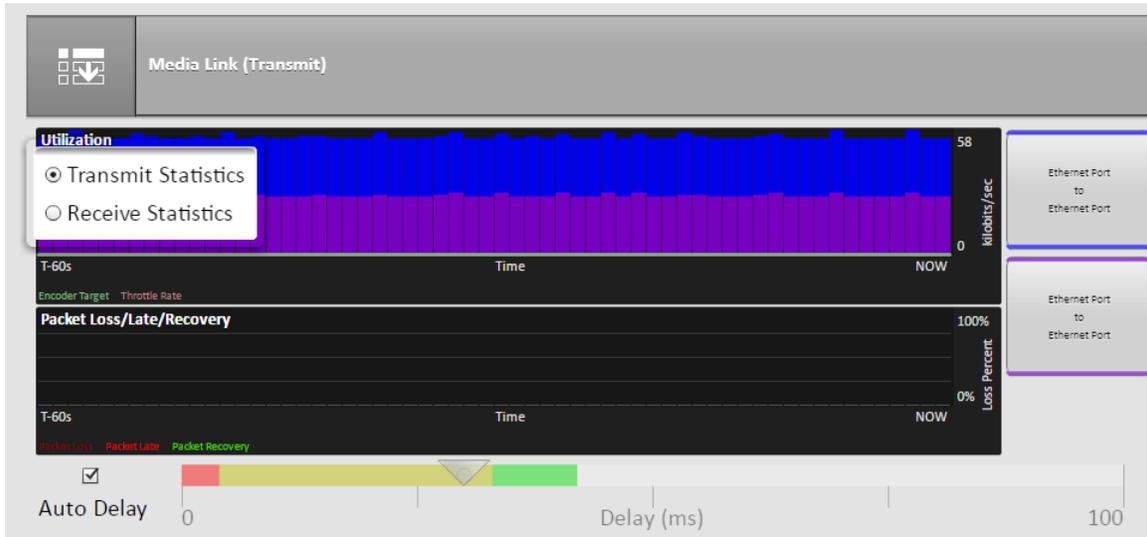


FIGURE 9

UTILIZATION GRAPH

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

If more than one network device is in use, the utilization graph will be color coded, indicating the relative utilization of each network device. The color code key for each network device appears on the right side of the graph. On ACCESS Portable, the key is below the graph.

Overlaid on the network utilization graph are two colored lines:

- 1 **Encoder target** - This reflects the bitrate chosen in the profile used in the connection. This is treated as a maximum value, so utilization should mostly remain below this line. Because these values are averaged, there may be moments where the utilization moves above the target line momentarily.
- 2 **Throttle rate** - When **CrossLock** throttling is enabled (the default state) this line indicates how much throttling will be applied. You will see utilization stay mostly below the throttling line.

PACKET LOSS GRAPH

The bottom graph indicates, in percentage terms, what's gone wrong on the network during each one-second window. Three different color-coded entries appear here:

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

DELAY SLIDER

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



FIGURE 10

Figure 10 shows the **Delay Slider**. In this figure, the slider is in “**Auto Delay**” mode and the information on the slider is purely for informational purposes. Clicking off the “**Auto Delay**” box sets the system to **Manual Delay** mode and allows the slider to be moved with a mouse.

The entire slider is scalable, and the range of it from left to right will vary from one hundred milliseconds to several seconds depending on the range of delays currently being addressed. In either **Auto** or **Manual** mode, a series of color bars are overlaid on the slider, to signify delay “zones” of safety. Furthest left is the red zone, which indicates a buffer level that is too low for stable transmission. The yellow zone indicates a delay buffer that may have stability issues, and the green zone indicates a buffer level that should provide stability. These “zones” scale, increase and decrease in size based on the history of jitter experienced by **CrossLock** on the network.

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



FIGURE 11

Figure 11 shows the slider in “**Manual Mode**”. Here, the arrow becomes a moveable cursor, and it’s up to the operator to determine how best to set the compromise between delay and stability.

Any settings made in Manual Mode will be erased after the current **CrossLock** session is terminated. In order to make delay buffer changes permanent, use the settings in the profile manager as outlined in the manual.

CROSSLOCK TAB DETAILED VIEW

A powerful feature of the **CrossLock Link** tab is to allow the user to “drill down” to the statistics for each network interface, and view the performance of that network alone. By clicking the button that appears for each interface on the right side of the tab, a new window opens that shows graphs similar to the “overview” graph, but limited to the performance of that particular network.

The **Detailed View** is most useful when more than one network is being used by **CrossLock**, as it allows comparison of the quality and delay figures of the various networks. As with the overview graphs, a choice is available in the pull-down menu to select between transmit (outgoing) data and receive (incoming) data for each network.

Due to CPU resources, **Detailed View** is only available on the Web-based user interface.

BONDING VS REDUNDANCY IN CROSSLOCK

When using **CrossLock** with multiple networks, the system will default to “Bonding” mode, which sums the data capability of each network together and determines the proper allotment of data between them. This is the best mode for wireless or any other network with possible congestion problems. Because of the dynamic data allotment, one network can disappear entirely with minimal audio corruption.

For users on networks where congestion is not an issue, and confidence is high, Redundant mode may be a better choice. In this mode, the entire audio channel is delivered to each network. Redundant packets at the decoder are discarded. While this mode uses more bandwidth, it results in less interruption if one network is lost entirely.

To change **CrossLock** from the default Bonding to Redundant mode, go to **System Settings->CrossLock VPN settings** and choose “**Redundant Transmission**”.

CROSSLOCK ADVANCED SETTINGS

Selecting the **Advanced** option under **CrossLock VPN** settings reveals the following **CrossLock Advanced** settings:

UDP Port - By default, **CrossLock** uses UDP port **9001** for connections. For best results, this port should be open for incoming data on at least one of the codecs in the link. This means that unless the ACCESS is 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 firmware 4.0 and higher uses security certificates assigned to the codec hardware to authenticate it as a Comrex product. This option determines whether connections will be made to codecs without these certificates. Certificates are assigned to codecs by the Switchboard server after an upgrade to firmware 4.0 or higher (Switchboard upgrade not necessary). Because some codecs may be firewalled and not received certificates after upgrades, this option is defaulted off.

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

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

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.

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.

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.

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.

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.

FIRMWARE 4.0 TOOLBOX

Aside from the **CrossLock** function, firmware 4.0 features a new **Toolbox** network manager that can be accessed either from the Web-based user interface or the **Device Manager** software. This allows easier network configuration, especially on ACCESS Rack.

USING DEVICE MANAGER

Figure 12 shows that when running firmware 4.0, five tabs appear on the right-hand pane after **Device Manager** has logged in (instead of the usual four). The fifth tab is labeled **Web Configuration**. This will open a simplified setup interface on ACCESS called **Toolbox**. The **Toolbox** interface allows you to configure several options including the Ethernet port. You will need to log in to **Toolbox** separately with a user name (any) and password (default = **comrex**) to enter the **Toolbox**.

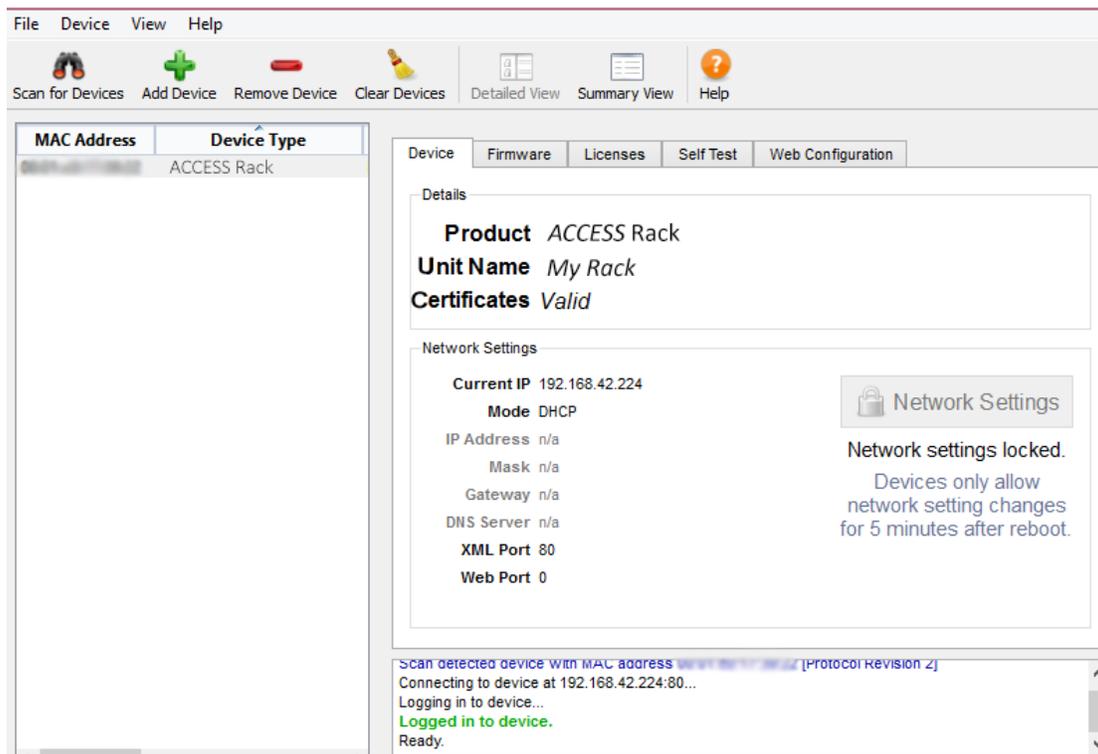


FIGURE 12

Once logged into **Toolbox**, choose the **Network/Admin/CrossLock** option and then choose **Set up Ethernet**. Choose the Ethernet port that appears in the list. Figure 13 shows the Ethernet settings of **Toolbox**.

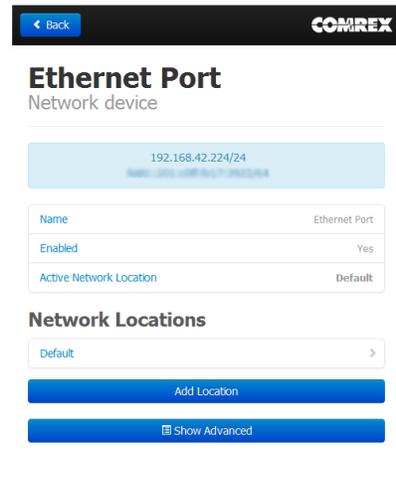


FIGURE 13

Toolbox also allows you to configure any wireless devices attached to the USB ports on ACCESS.

USING TOOLBOX VIA WEB INTERFACE

Along with **Device Manager**, **Toolbox** can also be accessed directly through the built-in web page via a browser. To log into **Toolbox** enter the device's address as `<ip_address>/cfg` (e.g. `192.168.0.34/cfg`)

NEW NETWORK MANAGER FEATURES

The following new features are present on both the touch-display user interface on the ACCESS portable and the web-based **Toolbox**.

LOCATIONS

ACCESS firmware 4.0 includes the ability to have multiple “locations” programmed into it for different network settings. E.g., if you are moving ACCESS between venues, and want to store the static IP information for each venue, you will define a new “location” (giving it a unique name) using the “**Add Location**” option shown in Figure 14. Once multiple locations are defined, you can switch between them using the “**Active Location**” option in Figure 14. 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.

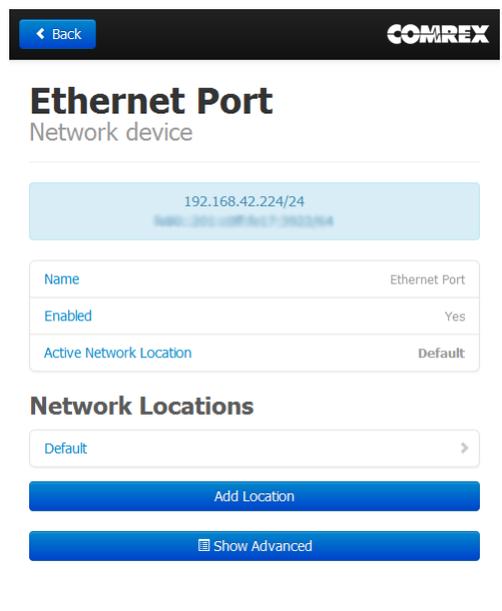


FIGURE 14

When setting up a Wi-Fi connection in firmware 4.0, you can scan for all available Wi-Fi networks using the “scan” function as in previous firmware. But once selected, a Wi-Fi network must be applied to a location by clicking the “Create Location” button in the scan menu. If the Wi-Fi adapter’s default location is set as “default”, it will check all location settings when the Wi-Fi adapter is enabled, and choose the first location “match” it finds.

ADVANCED NETWORK SETTINGS

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

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

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

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