APÉNDICE ACCESS 4.0

FIRMWARE

Apéndice ACCESS 4.0 Firmware

El manual ACCESS describe las operaciones del firmware 3.x. Firmware 4.x agrega significantes mejoras y cambia el comportamiento "base" del producto en muchas maneras. Este apéndice describe estos cambios.

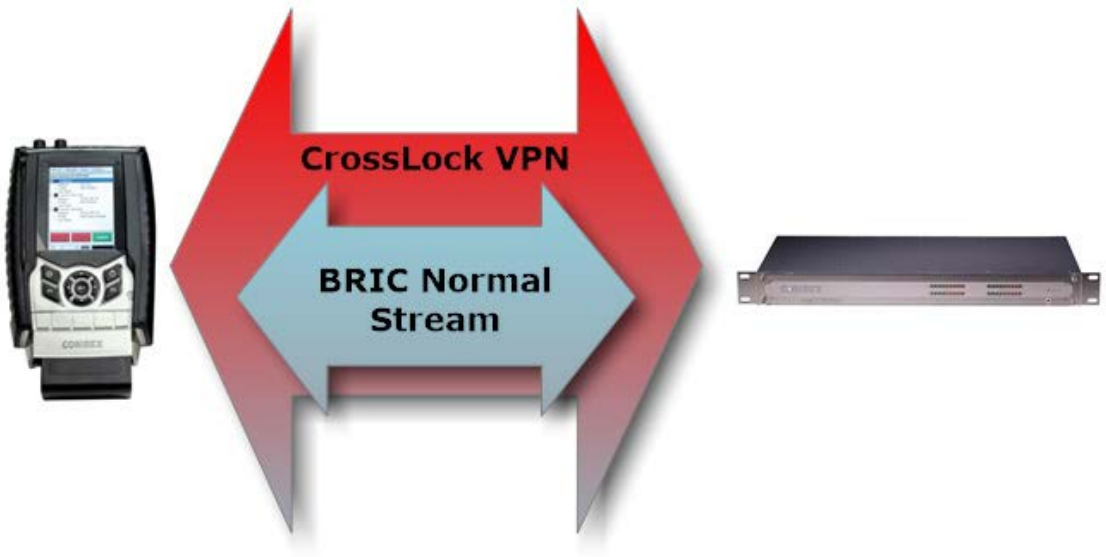
INTRODUCCIÓN:

Si estas familiarizado con Access 3.0 firmware o si actualizó ACCESS de un firmware anterior a 4.0 o más, aquí están las diferencias importantes:

1. **CrossLock** – Esto es una nueva y confiable opción disponible para la conexión entre dispositivos Comrex que poseen compatible firmware entre sí. CrossLock permite el uso de 2 redes en simultáneo para dar mayor confiabilidad o exactitud.
2. **Switchboard** – Anteriormente llamado "BRIC-TS", este nuevo servidor (herramienta) tiene un rol mayor en realizar las conexiones usando CrossLock. Es altamente confiable, pero no es requisito, para todas conexiones que se realicen con CrossLock.
3. **Ports** [Puertos] – CrossLock realiza conexiones en el puerto UDP 9001. Comúnmente Comrex hace sus conexiones de audio "códec" a través del puerto UDP 9000. Esto podría requerir abrir otros puertos adicionales en los ajustes de su router o en su firewall.
4. **Encoder** [Codificadores] – La versión 4.0 removió la habilidad de elegir varias anticuadas ofertas de distintos decodificadores como HQ1, HQ2 y ULB. Esto se debe a que la existencia de la alta calidad de las opciones de comprensión (familia AAC y Opus) son superiores para uso virtual. El perfil pre-equipado, usado en 4.x (para conexiones que no fueron asignadas a un perfil) ahora es Opus mono (esto es ajustable en la interfaz del usuario). Las conexiones que se realizan para 3.x e inferiores unidades, seguirán funcionando con los codificadores anteriormente mencionados pero estos no estarán disponibles para elegir como perfiles.
5. Previas versiones de firmware usaron puertos TCP 8080 para comandos XML usados para la interfaz web y el **Device Manager** [Administrador de Dispositivos]. Estas conexiones ahora son realizadas por un solo puerto TCP 80 (junto con el resto del tráfico web). En algunos casos, puede que tenga que cambiar la configuración del Administrador de dispositivos para interactuar correctamente con su ACCESS.
6. Usando CrossLock, la memoria intermedia (buffer) del decodificador Jitter (y por lo tanto el end-to-end retardo) es visualmente representada en un gráfico de barras y puede ser manipulado manualmente por medio de un control deslizable en la interfaz del usuario.
7. El modo "Stereo POTS" y "POTS PPP" no son más soportados.

INTRODUCCION A CROSSLOCK:

CrossLock describe una nueva capa de fiabilidad que se establece entre los dispositivos Comrex para la antelación de una conexión. Esta capa toma la forma de una Red Virtual Privada (VPN) entre los dispositivos. El flujo del ACCESS es transportada con esta VPN. Se puede apreciar, a continuación, en la Figura 1.



En adición a transportar el audio, **CrossLock** permite, además, que otra información sea compartida entre los extremos, incluyendo información acerca de la calidad de la red y el ajuste del retardo del otro extremo. Esto proporciona un mejor control del retardo en cualquier extremo del enlace.

Uno o ambos extremos de una conexión **CrossLock** pueden utilizar múltiples interfaces de red. Esto puede tomar la forma de dos conexiones Ethernet o cualquier mezcla de redes cableada e inalámbrica. Un escenario común sería conectar uno o dos modems 3G/4G al ACCESS portable. En caso que una red tenga bajo rendimiento, la mayoría o toda la data será enviada a una red en buen estado. Se muestra en la Figura 2:

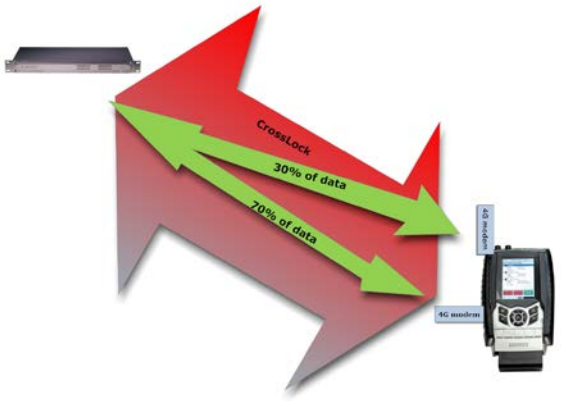


Figura 2.

Por defecto (default), **CrossLock** utilizará cualquier red que ACCESS considere que es capaz de transportar data. Si el retardo aumenta en una de las redes y el paquete se pierde, ACCESS puede decidir si remueve los paquetes de esa red que no está funcionando por completo.

ACCESS puede seguir utilizando esta red para comunicaciones en segundo plano y correcciones de errores.

La configuración de **CrossLock** por defecto (default) es “Bonding”, el cual es lo mejor para la mayoría de usuarios. Este reducirá el posible ancho de banda de las redes disponibles y enviará un solo media stream con un background y correcciones de errores de la información. Un modo alternativo puede ser empleado, conocido como “Redundacy”. En este modo todo el media stream es replicado en cada red (con el background y las correcciones de errores de información). Este modo es preferido solamente en ambientes donde ambas redes tienen gran ancho de banda y corto retardo (como en las redes cableadas). Porque el “Modo Bonding” tiene redundante y rápida capacidad de recuperación por eso se prefiere para las redes inalámbricas.

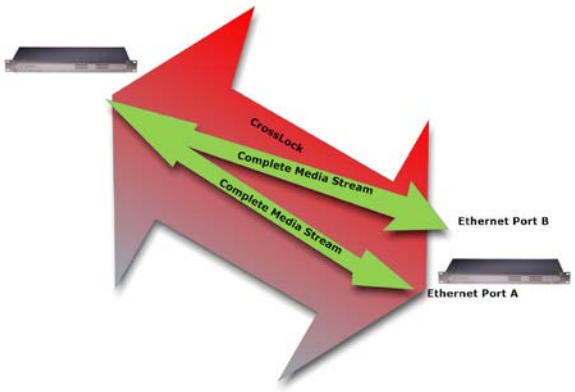


Figura 3.

El uso dual de las redes en ambos extremos del enlace no es soportado cuando al menos un codec es ACCESS portable clasico. El poder de la CPU en ACCESS portable clasico no puede ser soportado.

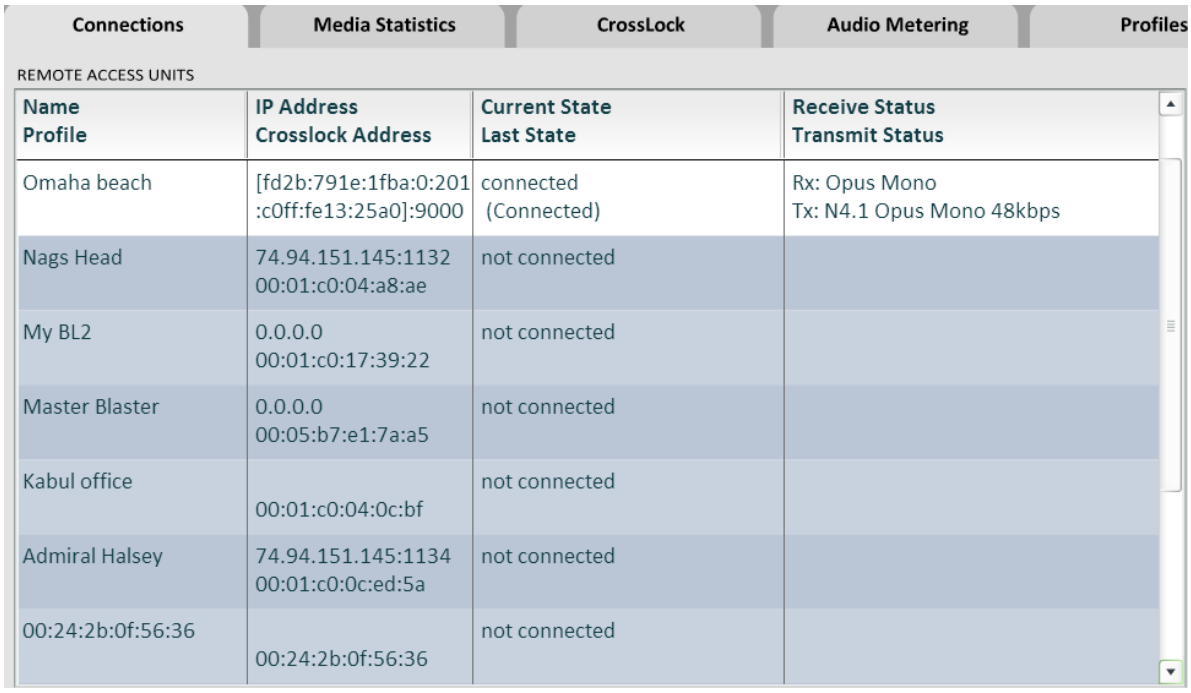
CROSSLOCK & SWITCHBOARD:

Es recomendable que las conexiones CrossLock se realicen en conjunto con el “Switchboard Traversal Server”. Los usuarios ACCESS pueden obtener una cuenta Switchboard para sus decodecs contactando a Comrex. Para la configuración y operación de “Switchboard Server” para ACCES, véase la “technote” en el website de Comrex.

Switchboard es útil, especialmente cuando se utiliza CrossLock porque las unidades ACCESS necesitan más información acerca de sus compañeros de conexión que las conexiones que se realizan sin CrossLock. Adicionalmente, a la direcciones IP de destino, cada conexión CrossLock requiere que cada ACCESS conozca el ID de la unidad del otro. Esto es requerido como una función de seguridad desde que CrossLock establece una VPN entre unidades. La Unit ID de un códec ACCESS es usualmente la Ethernet MAC Adress del códec.

Cuando se realizan conexiones vía Switchboard, la dirección IP y la Unit ID es transferida automáticamente entre los codecs y no es necesario ingresarla al iniciar el codec.

Switchboard lleva una “lista de amigos” de la flota en cada ACCESS o BRIC-Enlace. Esta lista aparece en la pestaña de Conexiones de ACCESS; tanto en la interfaz de usuario basada en la Web y (en el caso de ACCESS portable) en la pantalla.



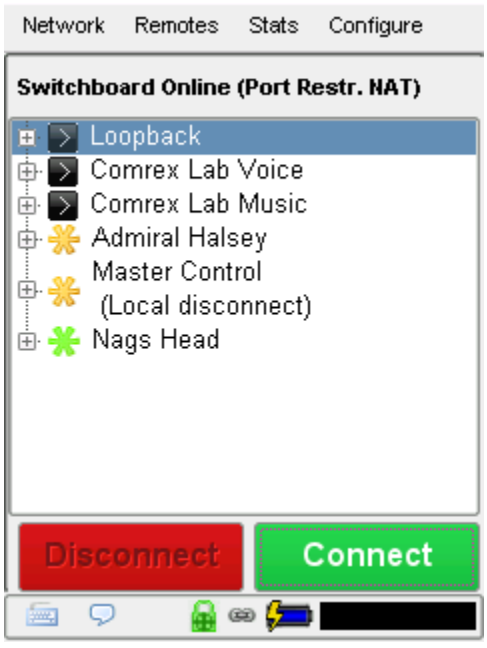


Figura 4.

En ACCESS Portable, las conexiones tienen un color con un códec de engranaje para indicar el estatus de cada otra conexión ACCESS o BRIC-Enlace en la flota. Los ítems con un engranaje color verde están listos para la conexión, amarillo significa ocupado y el rojo significa off-line.

REALIZANDO CONEXIONES CROSSLOCK VIA SWITCHBOARD:

No existe diferencia en realizar conexiones Switchboard vía CrossLock y vía no CrossLock. Si la conexión es intentada vía Switchboard, lo siguiente es verdadero:

1. El ACCESS o BRIC-Enlace el otro extremo está ejecutando el firmware 4.0 o superior.
2. El puerto CrossLock (UDP 9001) está abierto en el extremo.
3. Cada ACCESS es consciente de la otra Unit ID (Mac Adress). Esto es manejado "detrás de escena" en Switchboard.

Luego, una conexión CrossLock será intentada. Si el puerto 9001 esta bloqueado o si el extremo de la conexión tiene 3.x o inferior firmware, la conexión procederá en el modo comúnmente conocido como "BRIC Normal".

Una conexión CrossLock exitosa es indicada como se muestra en la Figura 5. Tenga en cuenta el icono de "lock" en el banner inferior está iluminado en verde durante una conexión CrossLock exitosa. Ya que CrossLock se estableció antes del flujo de audio y después espera otro tiempo, esto podría quedar verde inclusive cuando un flujo de audio no está activo.

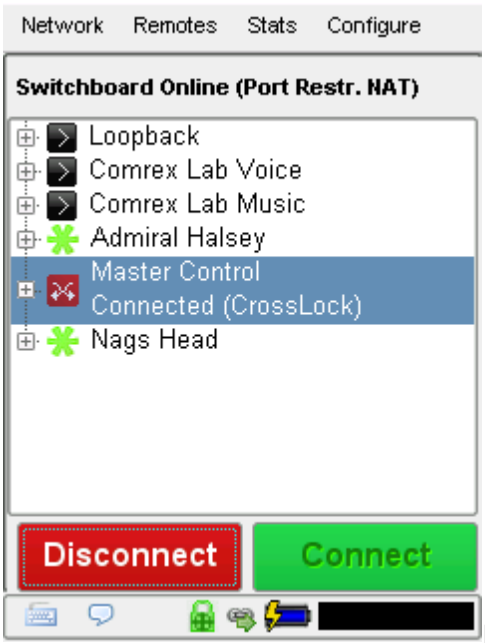


Figura 5.

REALIZAR CONEXIONES SIN CROSSLOCK EN FIRMWARE 4.0

Si a usted le gustaría desactivar el modo CrossLock completamente, puede ser desactivado en el menú del sistema de ajustes.

Debajo de configuraciones -> Sistema de Ajustes -> CrossLock VPN Settings, elija habilitar y deseleccione la opción de habilitar. Conexiones de salida o entrada de CrossLock no serán posibles.

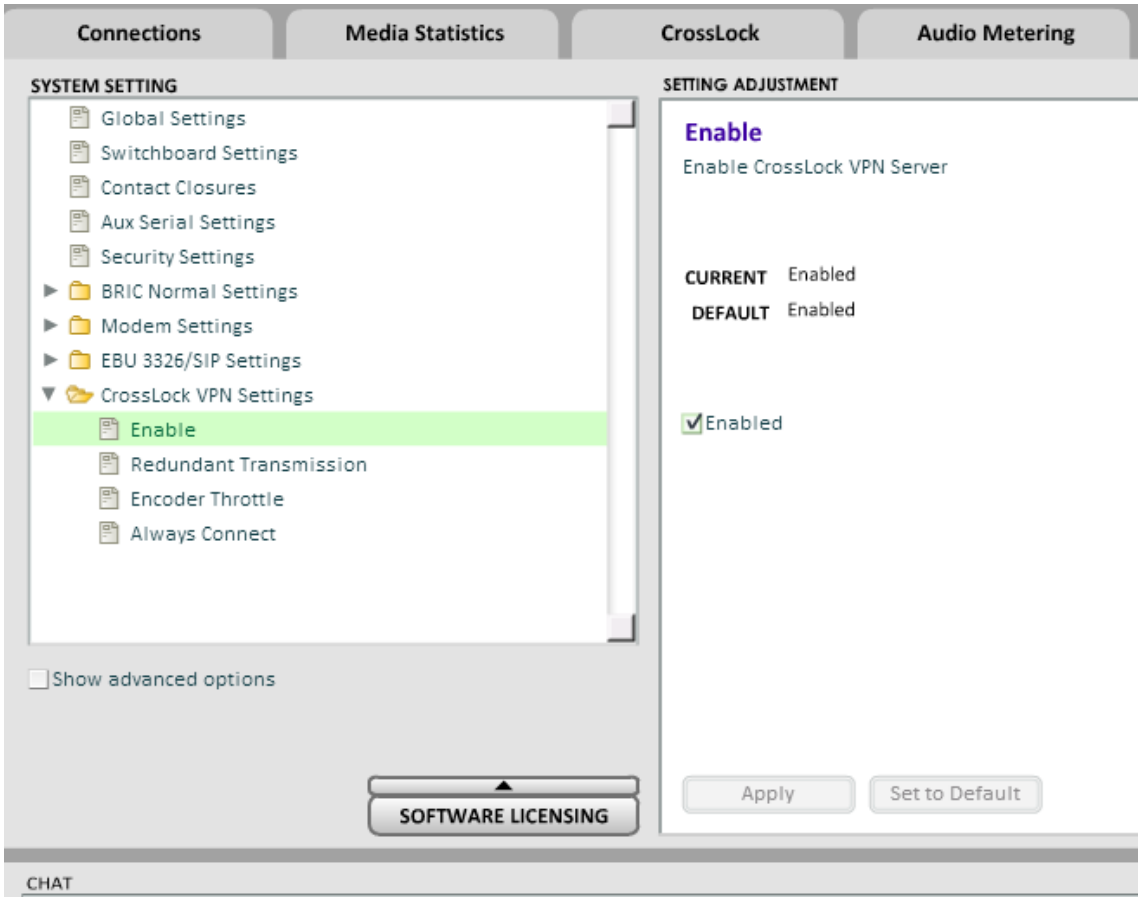
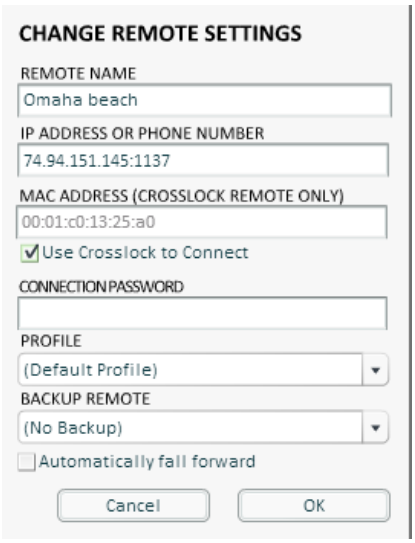


Figura 6.

También es posible desactivar individualmente conexiones CrossLock, debajo de las entradas remotas que aparecen en la lista de Switchboard. Escogiendo “Change Remote Settings” y deseleccionando la opción de CrossLock, esta conexión desactivará CrossLock. Figura 7.



REALIZAR CONEXIONES CROSSLOCK SIN SWITCHBOARD:

En caso de las conexiones no basadas en Switchboard (ej. redes cerradas o STLs) usted necesitará saber la Unit ID (Primary Ethernet Mac adress) de la unidad que usted desea conectarse. Como se muestra en la Figura 8, esto se introduce en el campo "Create New Remote" en el menú emergente en el campo "MAC Address".

Figura 8.

En adición, el codec receptor de la conexión debe tener una entrada similar con la MAC Address de la unidad que llama.

Esto es importante. La unidad receptora debe tener una conexión de salida programada en su libreta de direcciones, que contiene el Unit ID (MAC Address) de la unidad de la cual se llama, inclusive cuando nunca es usada para llamadas salientes.

Una vez que la MAC Address es ingresada en el campo, usted tendrá la opción de deshabilitar o habilitar CrossLock para esta conexión.

ESTADISTICAS DE CROSSLOCK:

Cuando una conexión CrossLock comienza a estar activa, las estadísticas de CrossLock son activadas. Las estadísticas son una herramienta muy poderosa que diagnostica la calidad de las conexiones como también el manejo del retardo de los ajustes durante la conexión.

Las estadísticas CrossLock están disponibles en ACCESS Portable debajo de Stats -> CrossLock Stats [Estadisticas -> CrossLock estadísticas]. En la interfaz web, la pestaña CrossLock comienza a estar activa.

La pestaña CrossLock es similar a la información disponible en la pestaña de Statics, la cual muestra el funcionamiento del flujo de data sin considerar capa de CrossLock.

En adición, la pestaña CrossLock contiene una barra de Retraso “Auto Delay Slider Bar”. Esta barra da indicadores visuales del retraso objetivo (retraso que el sistema piensa es requerido) y el retardo actual del enlace. El ajuste defecto de la barra es operación “automática” pero modo manual puede ser comprometido en situaciones cuando se lo desee.

Como se muestra en la Figura 9 se puede elegir entre ver los gráficos para la transmisión (saliente) o el recibimiento lateral (entrante) del enlace utilizando la opción de “pull down” en la parte superior izquierda.

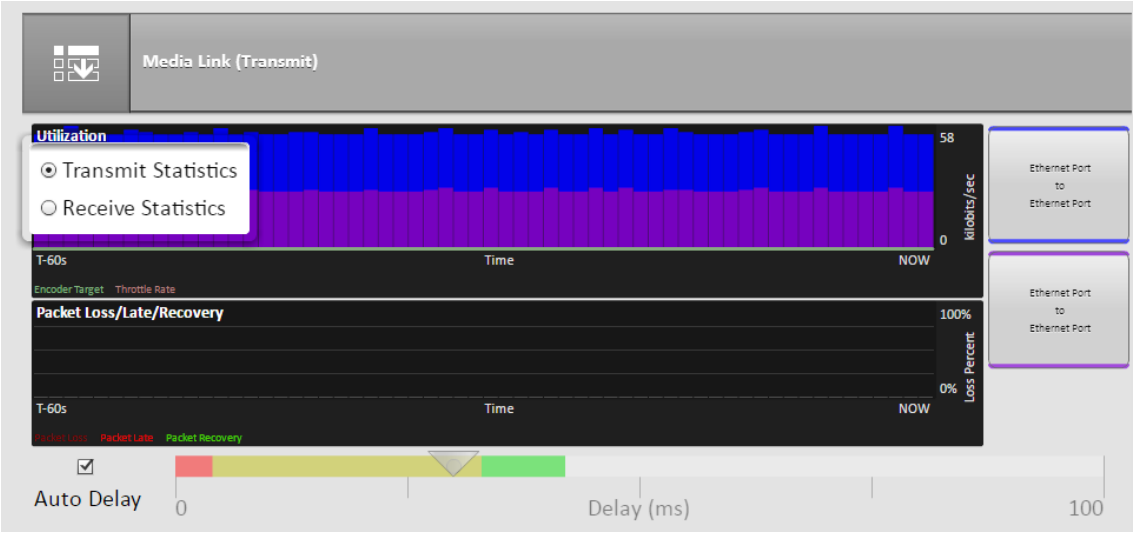


Figura 9.

UTILIZACION DEL GRAFICO

La sección de arriba contiene un gráfico que muestra la utilización saliente o entrante de la red. Las barras indican el promedio de la data que utiliza el sistema durante cada segundo. Se espera que el tamaño de las barras varie porque CrossLock tiene el control sobre la tasa de datos a través de la técnica llamada “Throttling”. Basada en las estadísticas de la red, CrossLock reducirá y aumentará la utilización dinámicamente.

Si más de un equipo está en uso, la utilización de los gráficos estará en distintos colores haciendo referencia al códec, indicando la utilización relativa de cada red. El color correspondiente de cada red aparecerá en el lado derecho del gráfico. En ACCESS Portable, la clave está debajo del gráfico:

Superpuestas en el gráfico de utilización de la red, se pueden ver dos líneas de color:

1. **Encoder target** - Esto refleja la tasa de bits elegida en el perfil utilizado en la conexión. Esta es tratada como un valor máximo, entonces la utilización tendría que permanecer sobre todo debajo de esa línea. Debido a que estos valores se promedian, puede haber momentos en los que la utilización se mueve por encima de la línea de meta pero serán momentáneos.
2. **Throttle rate [Regulador de Tasa]** – Cuando CrossLock throttling está habilitado (estado por defecto) esta línea indica cuanta reducción será aplicada. Usted verá que la utilización se queda mayoritariamente debajo de la línea de reducción.

GRAFICO DE PERDIDA DE PAQUETES

El grafico de abajo indica, en términos de porcentajes, que salió mal en la red durante cada segundo. Tres colores diferentes codificados aparecerán:

1. **Paquete perdido (Rojo oscuro)** – El sistema ha detectado que un paquete se ha caído completamente por la red y que nunca fue recibido por el decoder.
2. **Paquete atrasado (Rojo brillante)** – El sistema recibió el paquete pero fue muy tarde para decodificarlo y reproducirlo.
3. **Paquete recuperado (Verde) –** El paquete se perdió o está atrasado pero fue recuperado por Forward Error Correction (FEC) o Automatic Repeat Query (ARQ) correcciones de errores incorporado en CrossLock.

DELAY SLIDER

La forma más poderosa de estabilizar cualquier conexión de streaming es tener el decoder añadido al retardo de buffer de la conexión. Esto compensa por los cambios en la velocidad de los paquetes que fueron recibidos (conocidos como Jitter). CrossLock usa una combinación del retardo de buffer del decoder y corrección de errores para mantener a las conexiones estables. Cuando CrossLock está activo, la actividad del retardo buffer es ilustrada y controlada via el deslizador del retardo en la pestaña de CrossLock.

Figura 10.

La Figura 10 muestra el deslizador del retardo. En esta figura, el deslizador está en modo “auto retardo” y la información en el deslizador es puramente para usos informativos. Al deshacer la marca en la casilla del modo “auto retardo”, el sistema pasa al modo de “manual retardo” y permite al deslizador ser movido por el ratón (mouse).

El deslizador tiene una escala, y el rango de izquierda a derecha puede variar desde 100 mil milisegundos a varios segundos dependiendo del rango de retardos que se están dirigiendo actualmente. En cualquiera de ambos modos (Auto o Manual), una serie de barras cubrirán el deslizador que significaran las “zonas” de seguridad del retardo.

La zona izquierda más alejada (color rojo) es la que indica que el nivel de buffer es muy bajo para una transmisión. La zona amarilla indica que el retardo buffer puede tener problemas de estabilidad y la zona verde indica que el nivel del buffer debería proveer estabilidad. Esta “zona” de escalas incrementan y decaen en tamaño basándose en la historia que experimento el Jitter por CrossLock en la red.

En el modo **"Auto Delay"** [Retardo Automatico] otros dos elementos son de interés. La flecha descendente significa **"Target Delay**", el cual es el mejor valor de compromiso calculado por el sistema para balancear la estabilidad y el retardo. La "burbuja" indica el retardo actual. La burbuja que marca el retardo actual, intentará rastrear con el "Target Delay Arrow" [Indicador Target Delay] pero a veces puede caer fuera de ella. Esto usualmente indica que el sistema está reduciendo o aumentando el buffer activamente.

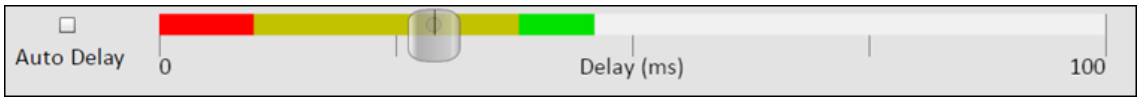


Figura 11.

La figura 11 muestra el deslizador en modo manual. Aquí, la flecha se convierte en el cursor desplazable y le toca al operador determinar la mejor manera de establecer el compromiso entre el retardo y la estabilidad.

Cualquier ajuste realizado en modo manual será eliminado luego de que la actual sesión de CrossLock se termine. En orden para hacer que el retardo buffer cambie permanentemente, utilice los ajustes del administrador de perfil como es detallado en el manual.

VISTA DETALLADA DE LA PESTAÑA CROSSLOCK:

Una poderosa característica de la pestaña de CrossLock es que le permite al usuario examinar profundamente las estadísticas de cada interfaz de cada red y mirar el funcionamiento de esa red solamente. Al cliquear el botón que aparece en cada interfaz en el lado derecho de la pestaña, una nueva ventana se abre mostrando un gráfico similar al grafico resumen pero este estará reducido al funcionamiento de la particular red.

La **"Detailed View"** [Vista Detallada] es útil cuando más de una red está siendo usada por CrossLock, ya que permite la comparación de la calidad y el retardo que figura en las distintas redes. Como en el grafico resumen, una opción está disponible en el menú despegable para seleccionar entre transmitir data (saliente) y recibir data (entrante) para cada red.

Debido a los recursos de la CPU, vista detalla esta solamente disponible en la interfaz web de usuario.

BONDING vs. REDUNDANT EN CROSSLOCK:

Cuando se utiliza CrossLock con múltiples redes, el sistema se pondrá por defecto en Bonding Mode, el cual resume la capacidad de la data de cada red en conjunto y determina la asignación adecuada de los datos entre ellas. Este modo es el mejor para redes inalámbricas o cualquier otra con posibles problemas de congestión. Debido a la asignación de data dinámica, una red puede desaparecer completamente con la mínima corrupción de audio.

Para usuarios en donde la congestión no sea un problema en la red y la seguridad es alta, "Redundant Mode" [Modo Redundante] puede ser la mejor opción. En este modo, el canal completo de audio es distribuido en cada red. Paquetes Redundantes se descartan en el decoder. Mientras que este modo usa más ancho de banda, resulta en menos interrupciones si una red se pierde totalmente.

Para cambiar **CrossLock** desde "Redundant Mode" a "Bonding Mode", diríjase a **Systems Settings -> CrossLock VPN Settings** y elija **"Redundant Transmission".**

AJUSTES AVANZADOS DE CROSSLOCK:

Seleccionando la opción "Advance", en la configuración CrossLockVPN se revela los siguientes ajustes avanzados de CrossLock:

Puerto UPD – Por defecto, CrossLock usa puerto UPD 9001 para las conexiones. Para mejores resultados este puerto debería estar abierto para data entrante o al menos en uno de los decoder en el enlace. Esto significa que al menos que ACCESS es una apertura a las conexiones de Internet (sin dar uso a firewalls o routers) el puerto necesitará ser renviado a este. En instancias en donde más de un decodec será sujeto a la misma IP pública, puede que usted tenga que cambiar el puerto de entrada. Puede ser cambiado aquí. Si este puerto es cambiado y Switchboard es utilizado para establecer conexiones, no se necesitaran cambios en el futuro. En casos de conexiones sin Switchboard, el cambio de puerto necesitará ser observado en la dirección de salida de la unidad de llamada.

Permissive [Permisivo] – Al utilizar "Modo Permissive" se remueve el filtro de la Unit ID completamente. Las conexiones CrossLock pueden ser realizadas sin tener en cuenta la ID de la unidad. Tenga en cuenta que la unidad del extremo debe conocer la ID de la unidad de este códec o también debe tener el "Modo Permissive" disponible. Recomendable para redes cerradas sin preocupaciones por seguridad.

Authenticity [Autenticidad] – ACCES firmware 4.0 o superior utiliza certificados de seguridad asignados al decodec hardware para autenticar como producto Comrex. Esta opción determina si se realizan las conexiones a los codecs sin estos certificados. Los certificados se asignan a los codecs por el servidor de Switchboard después de una actualización de firmware a 4.0 o superior (la actualización del Switchboard no es necesaria). Debido a que algunos codecs pueden ser firewalled y no recibieron certificados después de las actualizaciones, esta opción está descartada.

Encryption / Protection [Encriptación/Protección] – CrossLock tiene la habilidad de prevenir la intercepción de streams (codificación) y la alteración de los mismos (protección). Los requisitos de la CPU en esos modos son grandes y por lo tanto no es recomendable aplicar estas opciones a los streams que no los requieren. Están desactivados de forma predeterminada para conservar la CPU.

Maximum Delay [Máximo Retardo] **–** CrossLock opera por eligiendo la figura de "Target Retardo" basado en la performance de jitter en sus distintas redes a través de una ventana de tiempo. Para prever el retardo excesivo en caso de una red extremadamente extensa, tiene un ajuste de máximo retardo aquí. En caso de que múltiples redes con figuras jitter muy altas, este ajuste puede ser aumentado desde el predeterminado de cinco segundos por el usuario.

FEC – CrossLock tiene un poderoso algoritmo de posibles correcciones de errores que se activa en la presencia de múltiples redes usando cualquier exceso de banda ancha para añadir en la igualdad requerida. El uso de FEC es recomendado, pero puede ser inhabilitado aquí.

FEC Delay [Retardo FEC] – En ambos controles la cantidad de retardo es introducido en el sistema por FEC y también para ver hasta qué punto es efectiva la recuperación (la cual es dependiente en gran medida de la tasa de paquetes). La condición estándar de 100mS puede ser alterada solamente cuando lo recomienda el apoyo de Comrex.

Base FEC – Este parámetro se aplica una tasa constante de FEC focalización recuperación de la tasa de pérdida esperada especificada. Se mide en porcentaje de paquetes perdidos para ser corregida. Esto es útil cuando las retransmisiones no son efectivas (e.j red con gran retardo) y auto-FEC no está trabajando como es deseado. Debería ser usado en recomendación del apoyo de Comrex.

Retransmit [Retransmitir] - En adición a FCE, CrossLock utiliza un logaritmo estilo ARQ para permitir la retransmisión de los paquetes perdidos cuando el tiempo lo permita. Este modo puede ser inhabilitado aquí.

Header Compression [Compresion Header] **–** La naturaleza de los paquetes de internet algunas veces resulta en un IP saturada (RTP headers y otra información) actualmente usando casi el mismo ancho de banda como el contratado. CrossLock, por defecto, comprime alguno de estos headers para conservar el ancho de banda. En instancias en donde la red rechaza esto, o la inspección del paquete es requerido, esta compresión puede ser deshabilitada.

Always Connected [Siempre conectado] **-** Esta opción provee a CrossLock de estar siempre conectado con el destino. Por esta naturaleza, CrossLock usa muy poca data para que la utilización de la red en este modo (cuando está inactivo) sea muy pequeña. Si usted se conecta solo a un destino, teniendo CrossLock siempre conectado hace que las conexiones de media sean más rápidas y provee una indicación del status de las redes entre equipos (luz "listo" o Crosslock status). La mayoría de los usuarios deben dejar este ajuste apagado.

CAJA DE HERRAMIENTAS FIRMWARE 4.0:

Aparte de la función de CrossLock, firmware 4.0 cuenta con un nuevo gestor de red en ToolBox, al cual se puede acceder desde la interfaz de usuario web o por el software de Device Manager [Administrador de Dispositivos]. Esto permite una fácil configuración de red, especialmente en ACCESS Rack.

USO DE DEVICE MANAGER:

La Figura 12 muestra que cuando firmware 4.0 está funcionando, cinco pestañas aparecen en el panel de la derecha luego de que Device Manager se ha conectado (en vez de las usuales cuatro). La quinta pestaña es nombrada Web Configuration. Esta abrirá simple interfaz de ajustes en ACCESS llamada ToolBox. La interfaz de ToolBox le permite a usted configurar varias opciones incluyendo el puerto Ethernet. Usted necesitará ingresar a ToolBox por separado con un nombre de usuario (cualquiera) y una contraseña (por defecto será **comrex**) para ingresar a ToolBox.

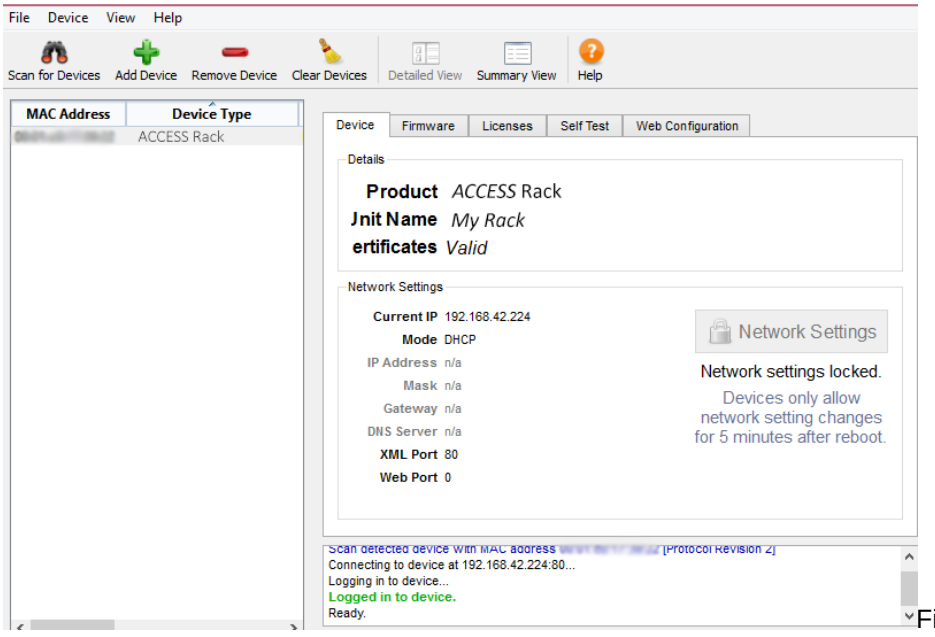
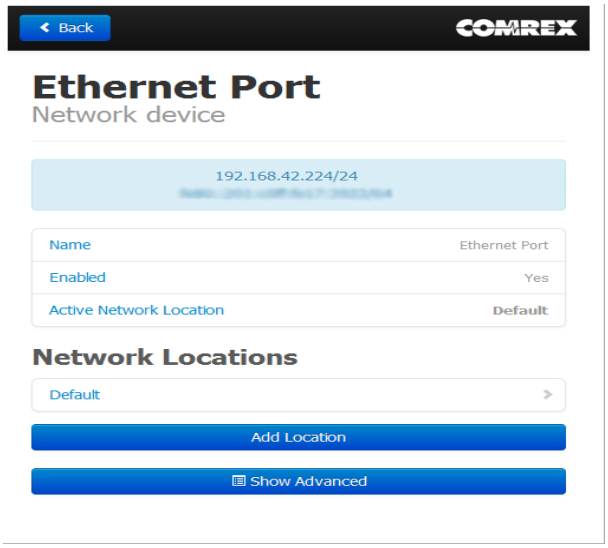


Figura 12.

Una vez que ingreso a ToolBox, elija Network -> Admin -> CrossLock y luego elija Set Up Ethernet. Elija puerto Ethernet que aparece en la lista. La Figura 13 muestra los ajustes de Ethernet en ToolBox. La Figura 13, lo muestra a continuación.



ToolBox también le permite configurar cualquier dispositivo inalámbrico unido a un puerto USB en ACCESS.

USAR TOOLBOX VIA INTERFAZ WEB:

Junto con Device Manager, también se puede acceder a ToolBox directamente a través de la página web integrada via un navegador web. Al acceder a ToolBox, entre la dirección del dispositivo como **<ip_address>/cfg** (e.j. 192.168.0.34/cfg).

NUEVAS CARACTERISTICAS DE NETWORK MANAGER:

Las siguientes nuevas características que se presentan en ambos es la interfaz de usuario de pantalla táctil en ACCESS Portable y ToolBox basado en web.

UBICACION:

ACCESS Firmware 4.0 incluye la habilidad de tener múltiples ubicaciones programadas para distintos ajustes de redes. E.j. si usted está moviendo ACCESS entre distintas ubicaciones y se desea almacenar la estática información IP para cada lugar, usted tendrá que definir una nueva ubicación (dándole un nombre único) usando la opción “Add Location” como se muestra en la Figura 14. Una vez que las múltiples ubicaciones están definidas usted puede cambiar entre ellas usando la opción “Active Location” de la Figura 14. Ubicaciones pueden ser configuradas en cualquier dispositivo de red, incluyendo adaptadores Wi-Fi. Esto puede ser utilizado en la programación de credenciales para uso en múltiples ambientes Wi-Fi.

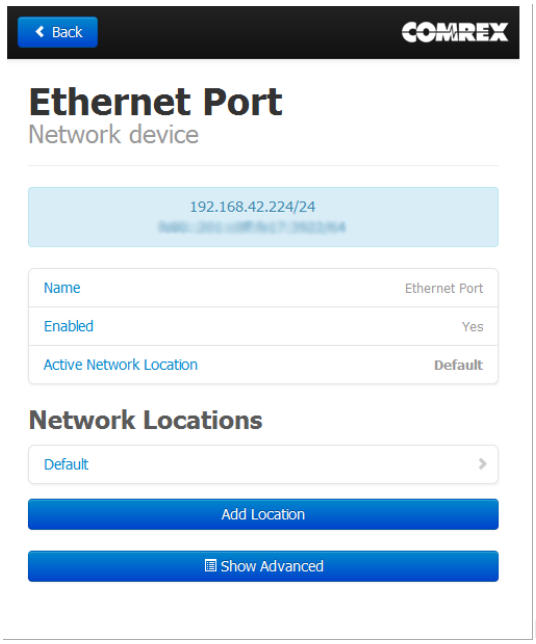


Figura 14.

Cuando se crea la conexión Wi-Fi en firmware 4.0, usted puede escanear por todas las redes Wi-Fi disponibles usando la función “scan” como en el firmware anterior. Pero una vez seleccionado, una red Wi-Fi debe ser aplicada a una ubicación se debe cliquear en “Create Location” en el menú de “Scan”. Si el adaptador Wi-Fi tiene por defecto la localización seleccionada como “defecto”, se comprobará todos los ajustes de ubicación cuando se habilita el adaptador Wi-Fi y elegirá la primera ubicación que coincida.

AJUSTES DE RED AVANZADOS:

Al elegir “Show Advanced” debajo de cualquier red, las siguientes opciones aparecen:

Preserve after Reset [Preservar luego del Reset] – Normalmente, cuando ACCESS se ajusta a los valores predeterminados de fábrica (via **Device Manager**), todos los ajustes de la red (incluyendo el principal Ethernet) son eliminados. Al cambiar esta opción a “si”, los ajustes de esta red se conservarán después de restablecimiento de fábrica. Se debe tener precaución, ya que es posible "quedarse afuera/excluirse" de ACCESS al ajustar los parámetros incorrectamente de Ethernet.

Use of CrossLock [Uso de CrossLock] – Normalmente activada, esta opción le permite especificar que este puerto no será considerado como parte de la conexión de CrossLock. Esto puede tener valor cuando se utiliza un puerto para razones de control solamente y un puerto secundario para CrossLock media.

Broadcast Config [Configuración de Broadcast] – Normalmente activado, esta opción instruye a ACCESS a no responder a la función “scan” usada por Deviced Manager. Precaución, sin la función de “scan”, “Network Recovery Mode” está inhabilitado.