9992-ENC
9992-ENC-4K-HEVC
Software Defined Broadcast Encoder

Product Manual
Version 1.2.0

9992-ENC-OM
Version 1.2.0

9992-ENC • Software Defined Broadcast Encoder Product Manual

- Cobalt Digital Inc. Part Number: **9992-ENC**

- Document Version: **1.2**

- Printed in the United States.

- Last Author: CAN

- Printing Date: 2023

The information contained in this manual is subject to change without notice or obligation.

Copyright

Notice

The material in this manual is furnished for informational use only. It is subject to change without notice and should not be construed as a commitment by Cobalt Digital Inc. Cobalt Digital Inc. assumes no responsibility or liability for errors or inaccuracies that may appear in this manual.

Trademarks

- openGear is a registered trademark of Ross Video Limited.

- COBALT is a registered trademark of Cobalt Digital Inc.

- DashBoard Control System™ is a trademark of Ross Video Limited.

All other product names and any registered and unregistered trademarks mentioned in this manual are used for identification purposes only and remain the exclusive property of their respective owners.

Important Regulatory and Safety Notices

Before using this product and any associated equipment, refer to the "**Important Safety Instructions**" listed below to avoid personnel injury and to prevent product damage.

Products may require specific equipment, and/or installation procedures to be carried out to satisfy certain regulatory compliance requirements. Notices have been included in this publication to call attention to these specific requirements.

Symbol Meanings

This symbol on the equipment refers you to important operating and maintenance (servicing) instructions within the Product Manual Documentation. Failure to heed this information may present a major risk of damage or injury to persons or equipment.

Warning — *The symbol with the word "**Warning**" within the equipment manual indicates a potentially hazardous situation, which, if not avoided, could result in death or serious injury.*

Caution — *The symbol with the word "**Caution**" within the equipment manual indicates a potentially hazardous situation, which, if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices.*

Notice — *The symbol with the word "**Notice**" within the equipment manual indicates a situation, which if not avoided, may result in major or minor equipment damage or a situation, which could place the equipment in a non-compliant operating state.*

ESD Susceptibility — *This symbol is used to alert the user that an electrical or electronic device or assembly is susceptible to damage from an ESD event.*

Important Safety Instructions

Caution — *This product is intended to be a component product of an 8300 series frame. Refer to the frame User Manual for important safety instructions regarding the proper installation and safe operation of the frame as well as its component products.*

Warning — *Certain parts of this equipment, namely the power supply area still present a safety hazard, with the power switch in the OFF position. To avoid electrical shock, disconnect all A/C power cards from the chassis' rear appliance connectors before servicing this area.*

Maintenance/User Serviceable Parts

Routine maintenance to this Cobalt Digital Inc. product is not required. This product contains no user serviceable parts. If the frame does not appear to be working properly, please contact Technical Support using the numbers listed under the "Contact Us" section on the last page of this manual. All Cobalt Digital Inc. products are covered by a generous 5-year warranty and will be repaired without charge for materials or labor within this period. See the "Warranty and Repair Policy" section in this manual for details.

Environmental Information

The equipment that you purchased required the extraction and use of natural resources for its production. It may contain hazardous substances that could impact health and the environment.

To avoid the potential release of those substances into the environment and to diminish the need for the extraction of natural resources, Cobalt Digital Inc. encourages you to use the appropriate take-back systems. These systems will reuse or recycle most of the materials from your end-of-life equipment in an environmentally friendly and health-conscious manner.

The crossed-out wheeled bin symbol invites you to use these systems.
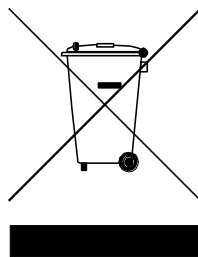
If you need more information on the collection, reuse, and recycling systems, please contact your local or regional waste administration.

You can also contact Cobalt Digital Inc. for more information on the environmental performance of our products.

Contents

Introduction

This manual covers the **9992-ENC** and the **9992-ENC-4K-HEVC Software Defined Broadcast Encoders**. These are multi-channel broadcast-grade encoders designed to meet the most stringent requirements for today's broadcasters. Our HEVC video encoding technology provides a dramatic compression efficiency improvement over previous video compression standards, while also supporting MPEG-2 and MPEG-4 AVC. The 9992-ENC is an industry standard openGear® card and provides an ideal platform for transitioning to state-of-the-art encoding capabilities.

Features:

- **Future-Proof** — Software-defined architecture supports video compression using MPEG-2 (H.262), MPEG-4 AVC (H.264) and HEVC (H.265).
- **Industry Standard Form-Factor** — The 9992-ENC is offered in the industry-standard openGear format and is compatible with existing deployed openGear frames.
- **High Density** — Supports up to four independent 1080p60 input signals, or a single UHD 4Kp60 input signal. One openGear frame can support up to 10 cards, for a total of 40 HD or 10 UHD 4K channels.
- **Full Audio Support** — The 9992-ENC supports MPEG-1 Layer II, AAC-LC, HE-AAC, LPCM (SMPTE-302M) and Dolby AC-3/EAC-3 (optional license). "Credits-based" audio processing allows flexible audio resource allocation.

9992-ENC Base Unit Features:

- Support for one encode channel up to 1080p60
- Support for MPEG-2 (H.262) and MPEG-4 AVC (H.264)
- Support for 4:2:0 8-bit/10-bit encoding
- Full ancillary data support
- Support for 2 stereo pairs (4 audio channels) in any combination of MPEG-1 Layer II, AAC-LC, and HE-AAC (v1/v2) modes
- Output options: UDP, RTP, HLS and RTMP[1]
- Remote control/monitoring via Dashboard™ software
- Five-year warranty

9992-ENC-4K-HEVC Base Unit Features:

- Support for one 4K encode channel or four encode channels up to 1080p60
- Support for MPEG-2 (H.262), MPEG-4 AVC (H.264), and HEVC (H.265)
- Support for 4:2:0 8-bit/10-bit encoding
- Full ancillary data support
- Support for 8 stereo pairs (16 audio channels) in any combination of MPEG-1 Layer II, AAC-LC, and HE-AAC (v1/v2) modes
- Output options: UDP, RTP, HLS and RTMP[1]
- Remote control/monitoring via Dashboard™ software
- Five-year warranty

---

[1] RTMP is available for AVC (H.264) only due to protocol limitations.

Optional Licenses:

- **+AVC^2** Additional 1080p60 encoder channel with MPEG-2 and MPEG-4 AVC (up to three additional channels, for a total of four channels per unit). Each license includes two +MP1L2-AAC licenses.
- **+HEVC^2** Enables HEVC encoding (per channel; up to four +HEVC licenses may be applied to a single unit).
- **+4K^2** Enables 4K encoding. (Requires all four encoding engines are licensed.)
- **+MP1L2-AAC** Adds one MPEG-1 Layer II, AAC-LC, or HE-AAC audio encoding pair. Three licenses can be combined to allow one 5.1 AAC-LC or HE-AAC surround encode. The encoder can have a maximum of 16 licenses (32 channels).
- **+ENCD-2.0** Adds one Dolby Digital/Dolby Digital Plus stereo audio encoding license.
- **+ENCD-5.1** Adds one Dolby Digital/Dolby Digital Plus 5.1 Surround Sound audio encoding license. This license can also be used to encode a Dolby stereo pair.
- **+RIST/ARQ-ENC** Adds RIST support (per unit)
- **+RIST/ENCRP-ENC Adds** RIST Main Profile encryption and authentication (per unit). Requires the +RIST/ARQ-ENC license to be present.
- **+SRT** Adds SRT support (per unit)
- **+SMPTE2022** Adds SMPTE-2022 support (per unit)
- **+422** Adds 4:2:2 encoding support license (per unit)

Rear I/O Modules:

- RM20-9992-ENC-B-HDBNC 20-Slot Frame Rear I/O Module (Standard-Width)
- (2) 12G/6G/3G/HD-SD-SDI Coaxial Inputs
- (2) 3G/HD/SD-SDI Coaxial Inputs
- (2) ASI Coaxial Outputs
- (2) GigE Ethernet Media Ports
- GPIO Port

(All SDI coaxial connectors HD-BNC.)

Note: Mates to card in odd slot.

---

^{2} Applicable only to the 9992-ENC.

Product Overview

Video Encoding

Encoding Standards:
- MPEG-2 (H.262)
- MPEG-4 AVC (H.264)
- HEVC (H.265)
- Support for up to four independent 1080p60 encode sessions (All encode sessions must use the same standard; mixed-standard encoding is not supported.)
- Support for UHD encoding in AVC and HEVC modes (Maximum resolution 4096x2160p60)
- Maximum bit rates:
  - UHD (4K) encoding: 150 Mb/s
  - HD encoding: 40 Mb/s (The first HD channel can be as high as 150 Mb/s.)
- Support for 4:2:0 and 4:2:2 color spaces in all modes
- Support for 8-bit / 10-bit encoding in all modes
- Full control of GOP size and structure. Advanced compression controls available.

Audio Encoding

Encoding Standards:
- MPEG-1 Layer II
- AAC-LC
- HE-AAC (v1/v2)
- Dolby AC-3
- Dolby EAC-3
- LPCM (SMPTE-302M)
- Dolby AC-3/EAC-3 pass-through support
  (5.1-Surround encoding available for AAC-LC, HE-AAC, Dolby AC-3 and Dolby EAC-3; subject to licensing)

Maximum number of channels supported (subject to licensing):
- MPEG-1 Layer II: 16 stereo pairs (32 audio channels)
- Dolby AC-3: 16 stereo pairs (32 audio channels)
- Dolby EAC-3: 8 stereo pairs (16 audio channels)
- AAC-LC: 8 stereo pairs (16 audio channels)
- HE-AAC (v1/v2): 8 stereo pairs (16 audio channels)

Ancillary Data Support

- Closed-Captioning: SMPTE-334M (EIA-608 and EIA-708 supported), Line 21 (SD sources)
- AFD: SMPTE-2016, Line 20/22 WSS (SD sources)
- SCTE-104 to SCTE-35 conversion
- SMPTE-2038 generic ancillary data transport (timecode, KLV, etc.)
- SMPTE-2108 HDR metadata

Inputs

- (2) 75Ω SDI inputs each supporting 12G-SDI, 6G-SDI, 3G-SDI, HD-SDI and SD-SDI
- (2) 75Ω SDI inputs each supporting 3G-SDI, HD-SDI and SD-SDI
- Support for all standard frame rates (interlaced and progressive):
  23.98, 24, 25, 29.97, 30, 50, 59.94, 60
  Note: Although two 12G/3G/HD/SD-SDI inputs are present, only one input can be used at a time to route to the maximum-available single UHD encoder engine.
  Note: UHD encode (single UHD/HD encoder) available only on 9992-ENC-4K-HEVC or 9992-ENC with a +4K license upgrade. In UHD mode, the other three HD encoder channels are not available.

Outputs

- (2) DVB-ASI outputs
- (2) Gigabit Ethernet ports for IP output, supporting the following protocols:
  - UDP unicast/multicast
  - RTP unicast/multicast with optional SMPTE-2022 FEC
  - HTTP Live Streaming (local or remote server)
  - RTMP (limited to H.264 only)
  - RIST
  - SRT
- Integrated multiplexer creates MPTS over IP or over DVB-ASI
- Support for DVB table generation

Encoder Block Diagram
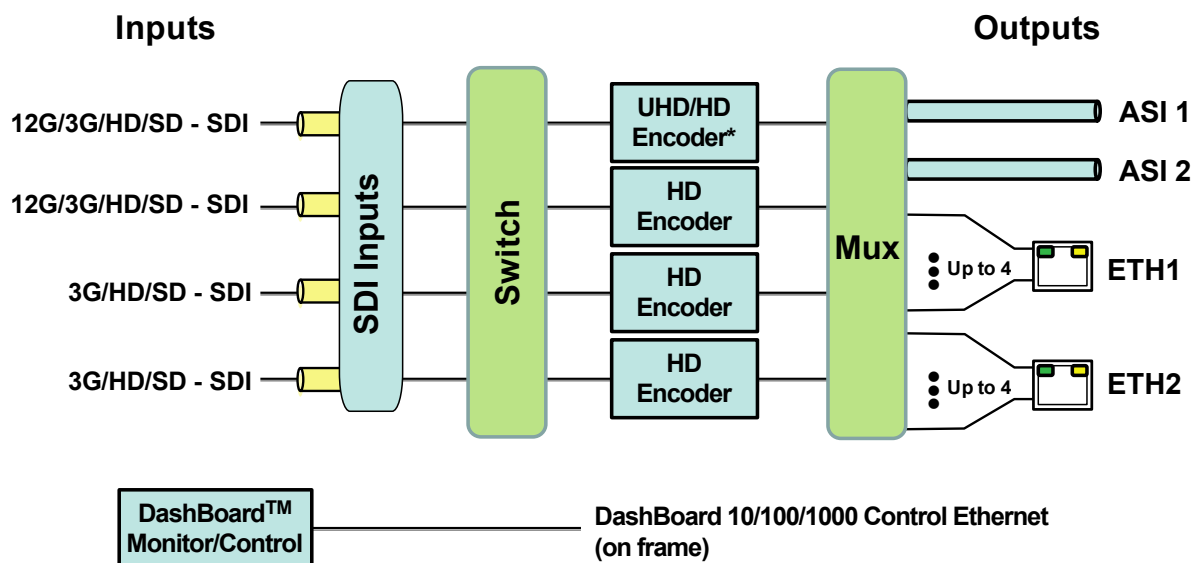
* In UHD mode, the other three HD Encoders are not available.

For the remainder of this manual, the term *port* for a physical input/output port (such as ASI or Ethernet), and *stream* for a transport stream present in the port. ASI ports support only one stream. Ethernet ports support multiple streams.

Indicators and Switches

The 9992-ENC card and its rear module are intended for installation only in 20-slot openGear® frames such as the 20-slot OG3-FR frame or the Cobalt HPF-9000 frame. Prior to installing the card, first install the corresponding rear panel I/O module.

Rear I/O Panel Indicators

The 9992-ENC rear I/O panel is depicted below. It includes the following:

- Eight HD-BNC connectors, organized as follows:
  - Connectors 1 and 2 support SD-SDI, HD-SDI, 3G-SDI, 6G-SDI and 12G-SDI signals. They correspond to Video 1 and Video 2 inputs in the GUI.
  - Connectors 6 and 8 support SD-SDI, HD-SDI and 3G-SDI signals. They correspond to Video 3 and Video 4 inputs in the GUI.
  - The remaining connectors are unused.
- Two ASI output ports on standard BNC connectors.
- Two 10/100/1000 Mb/s Ethernet ports on standard RJ-45 connectors.
- A GPIO block (currently unused)

Each of the video inputs has a green indicator LED, with the following states:
- **LED off:** no video signal detected, or input not configured.
- **LED ON:** video input locked to the video signal.

Each of the ASI output ports has a green indicator LED, with the following states:
- **LED off:** ASI output port is disabled.
- **LED ON:** ASI output port is configured and enabled.

Each of the Gigabit Ethernet ports has two indicator LEDs, with the following states:
- Green LED:
  - **Off:** No link
  - **On:** Link
- Yellow LED:
  - **Off:** No activity (transmit and/or receive)
  - **On:** Port is currently transmitting and/or receiving
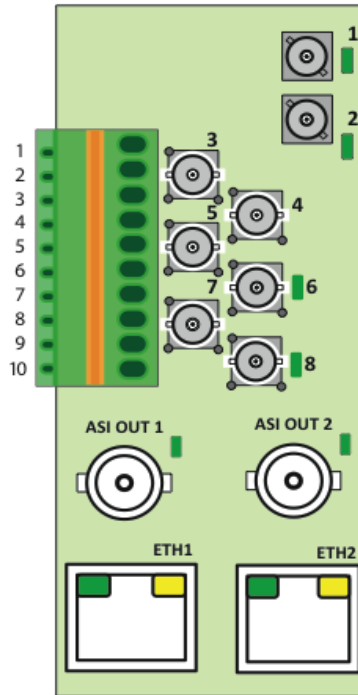
Front Indicators

A similar set of indicators exist in the front of the board. These are visible when the frame front door is opened. The indicator layout is depicted below.

The LED indicators are as follows:

- **PWR LED:** indicates that the power received from the frame is OK.
  - **Green:** power OK
  - **Off:** no power (or insufficient voltage – check the frame power status)
- **Status LED:** indicates the overall status of the board.
  - **STAT1:** is Green no active alarm
  - **STAT2:** is Red at least one critical alarm present
- **REF and DMOD:** are unused at this time.
- **SDI 1, SDI 2, SDI 3, and SDI 4 LEDs:** these behave the same as the corresponding rear I/O panel indicators.
- **AS1 1 and ASI 2 LEDs:** these behave the same as the corresponding rear I/O panel indicators.
- **ETH1 and ETH2 LEDs:** these indicate the status of the corresponding Ethernet connection.
  - **Off:** no link
  - **On:** link OK, port is transmitting and/or receiving packets

```
            Top Corner

     PWR     ○
     STAT1   ○
     STAT2   ●
     REF     ○
     DMOD    ○
     SDI 1   ○
     SDI 2   ○
     SDI 3   ○
     SDI 4   ○
     ASI 1   ○
     ASI 2   ○
     ETH 1   ○
     ETH 2   ○


              RESET   [●]


              SAFE BOOT  [●]      SDMMCBOOT  [●]
```
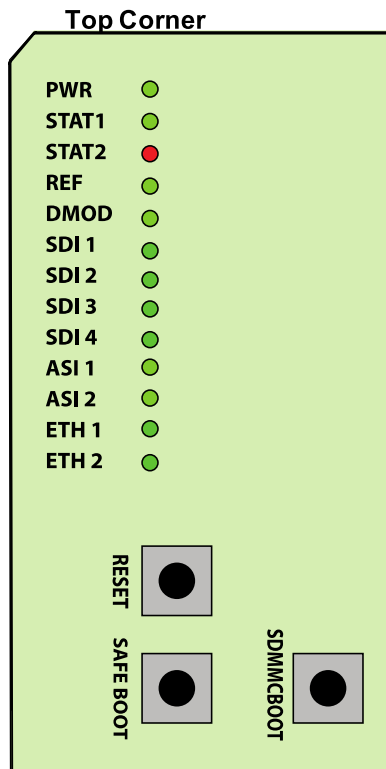
The 9992-ENC board has other LEDs that may or may not be illuminated. They are intended for engineering debug only.

Front Switches

The 9992-ENC has three pushbutton-type switches in the front, just below the LEDs, as depicted below. Their operation is as follows:

- **Reset Switch:** Pressing this pushbutton switch causes the card to reset.
- **Safe Boot:** This switch is used to recover the board in the unlikely case of a corrupted or broken firmware update. In most cases, the 9992-ENC will detect the error and automatically fall back into the factory-default firmware load. If it does not, pull the card out, press and hold this switch, and push the card back into the frame while still holding the switch. You can release the switch once the green and red Status LEDs light up simultaneously. This action causes the card to revert to the factory-default firmware and remove the persistent configuration.
- **SDMMC BOOT:** DO NOT USE. For engineering use only.

16

9992-ENC Operation and Management

The 9992-ENC is configured using the free Dashboard™ application, which is available for Windows, Apple OS X, and Linux. The graphic user interface (GUI) for the 9992-ENC is described in detail. As with any openGear™ card, it is divided into a **Statistics** panel on the left, and a **Configuration** panel on the right. Each panel has multiple tabs, corresponding to the various functions in the card. The **Card State** indicator in the **Status LEDS** area mirrors the **STAT1/STAT2** LEDs in the front of the card. If this indicator is green or yellow, the green **STAT1** LED will be lit; if this indicator is red, the red **STAT2** LED will be lit.
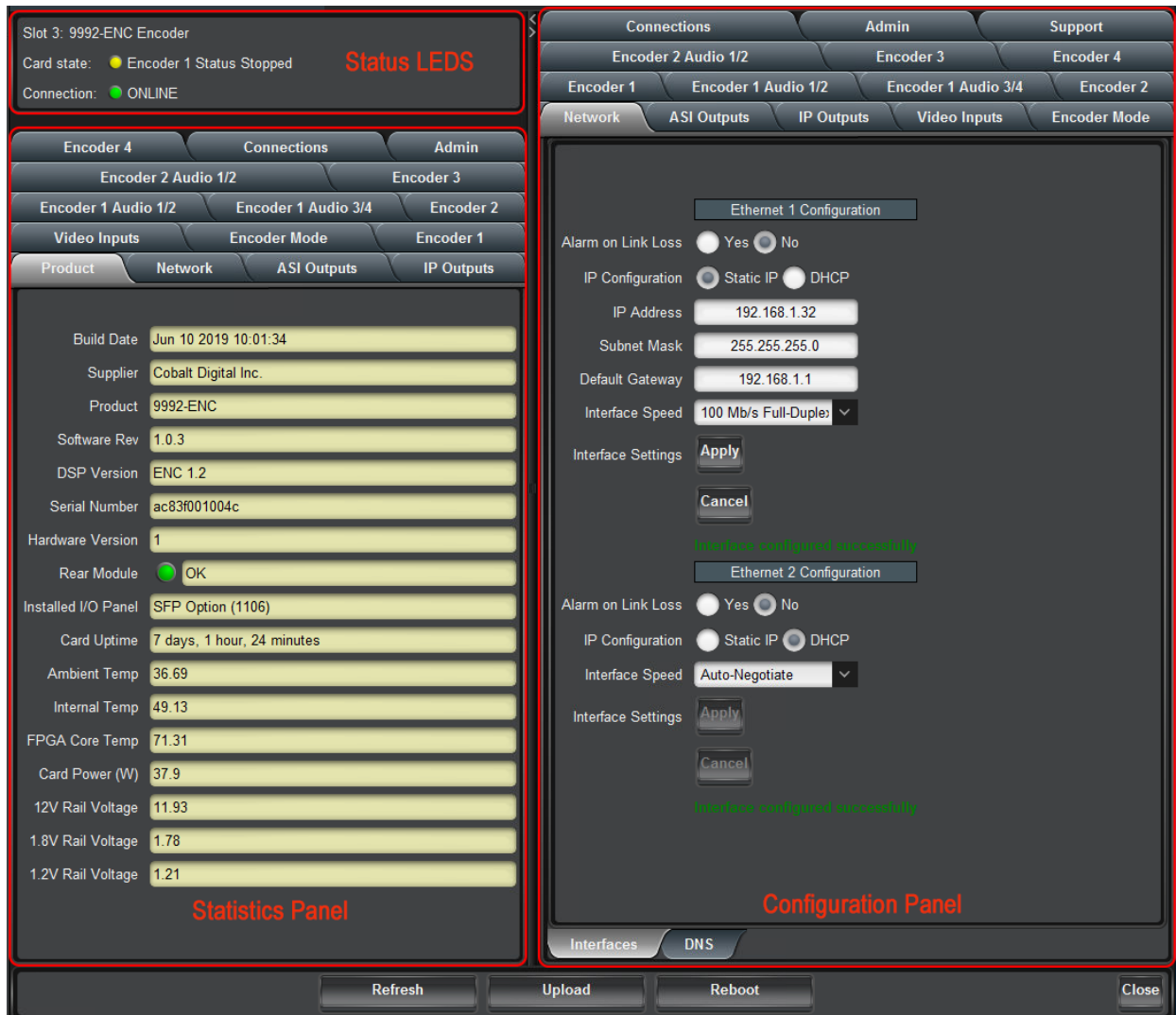
The following Statistics and Configuration panel tabs are available:
- **Product:** this tab provides general information on the card, including firmware version, uptime, temperatures, and other parameters. It appears <u>only</u> on the Statistics panel.
- **Network:** this tab is used to configure the IP addresses and network information for the Ethernet ports. The statistics side of the panel includes some additional information such as link state.

- **ASI Outputs:** this tab is used to configure/monitor the ASI ports.
- **IP Outputs:** this tab is used to configure/monitor the IP Output ports. The configuration panel provides the facilities to create, manage and delete ports; the statistics panel includes transmission status information.
- **Video Inputs**: this tab provides status information on the video inputs. In the configuration area, it can be used configure some input port parameters.
- **Encoder Mode:** this tab is used to configure some common parameters for all encoding sessions.
- **Encoder 1-4:** these tabs are used to configure the individual settings for each encoder session. Only one tab will be shown if the encoder is in single-channel mode.
- **Encoder X Audio Y/Z:** these tabs are used to configure up to two audio services for a given encoder. The number of such tabs presented is a function of the number of configured audio services.
- **Connections:** this tab is used to configure/monitor connections. The configuration panel provides facilities to create, edit and delete connections; the statistics panel provides a table where the status of all the connections in the unit can be inspected at a glance.
- **Admin:** this tab is used for general administrative functions, such as firmware upgrades, licensing, logs, and configuration management. The Test Packet Generator configuration is also found under this tab.
- **Support:** this tab provides customer support information. It appears <u>only</u> on the Configuration panel.

Product Tab

The Product Tab contains basic information about the 9992-ENC and is only available in the statistics panel.

Product Statistics Tab

The following information is available:
- **Build Date:** Date the firmware image was built.
- **Supplier:** Cobalt Digital Inc.
- **Product:** 9992-ENC[3].
- **Software Rev:** This indicates the firmware revision currently running. The format is Major Version • Minor Version • Build Number.
- **DSP Version:** This indicates the version of the firmware loaded in the device's DSP.
- **Serial Number:** This is the serial number of this particular 9992-ENC card.
- **Hardware Version:** This indicates the version of the encoder hardware.

---

[3] This field will show 9992-ENC even if the device is licensed as a 9992-ENC-4K-HEVC

- **Rear Module:** This indicates the status of the Rear I/O Module. It can have one of the following states:
  - ⬤ **OK**: The Rear Module is the correct module for the 9992-ENC.
  - ⬤ **Not Installed**: The 9992-ENC is not connected to a rear module. The card is operating normally, but it will not be useful as there are no input and output connections to it.
  - ⬤ **Wrong Module:** The 9992-ENC is connected to a rear module that was not designed for it (most likely from another openGear™ vendor). Depending on the signals present on that module, there may be a chance of damage to the 9992-ENC; It is recommended that this situation be rectified immediately. This alarm will cause the front status LED to turn red.
- **Installed I/O Panel:** This indicates what type of I/O panel is installed.
- **Card Uptime:** Indicates how long the card has been running since it was last rebooted.
- **CPU Status:** Summarizes the CPU utilization status. This indicator can have the following states:
  - ⬤ **OK**: CPU utilization is in the normal range.
  - ⬤ **High Load**: The 9992-ENC CPU utilization is between 65% and 75%.
  - ⬤ **High Load:** The 9992-ENC CPU utilization is higher than 75%.

  It is normal to have temporary high CPU loads as the user interacts with the GUI, or during firmware updates. If there is a consistent high load alarm during normal operation, the 9992-ENC may be oversubscribed and configuration changes may be necessary. Please contact Cobalt Customer Support.
- **CPU Utilization:** Indicates current CPU utilization. The 9992-ENC has two CPU cores (C0 and C1); this indicates individual core utilization.
- **Ambient Temp:** Indicates the temperature, in degrees Celsius, of the air intake of the card (measured at the front edge of the card).
- **Internal Temp:** Indicates the temperature, in degrees Celsius, at the back of the card.
- **FPGA Core Temp:** Indicates the temperature at the FPGA processing element.
- **Card Power (W):** Indicates the current card power consumption
- **12V Rail Voltage:** Indicates the voltage at this rail.
- **1.8V Rail Voltage:** Indicates the voltage at this rail.
- **1.2V Rail Voltage:** Indicates the voltage at this rail.

The openGear™ frame is designed to operate in environments with up to 40°C ambient. There is typically a 5°C temperature raise from the external ambient to the "Ambient Temperature" measured by the 9992-ENC. If that measurement is at 45°C or higher, action must be taken to cool down the ambient temperature.

In order to protect itself from damage, the 9992-ENC will shut down if any of the temperatures exceed 85°C. It will automatically start again when the temperature normalizes.

Network Tab

The Network Tab allows for configuration/monitoring of the two Ethernet ports.

Network Configuration Tab

The Network Configuration Tab is used to configure the network interfaces for the device.
- The **Interfaces** tab is used to set the individual parameters for each of the Ethernet ports.
- The **DNS** tab is used to optionally configure DNS servers.
- The **RIST Tunnels** tab is used to manage RIST Main Profile tunnels.
- The **Authentication** tab is used to configure RIST Main Profile authentication options.

Network Configuration Interfaces Tab

This tab is used to configure the IP address and connection details for the two Ethernet ports:

- **Alarm on Link Loss:** If set to **Yes**, the card will raise an alarm if this Ethernet interface loses link. The Card State indicator in Dashboard™ and the front Status LED will both be red. If set to **No**, the card will still report loss of link in the Statistics page but no alarm will be raised. It is recommended that the alarm for ports that are in use be turned on; only turn it off if you do not plan to connect that port to a network.
- **IP Configuration:** Select **Static** or **DHCP** method for configuration. If **Static** is selected, the following options are displayed:
  - **IP Address:** Enter the desired IP address for this Ethernet port.
  - **Subnet Mask:** Enter the desired subnet mask for this Ethernet port.
  - **Default Gateway:** Enter the desired default gateway for this Ethernet port, or 0.0.0.0 if no gateway is available.
- **Interface speed:** Configures the speed of the interface. The 9992-ENC Ethernet interfaces only support two modes: 100 Mb/s Full-Duplex and 1 Gb/s Full-Duplex[4].
  - **Auto-Negotiate:** The Ethernet port will auto-negotiate the speed.
  - **100 Mb/s Full-Duplex:** Force the port to 100Mb/s Full-Duplex mode. Note that the port will still perform auto-negotiation, but it will only advertise this mode.
  - **1Gb/s Full-Duplex:** restrict the operation to 1Gb/s Full-Duplex mode. Note that the port will still perform auto-negotiation, but it will only advertise this mode.
  Notes:
  - If the 9992-ENC streaming Ethernet interfaces are connected, to a 10 Mb/s switch, hub, or network feed, link will **not** be established and the port will not recognize the connection.
  - If you select **100 Mb/s Full-Duplex** or **1 Gb/s Full-Duplex** and the corresponding streaming Ethernet interface is connected to a switch, hub or network feed that does not support the selected speed, link will **not** be established and the port will not recognize the connection.
  - If the interface speed is set to **Auto-Negotiate**, the streaming Ethernet port will allow link to be established in 100 Mb/s Half-Duplex mode. However, this will be flagged as a warning.
- **Interface Settings:** If you make any changes to the IP Configuration, IP Address, Subnet Mask and/or Default Encoder fields, the **Apply** and **Cancel** buttons become active. The changes only take effect when you press the **Apply** button. Pressing the **Cancel** button reverts the fields back to their original values.
  Note that the 9992-ENC will check the consistency of the data entered and will reject invalid combinations (i.e., combinations where the gateway is outside the interface subnet).

Once the **Apply** button is pressed, a confirm message appears, click **Yes** to apply setting or **No**.

---

[4] Support for 10 Mb/s and Half-Duplex modes are not offered, as these are unsuitable for MPEG transport over IP applications. Moreover, any modern switch supports at least 100 Mb/s Full-Duplex.
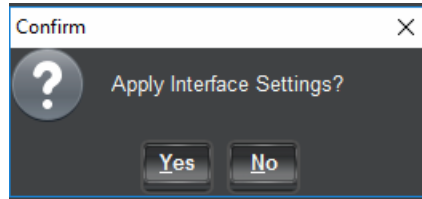
Once the setting is applied, a green success or a red error message will appear just below the **Cancel** button, as follows:
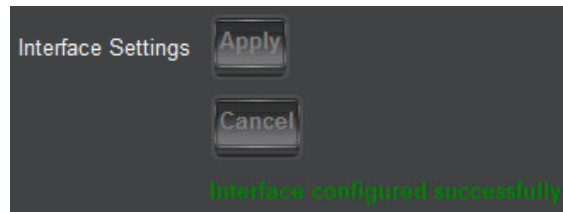
Network Configuration DNS Tab

The DNS tab allows manual configuration of up to two DNS servers. Additional DNS servers may be acquired via DHCP, if that method is configured. The DNS servers do not need to be in the same subnetwork as the streaming ports, as long as at least one default gateway is configured. DNS is used in conjunction with the RTMP or HLS output functionality. If you are not using these functions, there is no need to configure DNS servers.

The following applies to these configuration items:
- Values entered take effect immediately.
- An unused entry should be set to 0.0.0.0.
- DNS servers will be contacted in the order defined by the **DNS Priority** list. Note that the list automatically re-sorts as changes are made.

Network Configuration RIST Tunnels Tab
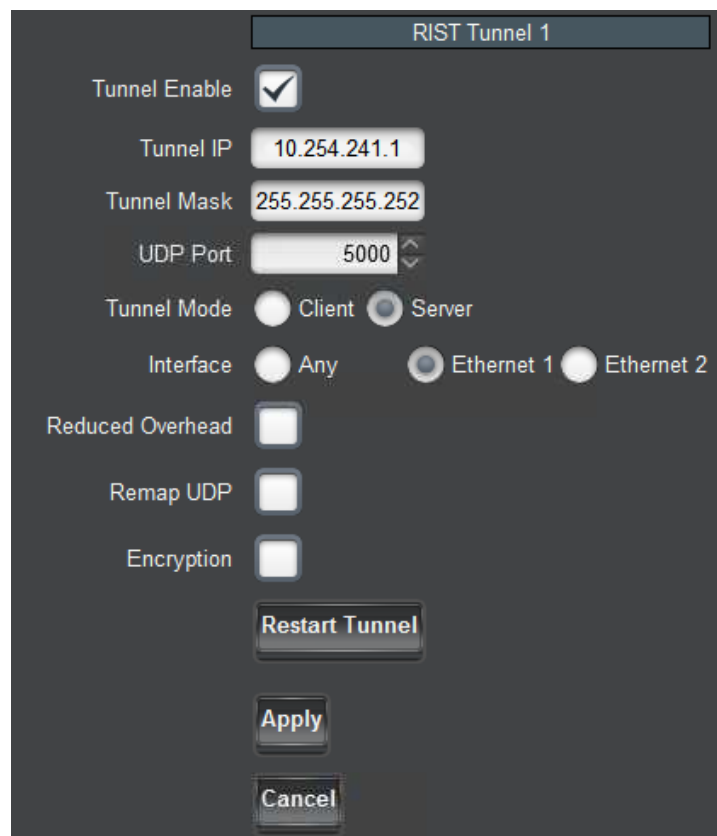
This tab allows the creation and management of RIST Main Profile tunnels. The 9992-ENC supports the creation of up to 4 RIST Main Profile tunnels. Creation of RIST tunnels requires the +**RIST/ARQ-ENC** license. RIST Main Profile tunnels use the GRE over UDP protocol.

In order to create a tunnel, check the **Tunnel Enable** box below:

Once the box is checked, the tunnel parameters are shown:

- **Tunnel IP:** this is the inner IP address of the encoder in the tunnel. It is not usually necessary to configure this parameter.
- **Tunnel Mask:** this is the subnet mask for the tunnel interface. It is not usually necessary to configure this parameter.

- **UDP Port:** this is the UDP port to be used in the tunnel establishment, as follows:
  - If the 9992-ENC is a **Server**, it will listen on this UDP port for incoming tunnel connections.
  - If the 9992-ENC is a **Client**, it will attempt to connect to this port in the server.
- **Tunnel Mode:** The 9992-ENC can be either a **Server** or a **Client**. If it is a server, it will wait to be contacted. If it is a client, it will actively attempt to contact the server. If **Client** is selected, an additional field appears where the server IP address can be entered:

- **Interface:** selects the network interface to use for this communication. The value of **Any** allows the device to select the most convenient interface based on the IP address. In particular, if the 9992-ENC is configured as a server, it will accept incoming connections on both Ethernet ports if the interface is set to **Any**.
- **Reduced Overhead:** RIST Main Profile defines a Reduced Overhead mode where only a simplified header. This reduces the overhead from 2.4% to 0.6%. This checkbox enables the use of Reduced Overhead mode for transmitted packets. Note that the 9992-ENC automatically detects incoming reduced overhead packets.
- **Remap UDP:** This box, if checked, causes the 9992-ENC to assume that all UDP packets coming in from the tunnel are destined to it regardless of their destination address. This control disappears in Reduced Overhead mode.
- **Encryption:** If this box is checked, the tunnel will be encrypted using DTLS, with optional authentication. Checking this box requires the +**RIST/ENCRP-ENC** license. Once this box is checked, the following additional options become available:

  - **Authentication:** If this box is not checked, the 9992-ENC will accept encrypted connections from any other device (regardless of whether it is operating as a client or a server). If it is checked, only authenticated connections will be accepted. Note that authentication requires prior setup to define acceptable connections; simply checking this box without any preparation will cause all connections (both incoming and outgoing) to fail. For a detailed explanation of how to set up the authentication function, please consult the section entitled "RIST Main Profile Authentication" later in this manual.
  - **Allowed Ciphers:** When the 9992-ENC negotiates an encrypted channel with a remote peer, it will negotiate a cipher suite, which includes both encryption and

authentication options. This list indicates which cipher suites the 9992-ENC is allowed to negotiate. The full names of the cipher suites are:

- **AES128-RSA:** TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- **AES128-ECDSA:** TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- **AES256-RSA:** TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- **AES256-ECDSA:** TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- **NULL:** TLS_RSA_WITH_NULL_SHA256

Notes:

- The **NULL** cipher has **NO ENCRYPTION**, only authentication. It is provided for testing purposes and **should not be enabled in production**.
- The use of AES 256 encryption is not allowed in some jurisdictions. Check your local laws before enabling.
- If there are no common ciphers enabled between the 9992-ENC and the peer, the connection will fail to be established.
- The 9992-ENC will negotiate the most secure cipher suite available. AES256 is preferred over AES128, and, for authentication, ECDSA is preferred over RSA.

- **Restart Tunnel:** This button causes a configured tunnel to disconnect and reconnect. Note that if the 9992-ENC is a server, it will be up to the peer to reconnect.
- **Apply/Cancel:** Each tunnel has independent Apply/Cancel buttons. Clicking on **Apply** causes the configuration changes to become active and persisted. Clicking on **Cancel** causes any changes to be discarded.

Network Configuration Authentication Tab

This tab controls the authentication options that are common for all RIST tunnels. Setting up authentication also requires access to web pages exposed by the 9992-ENC. The section entitled "RIST Main Profile Authentication" later in this document provides a detailed explanation of this process, and shows the relationship between the controls presented here and the web interface.
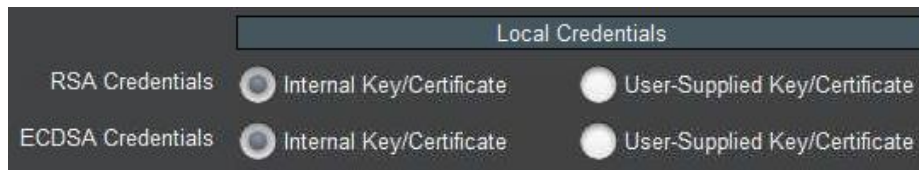
Access to the web interface is controlled by these settings:

- **Web Interface Password:** Web interface operations that are privileged require a password. This configuration item sets the password. You can select any password and enter it here. When executing a web interface operation that requires a password, use the same password there. The default password is `Admin` and it is strongly recommended that it be changed to something else.

- **Enable Web Config:** For security reasons, the web interface should only be enabled on Ethernet ports connected to a secured management network. Checking the box enables the web interface in the corresponding Ethernet port. If the box is not checked, the web interface is not available in that port.

The next section of the authentication tab pertains to the credentials the 9992-ENC uses for itself when negotiating a connection with a peer. The 9992-ENC has built-in keys and certificates. Using the web interface, custom keys and certificates can be uploaded to the device. The settings below select whether the 9992-ENC will use the built-in keys and certificates or the user-supplied keys and certificates:
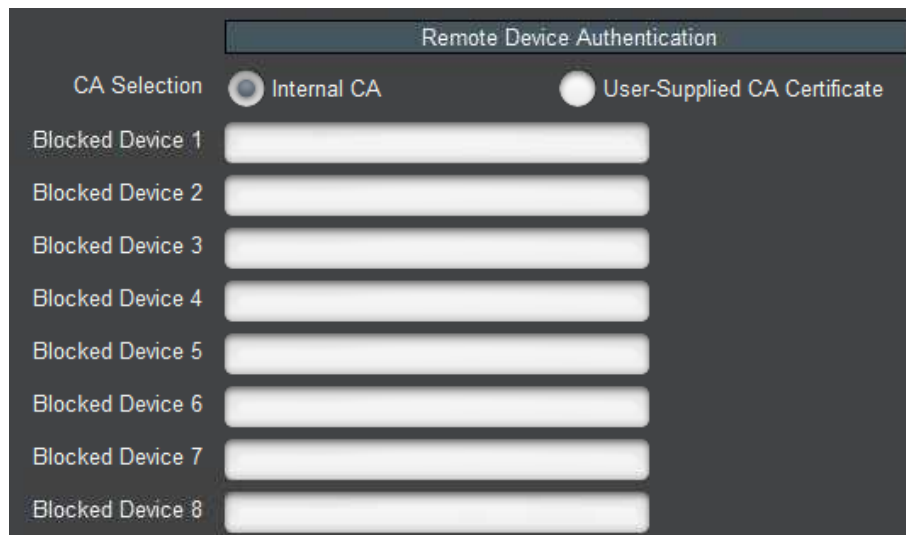
Notes:
- The RSA and ECDSA methods use different keys and certificates. Independent choices can be made for these two methods.
- The **User-Supplied Key/Certificate** option can only be selected if a user-supplied set of credentials has been previously uploaded to the device. The process of uploading credentials is described in the section entitled "Uploading Keys and Certificates" later in this manual.

This section of tab controls how the 9992-ENC authenticates remote devices:

If authentication is enabled, the 9992-ENC will agree to communicate with any peer presenting a certificate signed by a trusted Certificate Authority (CA). The 9992-ENC has a built-in CA, or an external CA certificate can be uploaded to it. Uploading an external CA certificate is done through the web interface; the process is described in the section entitled "Option 1: Use an

External Certificate Authority" later in this document. The **CA Selection** configuration item can choose between the local CA and the user-supplied CA. Note that selecting **User-Supplied CA Certificate** can only be done after a certificate is actually uploaded.

The 9992-ENC implements a blocked device list. This is a list of devices which have proper credentials (i.e., a certificate signed by the trusted CA) but should not be allowed to connect. Devices are identified by their **Common Name (CN)**. Section "Creating a Blocklist" later in this manual provides more detail on this process.

If you made any changes to the above parameters, these changes only take effect after you click on the **Apply** button. Clicking on the **Cancel** button reverts the changes.

If you are using the built-in CA in the 9992-ENC, it is important to back up its CA key. This section of the GUI provides this functionality:

Clicking on the **Save** button will generate a file called **CA_KEY.BIN** with the device's internal CA key. This file is encrypted and uses a proprietary format; it is not compatible with any third-party application.

If you need to restore a saved CA key to another Cobalt device, use the standard DashBoard upload function, available at the bottom of any tab:

Once the file is uploaded and validated, it is automatically installed as the device's CA key. A CA certificate is automatically generated to match this key, and can be downloaded through the web interface. An overview of the process can be found in the section entitle "Authenticating Remote Devices" later in this manual.

If you uploaded a new CA key to the 9992-ENC but later decide to revert to the original built-in key, this can be done simply by clicking on this button:

Network Statistics Tab

The Network Statistics Tab reports the status of the various functions in the Network tab.

Network Statistics Interfaces Tab

The following parameters are reported in the Network Statistics / Interfaces tab:

- **Alarm on Link Loss:** Reports the current setting of this parameter.
- **IP Address:** Reports the current IP Address for the port. If the port is set to DHCP and no address has been received, this will report 0.0.0.0.
- **Subnet Mask:** Reports the current Subnet Mask for the port. If the port is set to DHCP and no mask has been received, this will report 0.0.0.0.
- **Default Gateway:** Reports the current Default Gateway for the port.
- **Interface Speed:** Reports the current setting for this parameter.
- **Port 1/2 Link:** This indicator has the following states:
  - ● **Link OK**: The port has established link with the switch.
  - ○ **Half-Duplex Link:** The port is set to **Auto-Negotiate**, and it has achieved 100 Mb/s Half-Duplex link with the network connection. We do not consider Half-Duplex links suitable for video communication. The port will operate, but we recommend that this be addressed. If Alarm on Link Loss is set to Yes, the

Dashboard™ Card State will be yellow if there are no higher-priority alarms present.
- o ● **No Link:** The port does not currently have link. If Alarm on Link Loss is set to Yes, the Dashboard™ Card State will be red and the Status LED in the front of the board will also be red. If Alarm on Link Loss is set to No, this indicator will still be red, but the alarm will not propagate.
- **Port 1/2 Status:** This indicator is the port overrun status. It has the following states:
  - o ● **OK**: The port is operating normally.
  - o ● **TX Overflow:** In the current configuration, the IP outputs are attempting to transmit more than the port capacity (i.e., the overall output data for this port exceeds the interface speed of 100 Mb/s or 1 Gb/s). The Dashboard™ Card State will be red and the Status LED in the front of the board will be red. In this case, reduce the output bit rate (either by reducing the encoder bit rates or by removing output ports). **If this indicator is red, data is being dropped.**
- **Link Speed (Mb/s):** This parameter reports the actual speed negotiated with the switch for the port. If the port has no link, the value reported here is zero.
- **MAC Address:** This reports the MAC address of the Ethernet port.

Network Statistics DNS Tab

The Network Statistics DNS Tab reports the current DNS configuration, including the priority order.

	DNS Servers
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4
	DNS Priority
Priority 1	DNS Server 1
Priority 2	DNS Server 2
Priority 3	DHCP DNS Eth1
Priority 4	DHCP DNS Eth2
DHCP DNS Eth2	192.168.129.1

If any of the ports are set for DHCP, the DNS received from the DHCP server (if any) is displayed here. In the figure above, Ethernet 2 is set for DHCP and has received a DNS address through that process.

Network Statistics RIST Tunnels Tab

This tab shows the current configuration of the RIST tunnels. Only the enabled parameters are displayed.

Network Statistics Authentication Tab

This tab shows the current authentication options.

Network Statistics Tunnel Stats Tab

This tab is only present if there is at least one tunnel enabled, and only has entries for the enabled tunnels. The content is displayed below.

The fields are:

- **Full Datagram, Reduced Overhead, and Keep-Alive:** These fields show the number of received, transmitted, and dropped packets of each kind since the tunnel was established. A non-zero dropped count means that invalid packets are being received in the tunnel.
- **TX Rate (b/s):** This field shows the rate at which the 9992-ENC is transmitting in he tunnel, in bits/second.
- **RX Rate (b/s):** This field shows the rate at which the 9992-ENC is receiving packets from the tunnel, in bits/second.
- **Remote Endpoint:** This field shows the IP address and UDP port of the remote endpoint to which the 9992-ENC is connected. If the tunnel is configured as a client, this should match the server IP address and UDP port. If the tunnel is configured as a server, this will report the client's IP address and UDP port (which does not necessarily match the port at which the server is listening).
- **Remote Name:** This field reports the Common Name (CN) of the remote device. If encryption is not being used, this field will be blank. Note that, if this field is blank when authentication is enabled, it means that the peer did not send a CN or sent a blank CN. If you turn on authentication, connections with this peer will be rejected.
- **Remote MAC:** This field reports the remote MAC Address, if supplied in the Keep-Alive message. This field will be blank if the remote side does not send RIST Keep-Alive messages. While Cobalt devices will always send this information, it is legal for third-party devices to not include it.
- **Current Cipher:** This field shows the canonical name of the cipher suite currently in use. It will be blank if encryption is not enabled.

Network Statistics Remote Info Tab

RIST Main Profile defines an optional informational Keep-Alive message. If such message is present, its contents will be displayed in this tab. While all Cobalt devices generate these messages in RIST Main Profile mode, it is legal for peers not to send them. If these messages are not present, all the fields in this tab will be blank.

The fields are:

- **Features:** The Keep-Alive message has a number of feature flags. This field shows which flags are present in the message, as follows:

- o **X:** More capabilities. If this flag is set, it indicates that there are more capabilities included in the message.
- o **R:** Routing capability. If this flag is set, the device is willing to transmit and receive non-RIST traffic.
- o **B:** If this flag is set, device supports Bonding.
- o **A:** If this flag is set, device supports Adaptive Encoding.
- o **P:** If this flag is set, device supports SMPTE-2022 FEC.
- o **E:** If this flag is set, device supports seamless redundancy switch as per SMPTE-2022-7.
- o **L:** If this flag is set, device supports load sharing.
- o **N:** If this flag is set, device supports NULL packet deletion.
- o **V:** If this flag is set, device supports Reduced Overhead Mode.
- o **J:** If this flag is set, device is capable of sending, receiving and processing JSON information.

- **Tunnel IP:** This indicates the remote inner (tunnel) IP address, reported by the peer.
- **Remote IP:** This indicates the IP address the peer would like the 9992-ENC to take. This feature is not supported by the 9992-ENC. This value, if present, will be reported here but ignored.
- **Routing:** This indicates that the peer is capable of routing. Cobalt devices currently do not generate this flag.
- **Vendor:** This indicates the vendor of the peer. Cobalt devices will report "Cobalt Digital Inc".
- **Product:** This indicates the product name of the peer. The 9992-ENC will report "9992-ENC".
- **Version:** This indicates the software version currently running in the peer. The 9992-ENC will report the value found in the **Software Rev** field found in the Product Statistics Tab.

Video Inputs

The Video Inputs Tab is used to configure and monitor the encoder video inputs.

Video Inputs Configuration Tab

The 9992-ENC can operate in two modes:

- **Input Signal Timing Mode:** in this mode, the timing for the encoded stream is recovered from the video input signal. The video input signal must comply with the relevant SDI timing specifications to ensure that the bitstream STC is compliant. In this mode, the encoder can only accept independent signals in the Video 1 and Video 2 inputs. Signals in the Video 3 and Video 4 inputs, if present, must be externally frame-synchronized with the Video 1 or Video 2 signals. This mode presents the lowest latency in the encoder.
- **Framesync Mode:** in this mode, the bitstream timing is generated by the 9992-ENC and is guaranteed to be compliant. The encoder includes an internal framesync to guarantee operation. All input signals are internally synchronized to this input reference, and there is no requirement for the any of the signals to use the same time base. This mode will add a variable latency of up to one frame and will drop/repeat frames to keep the synchronization.

The Video Inputs configuration tab is shown below in both modes:
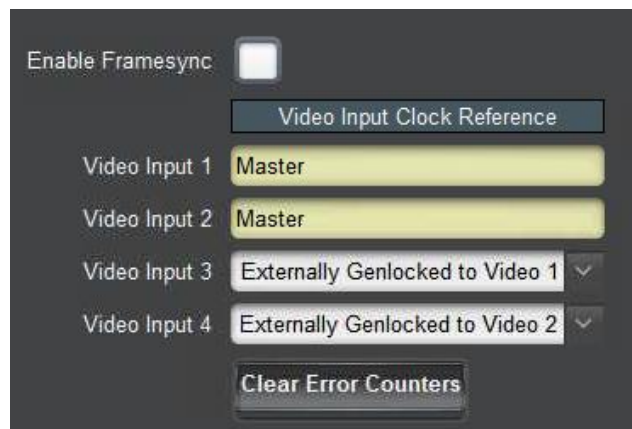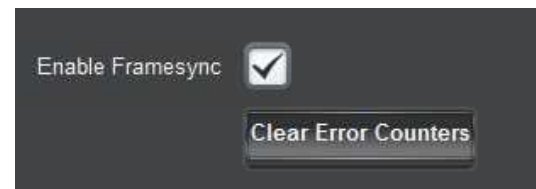
Input Signal Timing Mode   **Framesync Mode**

The **Enable Framesync** checkbox selects between the two modes. In Input Signal Timing Mode, the Video 1 and Video 2 inputs can take arbitrary signals, but Video 3 and Video 4 need to be externally synchronized to either one of these inputs. The **Video Input 3** and **Video Input 4** drop-down menus allow these selections to be made.

Regardless of mode, the 9992-ENC inputs keep a running count of CRC errors. Hitting the **Clear Error Counters** button resets this count back to zero.

Video Inputs Statistics Tab

The Video Inputs Statistics tab has two lower-level tabs, namely **External Inputs** and **Encoder Inputs**.

Video Inputs Statistics External Inputs Tab

The External Inputs tab shows the status of the actual encoder video inputs, as shown below.
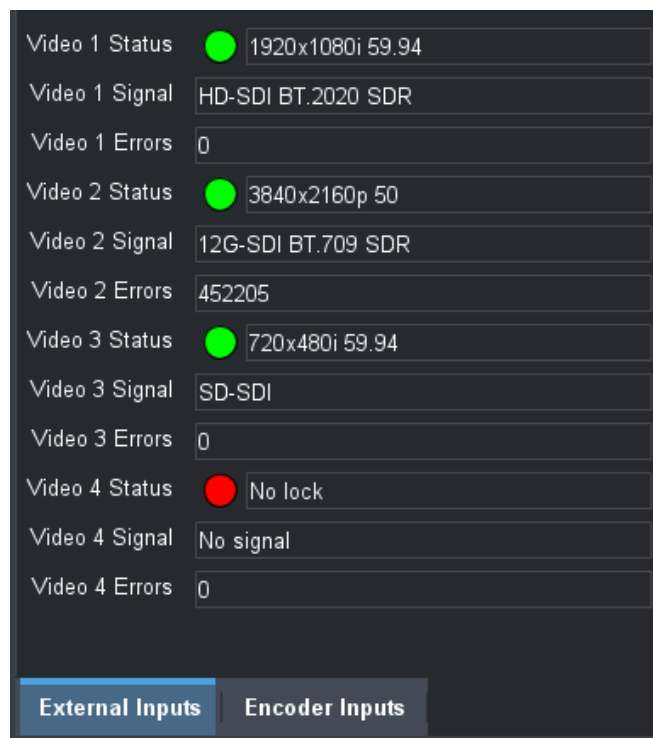
For each video input, the following information is indicated:
- **Video Status:** This shows what resolution and frame rate are detected in the video input. If there is no signal lock (i.e., no detected SDI framing), this indicator will be red and show **No lock**.
- **Video Signal:** This shows the type of signal detected. If there is signal, it will show the signal type, between SD-SDI, HD-SDI, 3G-SDI, 6G-SDI and 12G-SDI. If there is no signal, it will show **No signal**. If VPID is present in the signal, color space (BT.709 or BT.2020), transfer characteristics (SDR, HLG or PQ) and the video full range flag are also shown.
- **Video Errors:** This shows a running count of the CRC errors in that input. Hitting the **Clear Error Counters** button in the Video Inputs Configuration Tab resets this count to zero.
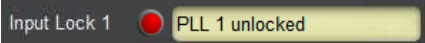
Video Inputs Statistics Encoder Inputs Tab

The Encoder Inputs tab shows the status of the internal encoder instances inputs. The individual fields are:
- **Input Lock 1/2:** This shows the status of the internal timing generators, as follows:
  - If the Framesync is disabled (**Enable Framesync** is not checked in the Video Inputs Configuration Tab), this will show the timing lock status of video inputs 1 and 2. The two possibilities are:
    - : The input has timing lock.

- ■ : The input has no timing lock.
  - o If the Framesync is enabled (**Enable Framesync** is checked in the Video Inputs Configuration Tab), this indicator will always show as follows:
    - ■
- • **DB 1/2/3/4 Status:** This shows the signal status of each of the four encoder instances. It identifies the signal that particular encoder instance is processing. Note that, if the signal is 4K, the four status indicators will show a 1920×1080p signal at the appropriate frame rate.

Encoder Mode

The Encoder Mode Tab is used to manage the parameters that are common to all encoder instances.

Encoder Mode Configuration Tab

The configurable parameters are:
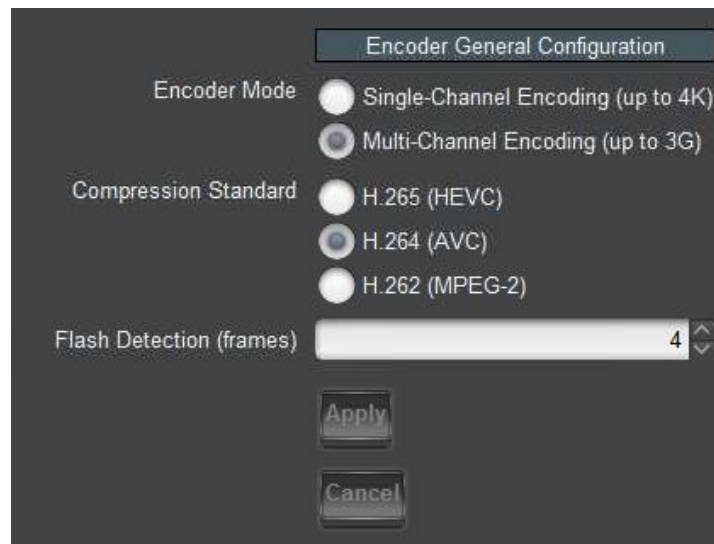
- **Encoder Mode**: The 9992-ENC can be configured either as a 4-channel HD encoder or a single-channel 4K encoder. Note that 4K operation requires the **+4K** option (factory installed in the 9992-ENC-4K-HEVC model). Also note that 4K operation is not supported for MPEG-2.
- **Compression Standard**: This selects the compression standard. Note that, in multi-channel mode, all channels will use the same compression standard. The options are:
  - **H.265 (HEVC):** This selects H.265 (High Efficiency Video Coding) compression. HEVC operation requires the **+HEVC** option (factory installed in the 9992-ENC-4K-HEVC model). When HEVC is selected, the **Latency Mode** selection is presented:
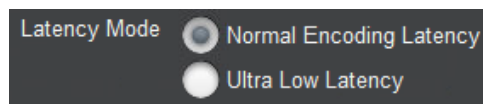
- **Normal Encoding Latency**: this mode is optimized for video quality, and all the HEVC parameters are available for configuration.
- **Ultra Low Latency**: this mode is optimized for low latency (less than one frame). Notes:
  - Many configuration parameters will not be available in this mode.
  - Ultra Low Latency operation requires the optional **+ULL** license.

o In Multi-Channel Encoding with Ultra Low Latency enabled, the encoder only supports **two** HD channels.

o Flash Detection is not available in Ultra Low Latency mode.

o **H.264 (AVC):** This selects H.264 (Advanced Video Coding).

o **H.262 (MPEG-2):** This selects H.262, which is more commonly known as MPEG-2 video encoding (ISO/IEC 13818-2).

- **Flash Detection (frames)**: The 9992-ENC has a video quality optimization function whereby it can detect scene changes and include I-Frames at change. However, for best video quality, this function needs to ignore flashes in the video. This setting configures the number of frames to be used in flash detection. Setting it to zero disables the function. Setting it to a non-zero value increases the encoder latency by the same number of frames. Note that this control will disappear in Ultra Low Latency mode.

Once you make your selections click, **Apply**. Note that making changes to this tab will cause all encoder instances to stop. Clicking on **Cancel** reverts any changes.

Note that the list of available output protocols changes based on the encoder compression standard.

Encoder Mode Statistics Tab

The Encoder Mode Statistics tab shows the current settings for the parameters in the Encoder Mode Configuration Tab.
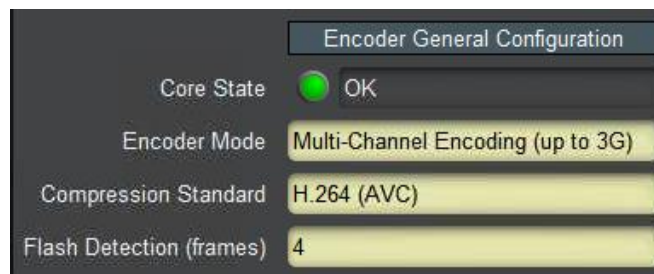
This tab has one additional indicator, **Core State**. This indicator should always show **OK**. If it does not, please reboot the encoder and contact Cobalt Digital.

Encoder 1-4 Tabs

The Encoder Tabs are used to configure/monitor the individual encoder channels. The number of tabs available depends on the configuration, as follows:

- In Single Channel mode, only the Encoder 1 tab is available.
- In Multi-Channel mode, the following tabs are available:
    o In HEVC Ultra Low Latency mode, the Encoder 1 and Encoder 2 tabs are available.
    o In all other modes, there will be Encoder 1 through Encoder 4 tabs.

The parameters in these Encoder tabs are identical.

In general, the encoder user interface will change as a function of the parameter selections. Controls may appear or disappear as applicable.

All encoder tabs have **Apply/Cancel** buttons at the bottom. Clicking on **Apply** implements the changes, clicking on **Cancel** reverts them.

Encoder Configuration Tab

The Encoder Configuration Tab is divided into the three following tabs:

- **Basic**: These are the common configuration parameters that apply to all encoding standards.
- **Advanced**: These are the more advanced configuration options. They are generally a function of the encoding standard.
- **Output**: These are the output configuration options.

Encoder Basic Configuration Tab

The Encoder Basic Tab Configuration Tab is divided into three general areas:

- **Encoder Configuration:** generic configuration parameters.
- **Video Parameters:** parameters related to video encoding.
- **Audio Parameters:** select the number of audio channels associated with this encoder

Basic Tab–Encoder Configuration

The encoder configuration will look different based on whether the encoder is in single or multi-channel mode, as shown below:
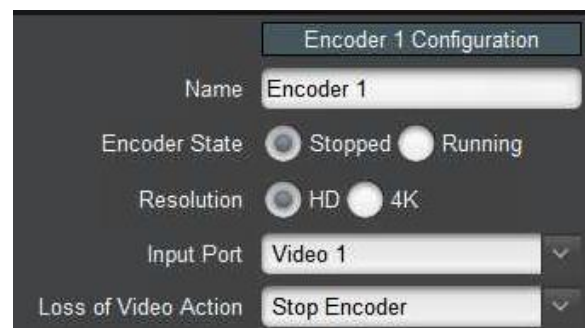
Multi-Channel Mode   **Single-Channel Mode**

- **Name:** All 9992-ENC encoders can be assigned a user-defined name. This name is used to identify the encoder later when making connections. Use any descriptive name suitable for your application, or accept the default.
- **Encoder State:** This control allows you to start/stop an encoder. This control needs to be set to **Running** for normal operation.
- **Resolution:** This control only appears if the encoder is in Single-Channel mode. Select **HD** for resolutions up to 1920×1080p, and **4K** for 3840×2160 resolutions.
- **Input Port:** This control is present if the encoder is in Multi-Channel mode, or if **Resolution** is set to **HD.** It selects the input port to drive this encoder instance. Note that multiple encoder instances can run independently from the same port, if desired. The encoder will automatically detect the signal and configure itself for the detected resolution and frame rate.
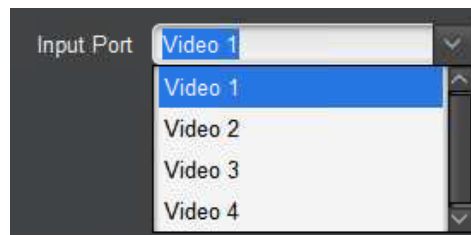
- o **4K Signal Source:** This control replaces the **Input Port** if the encNotoder is in Single-Channel mode and **Resolution** is set to **4K.** The options are shown below. The encoder can operate in Single-Link mode, where it will accept either a 6G-SDI or a 12G-SDI signal (which can be applied to either Video 1 or Video 2), or in Quad-Link mode, where it will take four SDI signals and combine them into one 4K image.
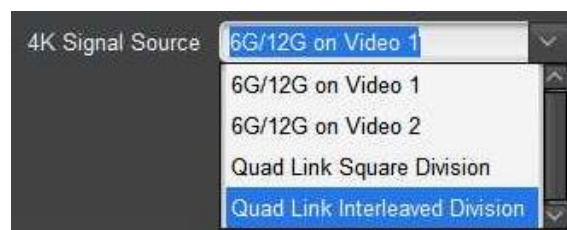
  Notes:
  - o While the encoder will automatically detect the frame rate of the incoming signal, it must match the selection above. For example, if Quad-Link is selected but a Single-Link signal is present, the encoder will not start.
  - o In Quad-Link mode, the signals must be connected in the correct order. The order is not automatically detected.
- **Loss of Video Action:** This control only appears if the **Enable Framesync** box in the Video Inputs Configuration Tab is checked. Regardless of the framesync setting, the 9992-ENC will not start without a video input signal. This control defines the encoder behavior if it loses the video signal **after** it is started. The options are:

41

- **Stop Encoder:** If this selected, the encoder will stop producing bitstream, and will only start again when the signal comes back. This is the behavior when the internal framesync is disabled.
- **Use Flat Field:** If this is selected, the encoder will continue operating with a flat field (i.e., a screen of a given color). Selecting this option opens an additional configuration item where the color of the screen can be selected, in YCrCb coordinates:

- **Freeze Frame:** If this is selected, the encoder will continue operating with the last good frame received from the input.

Note that these selections can be changed on-the-fly. For example, if flat field is selected and the encoder loses signal, you can select freeze frame after the video loss and the encoder will still put out the last good frame.

Basic Tab–Video Parameters

The basic Video Parameters are shown below:

- **Bit Depth:** Select from 8 Bits or 10 Bits.
- **Chroma Mode:** Select from 4:2:0 or 4:2:2. Note that 4:2:2 operation requires the **+422** optional license.
- **Down-Scale Video:** Select checkbox to down-scale the video. This causes the following additional controls to become available:

- o **Horizontal Resolution:** Enter the desired horizontal resolution in pixels.
- o **Vertical Resolution:** Enter the desired vertical resolution in pixels.

Notes:
- o The 9992-ENC will not upscale a signal. If you enter a resolution that is higher than the corresponding resolution of the incoming signal, that incoming resolution will be used. For example, if you select scaling to 900×900 and the incoming signal is 1280×720, the encoder output will be 900×720.
- o If the input signal is interlaced and the vertical resolution is not a multiple of 16, the encoder output will be converted to progressive.
- o The encoding standards supported by the 9992-ENC produce signals whose horizontal and vertical resolutions are multiples of 16. If you select a resolution that is not a multiple of 16, it will be internally rounded up and the signal will include cropping information for the decoder.

- **Progressive Half Frame Rate:** If this box is checked, progressive signals at 50, 59.94 and 60 frames/sec will be converted respectively to 25, 29.97, and 30 frames/sec. This box has no effect for other types of signals.
- **Progressive Conversion:** Check this box to convert an interlaced signal to progressive. This control has no effect for a progressive signal. The signal frame rates are not changed.
- **Spatial Filter Strength:** Select the strength of the spatial filter. A setting of 0 (zero) disables the filter. Increasing the spatial filter will make the image softer, which may provide better overall quality for lower bit rates.
- **Noise Reduction:** Select the level of noise reduction. The noise reduction filter is only available for interlaced content and has no effect for progressive content.
- **Video Rate Mode:** Select CBR (Constant Bit Rate) or VBR (Variable Bit Rate).
    - o **CBR**: Enter the desired elementary stream bit rate in bits/second.

    - o **VBR:** In VBR mode, multiple parameters are configurable:

- **Maximum Video Rate:** This control defines the maximum allowed video elementary stream bit rate. This control is not available for MPEG-2.
- **Average Video Rate:** This control defines the desired average elementary stream bit rate.
- **Minimum Video Rate:** This control defines the desired minimum elementary stream bit rate. This control is not available for MPEG-2.
- **Filler Video Bit Rate:** If you require that the elementary stream video bit rate do not fall below a certain value, set it in this control.

Basic Tab–Audio Parameters

- **Audio Channels:** Enter the desired number of audio channels. Note that an "Audio Channel" is equivalent to an "Audio PID" and can be mono, stereo, or surround (for supported audio encoding standards). Also note that, in RTMP output mode, this control is fixed to 1 as RTMP has no support for more than one audio channel.

Encoder Advanced Configuration Tab

The Advanced Configuration Tab is divided into three major areas:
- **Video Parameters:** These are advanced controls related to the encoding of the video. Which controls are displayed here depend on the video encoding standard.
- **VBI/Ancillary Data Insertion:** These parameters control ancillary data insertion. Ancillary data can be extracted from the video signal and mapped into the encoder output bitstream.
- **Mux Parameters:** These parameters control the PID assignments and contents of selected DVB tables.

Advanced Tab–Common Video Parameters

The Video Parameters displayed below are common to all encoding standards. Note that they will not necessarily be grouped this way in the Video Parameters area, but they will be present for all standards.
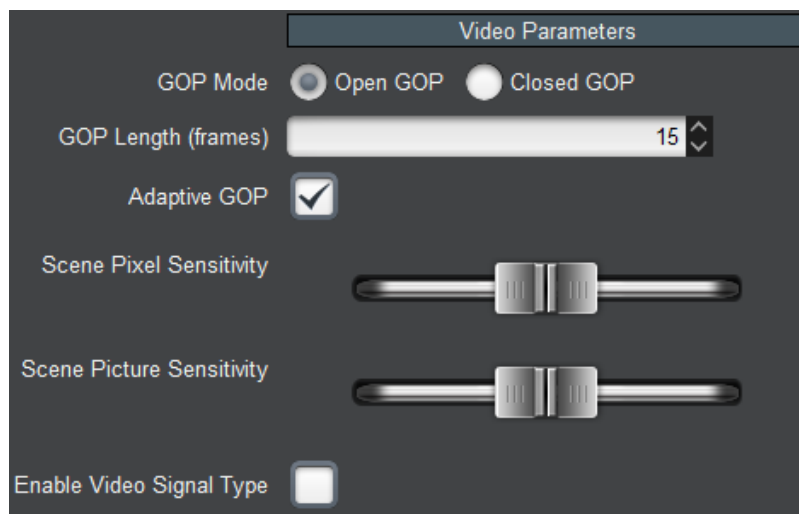
- **GOP Mode:** Select between **Open GOP** and **Closed GOP.** The normal setting is Open GOP, whereby the last frame(s) of a GOP can depend on frames in the next GOP. Closed GOP is used for some storage applications, and is required by some CDNs (such as YouTube); there is a very small negative impact in video quality if Closed GOP is selected.
- **GOP Length (frames)**: Select the GOP (Group Of Pictures) length, in frames. The actual GOP length may be slightly different depending on the GOP structure. For broadcast applications, a GOP corresponding to 0.5 sec is recommended. Larger GOP values can improve video quality.
- **Adaptive GOP**: Check this box to enable Adaptive GOP. When Adaptive GOP is enabled, a GOP may be terminated earlier on a scene change. Scene change detection can increase video quality for some content.
- **Scene and Pixel Picture Sensitivity**: These controls are only active if **Adaptive GOP** is checked. They control the scene change sensitivity at the pixel and frame levels. Moving the control to the left reduces the sensitivity, and moving them to the right increases it. For some content, having the sensitivity too high may cause video quality issues.
- **Enable Video Signal Type:** If this box is checked, video type information metadata is inserted in the video elementary stream. Additional controls become available to configure this metadata, as indicated below:

Automatic Settings Off

Settings Derived from VPID

If necessary, these parameters should be set to match the characteristics of the incoming video input signal. For example, for a PQ10 HDR signal with WCG, the following settings are suggested:

Note that the **Video Full Range** checkbox is not available in MPEG-2 mode.

The 9992-ENC can also automatically set the video signal type based on VPID. This will work well with PQ10 HDR signals and HLG signals. Note, however, that the VPID information is not as comprehensive as the full video signal type options.

Please consult the relevant standards for further guidance on these settings.

Advanced Tab–Additional HEVC Video Parameters

The HEVC-specific Advanced Tab parameters are shown below.

- **Level:** By default, the encoder will select the correct level based on settings. The automatic selection can be overridden here. Note that the encoder will ignore this setting if it is invalid (i.e., you cannot set a level lower than the minimum for your settings).
- **Profile:** By default, the encoder will select the correct profile based on settings. The automatic selection can be overridden here. Note that the encoder will ignore this setting if it is invalid based on the current configuration.
- **General Tier:** Select from a drop-down list, Main or High Tier.
- **Aspect Ratio:** If your application requires it, select the Aspect Ratio to be coded in the bitstream metadata.
- **Scene Change Block Period:** After a GOP is terminated early due to a scene change, the encoder will ignore further scene changes for a period of time, as this may improve
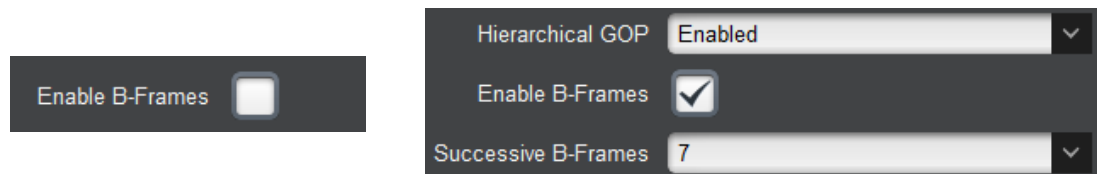
quality. If this parameter is set to **Auto**, the encoder will automatically set this period. If it is set to **Manual**, a new control becomes available for this period:

- o **Scene Change Block Frames:** Enter the number of frames after a scene change for which the encoder will ignore further scene changes.
  Note: this parameter is only effective if the **Adaptive GOP** box is checked (see Advanced Tab–Common Video Parameters).
- **Enable B-Frames:** Select the check box to enable B-Frames. If this box is checked, additional controls become available:

- o **Hierarchical GOP**: Available options are **Enabled**, **Disabled¸** and **Enabled (Low Delay)**. The best video quality is obtained with the **Enabled** setting.
- o **Successive B-Frames:** Select the number of successive B-Frames. The available selections will be a function of the **Hierarchical GOP** settings. The best video quality is obtained with the value of 7.
- **IDR Interval (GOPs):** This parameter controls how often the encoder inserts an IDR. If your network is not reliable, use a small value (less than 5) here. Having frequent IDRs may reduce the video quality at low bit rates, but if the interval is high, the artifacts due to dropped data will persist longer.
- **Use Temporal ID:** If this box is checked, the bitstream will include Temporal ID. This usually not necessary.
- **Encode P as B using L0:** If this box is checked, P-Frames will be encoded as B-Frames with L0. There is a small video quality improvement when this used.
- **Disable Min QP Control:** If this box is checked, the minimum QP control is disabled. It is usually not necessary to do this.
- **Adaptive Quantization:** If this box is checked, Adaptive Quantization is enabled. Enabling Adaptive Quantization can increase video quality. Unless there is a specific reason, Adaptive Quantization should remain enabled.
- **CPB Delay (ms):** This parameter controls the size of the CPB (Coded Picture Buffer), and represents a direct tradeoff between latency and quality. The CPB Delay is a direct component of the encoder delay. Increasing the CPB increases the latency but also increases the video quality. Unless your application is latency-sensitive, it is recommended that the CBP Delay be left at the default value of 1000 ms.
- **Horizontal GDR, Vertical GDR:** GDR (Gradual Decoder Refresh) is a technique that can reduce the encoder latency. Enabling one or both of these parameters may reduce the

end-to-end latency at the expense of video quality. The block size represents a tradeoff between latency and quality (higher block sizes will have higher latencies).

- **PPS Insertion:** This parameter controls where the Picture Parameter Set (PPS) is inserted. It is usually not necessary to make changes to it. Setting it to **Every Picture** may have a negative quality impact at lower bit rates because the overhead increases.
- **Deblocking Filter:** Check this box to enable the deblocking filter. Disabling the deblocking filter will degrade video quality. This control is provided for compatibility with low-end decoders; do not disable unless absolutely necessary.
- **Weighted Prediction:** Check this box to enable weighted prediction. Disabling weighed prediction will degrade video quality. This control is provided for compatibility with low-end decoders; do not disable unless absolutely necessary.

Advanced Tab–Additional HEVC Video Parameters in ULL Mode

If Ultra-Low Latency is enabled, several of the above parameters will no longer be available or will have their ranges restricted. The available parameters are shown below. The individual parameter descriptions from the previous section still apply.

Advanced Tab–Additional AVC Video Parameters

The AVC-specific Advanced Tab parameters are shown below.

- **Level:** By default, the encoder will select the correct level based on settings. The automatic selection can be overridden here. Note that the encoder will ignore this setting if it is invalid (i.e., you cannot set a level lower than the minimum for your settings).
- **Profile:** By default, the encoder will select the correct profile based on settings. The automatic selection can be overridden here. Note that the encoder will ignore this setting if it is invalid based on the current configuration.
- **Aspect Ratio:** If your application requires it, select the Aspect Ratio to be coded in the bitstream metadata.
- **GOP Structure:** Select between **IBBP, IBP** and **IP**. Selecting **IBBP** gives the best video quality, but some low-end decoders require **IP**.
- **Adaptive B-Frames:** Check this box to enable Adaptive B-Frames. Enabling this parameter improves video quality. It is suggested to leave this enabled unless you experience decoder compatibility issues with low-end devices.
- **First GOP Picture:** Select either B Picture or IDR Picture for the first picture in the GOP. It is usually unnecessary to change this setting.
- **IDR Interval (GOPs):** This parameter controls how often the encoder inserts an IDR. If your network is not reliable, use a small value (less than 5) here. Having frequent IDRs may reduce the video quality at low bit rates, but if the interval is high, the artifacts due to dropped data will persist longer.
- **CPB Delay (ms):** This parameter controls the size of the CPB (Coded Picture Buffer), and represents a direct tradeoff between latency and quality. The CPB Delay is a direct component of the encoder delay. Increasing the CPB increases the latency but also increases the video quality. Unless your application is latency-sensitive, it is recommended that the CBP Delay be left at the default value of 1000 ms.

50
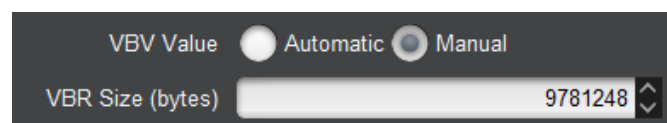
- **Low Latency (GDR) Mode:** GDR (Gradual Decoder Refresh) is a technique that can reduce the encoder latency. The actual GDR value (between 1 and 4 lines) makes little difference in the latency.
- **PPS Insertion:** This parameter controls where the Picture Parameter Set (PPS) is inserted. It is usually not necessary to make changes to it. Setting it to **Every Field/Frame** may have a negative quality impact at lower bit rates because the overhead increases.
- **Deblocking Filter:** Check this box to enable the deblocking filter. Disabling the deblocking filter will degrade video quality. This control is provided for compatibility with low-end decoders; do not disable unless absolutely necessary.
- **Weighted Prediction:** Check this box to enable weighted prediction. Disabling weighed prediction will degrade video quality. This control is provided for compatibility with low-end decoders; do not disable unless absolutely necessary.
- **Clip QP:** Check this box to clip the minimum value of pic_init_qp_minus26 to -26. This control is provided for compatibility with low-end decoders; do not check this box unless absolutely necessary.

Advanced Tab–Additional MPEG-2 Video Parameters

The MPEG-2 specific Advanced Tab parameters are shown below.
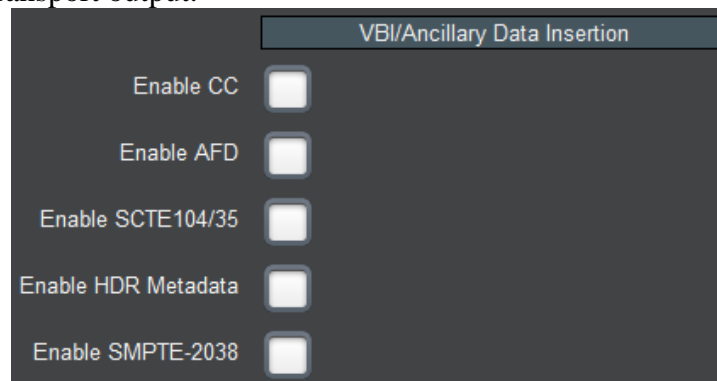
- **GOP Structure:** Select between **IBBP, IBP** and **IP**. Selecting **IBBP** gives the best video quality, but some low-end decoders require **IP**.
- **Aspect Ratio:** Selects the Aspect Ratio coded in the MPEG-2 bitstream. Choose it according to your signal requirements.
- **VBV Value:** This selects the value of the Video Buffer Verifier, which is the MPEG-2 equivalent of the CPB in AVC/HEVC. It represents a direct tradeoff between latency and quality. It is recommended that this be left in the **Automatic** setting. If **Manual** is selected, an additional control becomes available:

  o **VBV Size (bytes):** enter the desired VBV size. Reducing the VBV will reduce the latency, but also the video quality.

Advanced Tab–VBI/Ancillary Data Insertion

The 9992-ENC can extract the following data types from the video input signal and insert them in the compressed transport output:
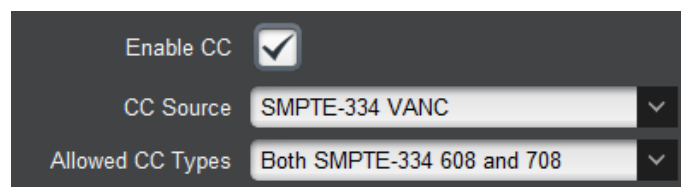
- Closed Captioning (CC)
- Active Format Description (AFD)
- SCTE 104 Ad Insertion Triggers (which are converted to SCTE 35 messages)
- HDR Metadata, carried over SMPTE 2108 ancillary data packets
- Any other generic ancillary data types, which are inserted using SMPTE-2038

Closed Captioning

The Closed Captioning controls are as follows:

- **Enable CC:** Check this box to enable Closed-Captioning insertion. Closed Captions are inserted in the video elementary stream, as per ATSC A/72. Both CEA-608 and CEA-708 captions are supported. Once this box is checked, additional controls are displayed:

- **CC Source:** This controls where the encoder extracts closed captions. The options are:
    - **SMPTE-334 VANC**: The encoder extracts CC information from ancillary data packets. Both CEA-608 and CEA-708 modes are supported (and automatically detected).
    - **CEA-608 Line 21**: This option is only effective if the input is SD. The encoder will extract all the CEA-608 information from both fields of Line 21, if present. If the input is not SD, the encoder will always look for CC ancillary data packets.
- **Allowed CC Types:** SMPTE-334M specifies two types of Closed-Captioning information in the VANC:
    - EIA-708 captions on DID 0x161, SDID 0x101
    - EIA-608 captions on DID 0x161, SDID 0x102

This control has the following settings:

- **Both SMPTE-334 608 and 708:** the encoder will accept and process either format. However, note that if both formats are present, the captions will be inserted twice.
- **SMPTE-334 708 Only:** the encoder will accept only EIA-708 captions on DID 0x161, SDID 0x101, and will discard any EIA-608 captions received on DID 0x161, SDID 0x102.
- **SMPTE-334 608 Only:** the encoder will accept only EIA-608 captions on DID 0x161, SDID 0x102, and will discard any EIA-708 captions received on DID 0x161, SDID 0x101.
- **OP-47 Captions:** the encoder will only accept OP-47 captions on DID 0x143, SDID 0x102, and will discard SMPTE-334 captions. If this option is selected, the following additional controls appear:

- **OP-47 Language Code:** This field allows the setting of the 3-letter ISO 639-2 language code for the OP-47 captions. It is carried in the PMT.
- **OP-47 Page Number:** This field allows the setting of the OP-47 Page Number in the PMT. Note, however, that the page number is also encoded in the captions themselves. The 9992-ENC is not capable of altering the OP-47 data flow to match this field. It must match the actual page number of the captions.

Active Format Description

The 9992-ENC extracts Active Format Description (AFD) information from the incoming video signal and insert into the compressed bit stream. It can be extracted from the following sources:

- For SDI signals, AFD information can be present in the VANC as per SMPTE-2016-3. This is the primary way of conveying AFD information on a professional video feed.
- For SD signals (either from Composite or SD-SDI sources), AFD information can be synthesized from Wide Screen Signaling (WSS) data present in the VBI (line 20 for NTSC signals, line 23 for PAL signals).
- The 9992-ENC has the option of inserting a user-defined AFD code (instead of receiving it from the video input).
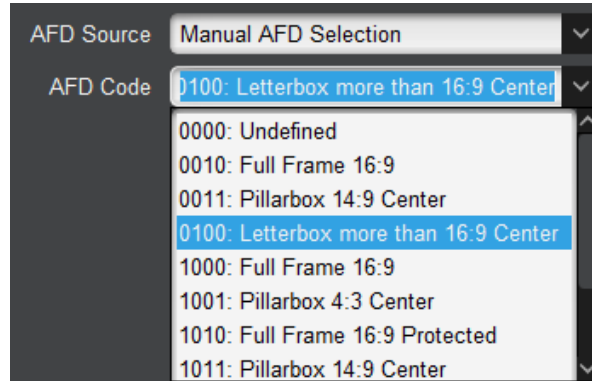
The AFD controls are as follows:

- **Enable AFD:** Check this box to enable AFD extraction and insertion. AFD is inserted in the video elementary stream as per ATSC A/72 and ETSI TS 101 154.
- **AFD Source:** Selects the input source of AFD information.
  The options are:
  - **Line 20 WSS/Line 23 WSS:** This option causes the encoder to synthesize AFD information from WSS. It is used only if the input resolution is SD, otherwise the encoder falls back to SMPTE-2016. It will be displayed as Line 20 for NTSC and Line 23 for PAL. For PAL inputs, the conversion follows ETSI TS 101 154 Appendix B.4.
  - **SMPTE-2016-3 VANC:** This option causes the encoder to extract AFD from the VANC.
  - **Manual AFD Selection**: This option allows the user to specify a fixed AFD code to be inserted. Any AFD information received from the input is ignored. This can be used to override the original AFD information, or when the video is being scaled (e.g., when the input is HD and is being converted to SD).
- **AFD Code:** This control is displayed <u>only</u> when AFD Source is set to Manual AFD Selection. It corresponds to the codes listed in SMPTE-2016-1, Table 1.

SCTE 104 Ad Insertion Triggers
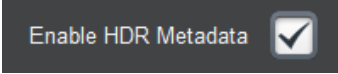
The 9992-ENC is capable of extracting SCTE 104 triggers from the VANC (inserted as per SMPTE 2010) and converting them to SCTE 35 triggers in the output transport stream:

- **Enable SCTE 104/35:** Check this box to enable SCTE 104 extraction. The SCTE 104 triggers are inserted in the transport stream as SCTE 35 sections.

SMPTE-2108 HDR Metadata

The 9992-ENC is capable of extracting SMPTE-2108 HDR Metadata from the VANC and insert it in the video elementary stream as SEI messages.

- **Enable HDR Metadata:** Check this box to enable SMPTE 2108 extraction and insertion as SEI messages in the video elementary stream.

SMPTE-2038 Generic ANC Transport

The 9992-ENC is capable of extracting any generic (non-specific) ANC data (both from the VANC and the HANC) and inserting them into the output transport stream:

- **Enable SMPTE-2038:** Check this box to enable generic ANC extraction and insertion using SMPTE-2038. Once checked, the following additional controls are displayed:
    - o **Maximum Bit Rate (b/s):** Some types of ANC data, such as VITC or LTC, may use a non-trivial amount of bandwidth in the output. This parameter controls how much bandwidth to reserve in the transport stream output for ANC data, for NULL-padded CBR outputs. If the ANC data bit rate exceeds this value, packets may be dropped. For ANC data that appears only occasionally, a bit rate of zero may be specified. Note that the encoder measures the actual ANC rate in the transport stream and reports it in the **Status** tab (please refer to the Encoder Statistics section of this manual).
    - o **Offset (frames):** The encoder will include information in the transport stream that enables the decoder to restore the ANC data to the exact same frame it came from. This control allows the encoder to offset this information to a range of -5 to +5 frames (i.e., the decoder will restore the ANC data to an earlier or later frame based on this setting). The default setting of 0 offset is recommended and will properly reinsert timecode into its corresponding SDI source frame.
    - o **Enable/DID/SDID:** The encoder can support transport of up to 4 DID/SDID pairs per video input. They are specified here. Check the **Enable** box to enable a particular DID/SDID. Note that GUI shows the full 10-bit DID/SDID, but it accepts 8-bit entries as well. For example, the DID/SDID for VITC is 0x60/0x60 (8-bits). Simply enter "60", and the encoder will compute the final 10-bit value (0x260) and display it. DID/SDID values are always entered in hexadecimal. The leading "0x" does not need to be entered, but will be automatically added by the encoder.

Notes:
- Only four DID/SDID pairs can be specified per video input.
- The SMPTE-2038 feature is not available for SMPTE-334M Closed-Captioning, OP-47 Captions, SMPTE-2016 AFD, SCTE-104 triggers and SMPTE-2108 HDR Metadata, as there are well-defined standards for carriage of this information. Therefore, the following DID/SDID pairs will always be ignored if specified for SMPTE-2038 (even if the corresponding feature is disabled):

DID	SDID	Data Type
0x161	0x101	EIA 708 CC
0x161	0x102	EIA 608 CC
0x143	0x102	OP-47 Captions
0x241	0x205	AFD
0x241	0x107	SCTE-104/SMPTE-2010
0x241	0x20C	SMPTE-2108 HDR Metadata

Advanced Tab – Mux Parameters

These parameters control the details of the audio/video multiplexing, and the (P)SI tables. If the Output Protocol in the Encoder Connections Tab is set to RTMP, these parameters will not be shown as RTMP does not use the Transport Stream container.
The following Mux Parameters are always available if the Output Protocol is not set to RTMP:
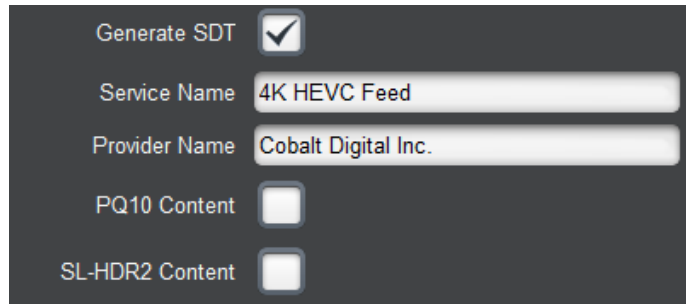
- **PMT PID, PCR PID, Video PID, Audio PID, SCTE 35 PID, SMPTE 2038 PID, and OP-47 PID:** These parameters control the Packet Identifier (PID) values for the PMT, PCR, Video, and Audio, and the various ancillary data formats. The values can be entered in hexadecimal (prefixed by 0x) or in decimal. Valid values are from 0x20 (32) to 0x1FFE (8190). PMT PID, Video PID and Audio PID must be distinct values. PCR PID can either be the same as the video PID or distinct from the other values as well. The user interface will not accept an invalid entry at any time – it will immediately revert to the previous value. The number of audio PIDs displayed corresponds to the number of audio channels configured in the Basic Tab–Audio Parameters. The SCTE 35 PID entry is shown only if SCTE 104 Ad Insertion Triggers are enabled. The SMPTE-2038 PID entry is shown only if the feature is enabled. The OP-47 PID entry is only shown if OP-47 captions are enabled.
- **Program Number:** Enter the desired program number for this encoder channel. Valid program numbers go from 1 to 65535 and are always entered in decimal.
- **Transport Stream ID:** Enter the desired Transport Stream ID for this encoder channel. Values in this field can be entered both in hexadecimal (prefixed by 0x) or in decimal.
- **Generate SDT:** This box is always shown but is not selectable for the HTTP Live Streaming and RTMP protocols. If this box is checked, an SDT will be generated for this encoder channel. Additional SDT parameters become available once this box is checked, as depicted below.
- **Service Name:** Enter the desired SDT service name for this encoder channel. The default name is **Slot X Encoder Y**, where **X** is the openGear® slot number where the 9992-ENC is installed, and Y is 1 through 4 (for Encoder 1 through Encoder 4).

- **Provider Name:** Enter the desired SDT service provider name. The default is **Cobalt Digital Inc**.

If the encoding standard is set to HEVC and the encoder is configured for 10-bit operation, the following two additional checkboxes become available:

- **PQ10 Content:** if this box is checked, the SDT will signal that the video service contains content in PQ10 format.
- **SL-HDR2 Content:** if this box is checked, the SDT will signal that the video service contains content in SL-HDR2 format. Note that, in this case, the PQ10 box must also be checked. The encoder will enforce this by automatically checking the box. Conversely, if the PQ10 box is unchecked, the SL-HDR2 box will also automatically be unchecked.

Encoder Output Configuration Tab

The Output Configuration Tab allows you to configure the encoder output protocols. Note that not all protocols are available for all compression standards, as indicated in the table below. The table also indicates which protocols have MPTS mux support.

Protocol	MPEG-2 (H.262)	AVC (H.264)	HEVC (H.265)	MPTS
ASI/IP Streaming	✓	✓	✓	✓
RIST	✓	✓	✓	
HLS		✓	✓	
RTMP		✓		
SRT	✓	✓	✓	

The Output Protocol selection is displayed below. The actual choices offered will depend on the compression standard.
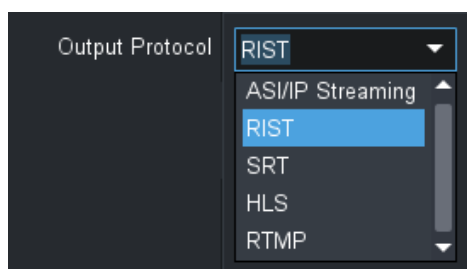
- o **ASI/IP Streaming:** the output of the encoder is available for connection to ASI Outputs and IP Outputs, as described later in this manual.
- o **RIST:** the encoder will transmit RTP streams compliant with the Reliable Internet Stream Transport, and will accept retransmission requests as per VSF TR-06-1. It also supports Source Adaptation as per VSF TR-06-4 Part 1 and NULL Packet Deletion as per VSF TR-06-2.
- o **SRT:** the encoder will operate in SRT mode. It can be configured as a caller, listener, or in rendezvous mode.
- o **HLS:** the encoder will operate in HTTP Live Streaming (HLS) mode. It can push content to an external server, or it can publish content to an internal web server.
- o **RTMP:** the encoder will operate as an RTMP client, connect to a specified RTMP server and publish the stream, similar to the Adobe Flash® Live Media Encoder (FMLE). If this is selected, a number of parameters in the Encoder Configuration tabs will either disappear or become grayed out.

The options displayed will change according to the protocol.

Output Tab–ASI/IP Streaming

- The figure below shows the configuration options in ASI/IP Streaming mode. The list of ports offered for connection always includes the encoder's ASI outputs, and will include however many IP Outputs created in the IP Outputs Tab.

In order to connect to a given port, simply check the box in front of that port. A given encoder channel can be connected to more than one port. Note that if multiple encoder instances are connected to the same port, the output will be a Multi-Program Transport Stream (MPTS). The internal mux will resolve any PID conflicts by remapping and adjusting tables. SDT information will be merged.
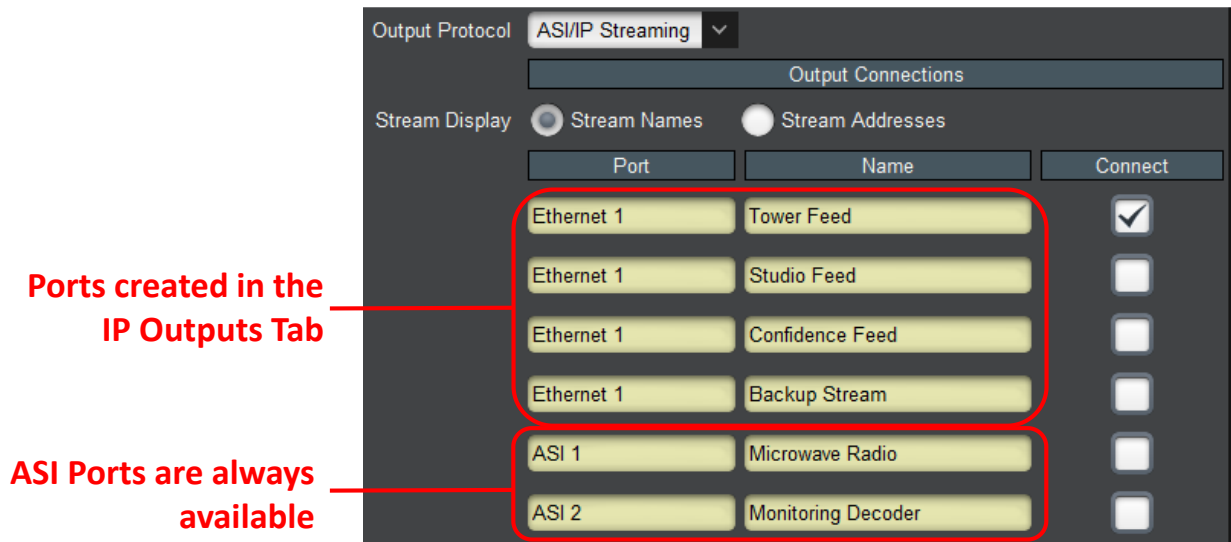
The **Stream Display** selector controls how streams are displayed. The picture above shows the **Stream Names**, where the ports are identified by their names (which are configurable). Selecting **Stream Addresses** shows the destination IP Address and UDP ports, as illustrated below.
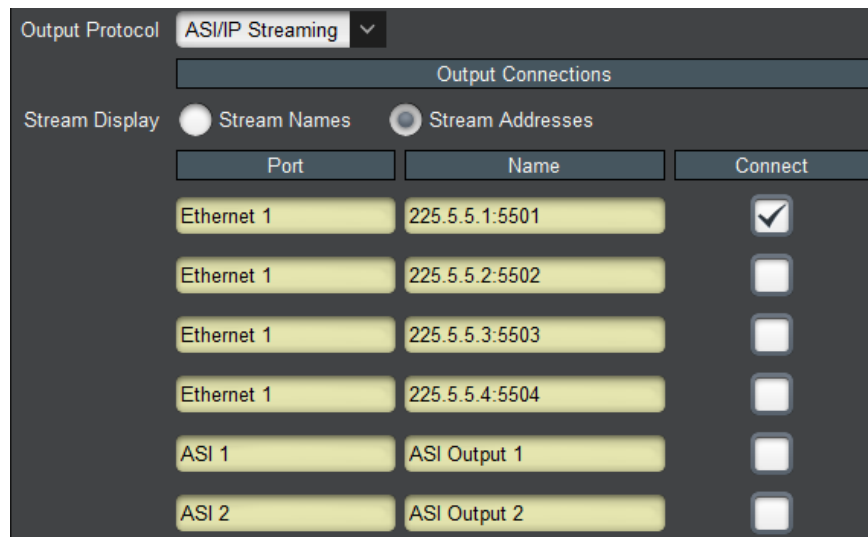
Output Tab–RIST

The figure below shows the output tab when RIST is selected. In this mode, up to four copies of each stream can be sent by the encoder. The basic parameters are:

- **Drop Null Packets:** check this box to remove the NULL packets from the output. Note that most professional-grade IRDs require NULL packets. The professional decoders from Cobalt Digital can operate without NULL packets. If this box is checked, the **Null Packet Deletion** control is not shown.

- **Protocol:** select the output protocol variation. The options are:
  - **UDP:** this provides transport stream packets directly over UDP, with no packet loss recovery. This option is offered to allow UDP operation over RIST Main Profile tunnels, for networks where packet recovery is not necessary.
  - **RTP:** this provides transport stream packets over RTP, with no packet loss recovery. This option is offered to allow RTP operation over RIST Main Profile tunnels, for networks where packet recovery is not necessary. RTP requires that the UDP port used be an even number.
  - **RIST:** this provides packet loss recovery using the Reliable Internet Stream Transport (RIST), as per VSF TR-06-1. This selection requires the optional **+RIST/ARQ-ENC** license to be installed in the encoder. Since RIST is based on RTP, the UDP port used will have to be an even number. Note that, if RIST is configure to send the RTP stream to port P, it will also send RTCP packets to port P+1. When RIST is selected, the following options become available:

The RIST configuration is:
- **NACK Window (ms):** specify how long the encoder should buffer transmitted packets in expectation of retransmission requests. The exact number does not matter much; a value in the order of 5000 milliseconds should cover most cases.
- **Transmission Mode:** this parameter controls how the encoder handles multiple destinations. The options are:
  - **Independent Destinations:** The encoder treats each destination enabled under **Stream Destinations** as an independent receiver. Retransmission requests will be independently handled per destination.
  - **Replicated Streams:** The encoder assumes that it is sending multiple copies of the stream to the same receiver, to implement SMPTE-2022-7 Seamless Switching. Retransmissions may not be sent over the same destinations as the requests.
  - **Bonded Streams:** The encoder splits the streams equally over the configured destinations. For example, if there are three destinations, each will get 1/3 of the packets. It is assumed that all destinations correspond to the same receiver, and the receiver will re-order the packets prior to consuming them.
- **Limit Retrans Rate:** if this box is checked, the retransmission rate is limited. A new parameter becomes available, where the maximum retransmission rate can be entered.

- **Adaptive Encoding:** Check this box to enable Source Adaptation as per VSF TR-06-4 Part 1. Adaptive Encoding requires the receiver to send back TR-06-4 Link Quality messages; the 9992-ENC will dynamically change its video bit rate to adapt to reported network conditions. Note that Adaptive Encoding requires either **Null Packet Deletion** or **Drop Null Packets** to be enabled. If this box is checked, the following additional parameter becomes available:

- **Lowest Video Rate (%):** Determines the lowest bit rate the encoder is allowed to go when adapting to the network conditions, expressed as a percentage of the video bit rate.
- **Null Packet Deletion:** If this box is checked, the encoder will implement Null Packet Deletion as per VSF TR-06-2. In this mode, NULL packets are removed, but an RTP extension header is added to the packet indicating their original positions. A compliant receiver can re-insert the NULL packets and re-create a compliant CBR transport stream.

Stream Destinations: up to 8 stream destinations can be configured. They will all receive the same content and share the same NACK window if RIST is enabled. The destination parameters are:
- **Enable:** check this box to enable transmission to this particular destination.
- **Destination:** enter the destination IP address.
- **UDP Port:** enter the destination UDP port. In RIST and RTP modes, this UDP port must be an even number. Odd numbers will not be accepted in the GUI.
- **Interface:** select the desired streaming interface. RIST tunnels defined in the Network Configuration RIST Tunnels Tab can also be selected here.
- **TTL:** select the desired Time-To-Live for the packets. The TTL value specifies how many routers the packet can cross before being dropped.
- **TOS:** enter the value of the Type-Of-Service (TOS) field in the IP header, if desired, between 0 and 255. The upper 6 bits of field are also known as the DSCP (Differentiated Services Code Point). Note that setting this field will have no effect on the traffic QoS unless the routers in the path are configured to honor the value.

Output Tab–HLS

In HLS mode, the encoder creates HLS segments and manifest files, and posts them to a server. The server can be a local web server in the encoder itself, or it can be a remote server. If the server is remote, multiple protocols can be used to transfer the segments and manifest files.

The 9992-ENC supports SCTE-35 signaling on HLS outputs, and will terminate a segment early to ensure that the frame signaled by the SCTE-35 message is an IDR at the beginning of a segment. The SCTE-35 transport packet is always included in the bitstream. The 9992-ENC may optionally signal the SCTE-35 message in the HLS manifest.

HLS Common Parameters
The picture below shows the HLS parameters that are common to all modes:
- **Server Location:** selecting **Remote** configures the encoder to upload the segment and manifest files to a remote server. Selecting **Local** configures the encoder to place the segments in its local web server, where they are directly-accessible to clients.
- **Segment (sec):** Number of seconds per segment. This defines the approximate size (in seconds) for the above bitstream encoded files. The valid range is from 1 to 20 seconds. Note that the clients will experience latency approximately equal to the segment size times the number of segments.
- **Number of Segments:** This defines the number of bitstream segments advertised in the playlist. The minimum number, as per the HLS specification, is 3. Some set-top boxes require 4 segments. Apple devices (iPads, iPhones, etc.) work well with 3 segments.

- **Cue Manifest Mode:** The 9992-ENC can add the SCTE-35 signaling to the HLS manifest. This controls the format used in the signaling, as follows:
  - **None:** SCTE-35 messages are not added in the manifest.
  - **SCTE-35:** SCTE-35 messages are added to the manifest using the EXT-X-SCTE35 tag, as per SCTE-35 section 12.2.2.
  - **Cue-In/Cue-Out:** SCTE-35 splice messages are converted to Cue-In/Cue-Out markers in the manifest.
  - **Cue+Message:** SCTE-35 messages are converted to Cue-In/Cue-Out and also inserted in the manifest.
- **Program Name:** this is the program name that goes in the manifest. Most HLS clients ignore this information.

HLS Local Server

No additional configuration options are required for HLS Local Server. The URL to access the content is:

<div align="center">

http://encoder_ip_address/HLS/encoderX.m3u8

</div>

Where **encoder_ip_address** is the IP address of either one of the Ethernet ports, and **X** is the encoder channel number (1 to 4). For example, if the encoder is at 10.10.9.10, and Encoder 1 is configured for HLS, the URL will be:

<div align="center">
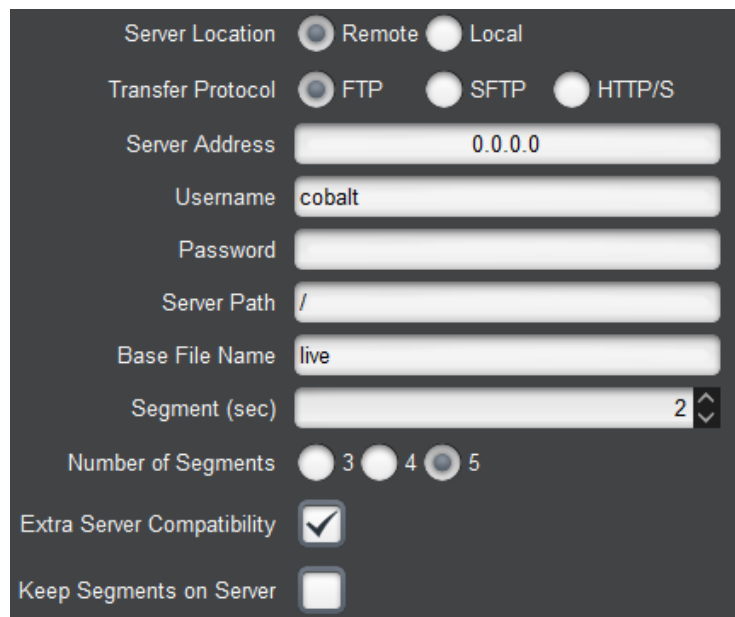
http://10.10.9.10/HLS/encoder1.m3u8

</div>

HLS Remote Server–FTP or SFTP Transfer

The specific parameters for this mode are:
- **Transfer Protocol:** This configures the protocol to be used between the encoder and the web server for uploading the files. The two options covered in this section are **FTP** and **SFTP** (Secure FTP). FTP exchanges data and password in the clear, while SFTP encrypts both flows.
- **Server Address:** Enter the IP address of the web server here. It needs to be reachable from either one of the encoder Ethernet ports.
- **Username:** Enter the username to be used when uploading the files to the server.

- **Password:** Enter the password corresponding to the user name, to be used when uploading the files.
- **Server Path:** Enter the absolute server path for the directory where the files should be placed. It is recommended that a separate directory be created for each encoder channel.
- **Base File Name:** Enter the base file name for the files created in the server. The encoder will create the following files:
  - **basename.m3u8:** This is the top playlist file. For the example above, where the base file name is **live**, the playlist file will be **live.m3u8**. This file will contain a single bit rate profile. It is created when the encoder starts, and not changed during operation. For backward compatibility with previous versions, a top playlist with a **.m3u** extension and identical contents will also be created.
  - **basename_p.m3u8:** This is the current playlist file for the encoder profile. It is updated every time a new segment is created.
  - **basename_XXXX.ts:** These will be the bitstream encoded files. XXXX is an increasing count. For the example above, the encoder will create files named **live_1.ts**, **live_2.ts**, **live_3.ts**, **live_4.ts**, and so on. At any given point in time, there will be five or six consecutive files in the configured directory if the encoder is configured to remove older files.
- **Extra Server Compatibility:** Check this box if the encoder has problems renaming files in the server. This is typically required for Windows FTP servers. Linux-based servers do not need this.
- **Keep Segments on Server:** Normally, when a segment falls out of the playlist file, it is automatically deleted by the encoder. If you check this box, the bitstream is left in the server. Clients will still start playing from the first segment in the playlist.

HLS Remote Server–HTTP/HTTPS Transfer

This mode uses HTTP PUT to transfer files to an HTTP server. The specific parameters for this mode are:

- **URL Entry Mode:** this controls the way the upload URL is specified. If set to **Single URL**, the full URL is entered in the **Upload URL** field. If set to **Split URL**, the **Upload URL** field becomes read-only and the following additional fields appear:

  In this mode, the 9992-ENC will construct the final URL by concatenating the **Upload URL Base** field with up to 3 arguments. These arguments must include the **=** sign to be accepted. The 9992-ENC will automatically include a **?** between the Upload URL Base and the arguments, and separate the arguments with the **&** sign. The final Upload URL is shown as well.

- **Upload URL:** this is the base URL to be used to upload the segment and manifest files. The 9992-ENC supports both **http://** and **https://** URLs. Host names can be used if the encoder is configured with a DNS server (see the Network Configuration DNS Tab). Note that, for **https://** URLs, the encoder **will not** authenticate the server – the protocol is being used to provide only encryption, not authentication.
- **Enable Host Header:** if this box is checked, the encoder will send an HTTP host header with each request. A new field will be presented here the contents of the host header can be entered:

- **Base File Name:** this field is the same as in HLS Remote Server–FTP or SFTP Transfer, and the same files will the transferred. The final HTTP URL will be the concatenation of the **Upload URL** field, the base file name, and the extensions described above.

Output Tab–RTMP

The 9992-ENC can operate as an RTMP client, and publish a real-time, live bitstream to an RTMP server. The 9992-ENC can generally connect to the same servers as the Adobe Flash Live Media Encoder (FMLE).

An RTMP server publishing point is defined by the following:

- An RTMP URL, of the form:

$$\texttt{rtmp[t][e][s]://servername/app}$$

- A stream name

The first part of the URL defines the protocol, as follows:
- `rtmp`: standard RTMP with no security
- `rtmpt`: RTMP tunneled over HTTP
- `rtmpe`: encrypted RTMP using proprietary security
- `rtmps`: encrypted RTMP over SSL
- `rtmpte`: encrypted RTMP using proprietary security, tunneled over HTTP
- `rtmpts`: encrypted RTMP over SSL, tunneled over HTTP

The `servername` field is the host name or IP address of the RTMP server to be contacted. The `app` field is the application in the server that should receive the data being transmitted. Note that, depending on the service, the `app` field may contain a complete path or even a set of parameters.

The 9992-ENC encoder can be configured with primary/backup RTMP servers. If it cannot connect to the primary server, it will automatically try the backup.

The RTMP configurable parameters are:

| Output Protocol | RTMP |
| RTMP Protocol | rtmp |

Primary Server

Primary Server	server.domain.com
Primary Network Interface	● Any ○ Ethernet 1 ○ Ethernet 2
Primary App	app/parameters
Primary Server URL	rtmp://server.domain.com/app/parameters
Primary Stream	livestream

Backup Server

Backup Server	backup.domain.com
Backup Network Interface	● Any ○ Ethernet 1 ○ Ethernet 2
Backup App	backup_app/backup_parameters
Backup Server URL	rtmp://backup.domain.com/backup_app/backup_parameters
Backup Stream	backup_livestream

Common Parameters

Redundancy Switch Time (sec)	10
Port Selection	● Use Default ○ Specific Port
Authentication	○ Yes ● No
Connect	● Yes ○ No

- **RTMP Protocol:** Select the protocol variant, as discussed above.
- **Primary Server:** Enter the host name or IP address of the primary (or single) RTMP server to be contacted. If you want to use host names instead of IP addresses, make sure to configure at least one DNS server. DNS servers may be configured in the Network Configuration DNS Tab.
- **Primary Network Interface:** Select the network interface to be used when contacting the primary server. The settings are:
    - **Any:** use the "best" network interface to connect to the server.
    - **Ethernet 1:** preferably use Ethernet 1 to connect to the server. If the server is not in the same subnet as Ethernet 1, and no default gateway is set for Ethernet 1, this setting will be ignored.
    - **Ethernet 2:** preferably use Ethernet 2 to connect to the server. If the server is not in the same subnet as Ethernet 2, and no default gateway is set for Ethernet 2, this setting will be ignored.
- **Primary App:** Enter the application name in the primary server, as discussed above. Consult your CDN or server documentation to find out what should be entered in this field.

- **Primary Server URL:** This informational field is automatically updated as you configure the RTMP parameters. It displays the full RTMP URL for the primary server.
- **Primary Stream:** Enter the stream name for the primary server. Consult your server documentation or CDN to find out what should be entered here. Some servers allow arbitrary stream names, while others use this field for authentication and thus require specific names.
- **Backup Server:** If you have a backup RTMP server, configure it here; otherwise, this field can be left empty. The encoder will only attempt to contact the backup RTMP server if it cannot establish a connection with the primary server.
- **Backup Network Interface:** Select the network interface to be used when contacting the backup server. The meaning of the choices is the same as the **Primary Network Interface** described above.
- **Backup App:** Enter the application name in the backup server. If this field is left blank, the value entered for **Primary App** is used.
- **Backup Server URL:** This informational field is automatically updated as you configure the RTMP parameters. It displays the full RTMP URL for the backup server.
- **Backup Stream:** Enter the stream name for the backup server. If this field is left blank, the value entered for **Primary Stream** is used.
- **Redundancy Switch Time (sec):** This field is only displayed if a **Backup Server** is specified (i.e., it will not be present if **Backup Server** is left blank). It sets the timeout for encoder to switch servers after the RTMP connection is established, if the server stops accepting data (i.e., when the **IP Output Rate** goes to zero).
- **Port Selection:** If your RTMP server is using the default TCP ports for the protocol variant, select **Use Default**. If your server is using a non-standard port, select **Specific Port**. When **Specific Port** is selected, an additional field is displayed:

- **Port:** This field is only displayed if **Port Selection** is set to **Specific Port**. Configure a non-standard TCP port here.
- **Authentication:** Some RTMP servers require username/password authentication for access. If your server does not require authentication, select **No**, otherwise select **Yes**. If you select **Yes**, additional fields are presented:

- **Username:** Enter the username to be used for authentication.
- **Password:** Enter the password to be used for authentication.

- **Connect:** This parameter controls whether or not the encoder should actually establish a connection with the server. If you set this parameter to **No**, the encoder will run but no data will be transmitted. This is useful to pre-configure a session, and turn it on later when it comes the time to broadcast.

Some CDNs only accept frame rates up to 30 fps and prefer progressive content. The 9992-ENC can convert any input signal to progressive at a lower bit rate (see Basic Tab–Encoder Configuration).

In RTMP Mode, the 9992-ENC will force Closed GOP operation (see Advanced Tab–Common Video Parameters).
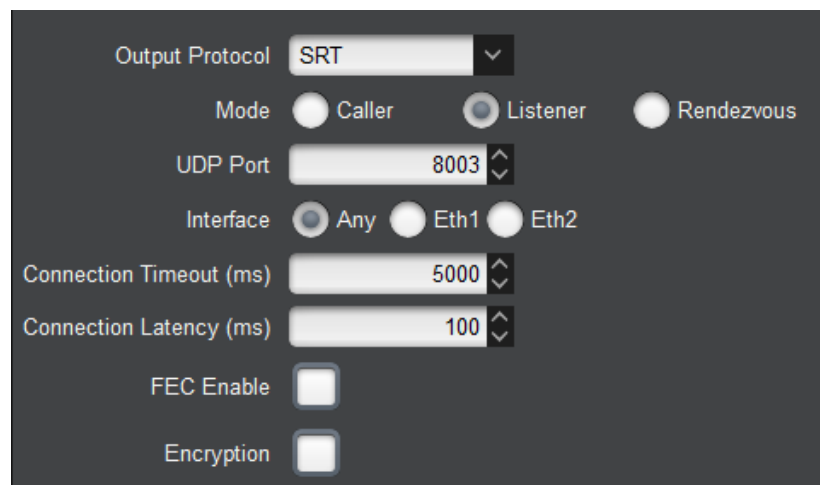
Output Tab–SRT

By virtue of being an encoder device, the 9992-ENC is always a sender. However, as far as the SRT connection is concerned, it can be a server ("listener"), waiting to be contacted by the receiver, or a client ("caller"), which explicitly starts the connection with the receiver. In either case, once the connection is established, the 9992-ENC will only send. The FEC settings and encryption key length are configured in the 9992-ENC and transmitted to the receiving device.

SRT supports a "rendezvous mode", where, **_under very limited situations_**, two SRT devices behind firewalls can connect to each other without firewall pre-configuration or port forwarding. For this mode to work, the firewall must not remap UDP source ports. Most modern firewalls **do** remap UDP source ports. The mode is included in Cobalt devices for extra compatibility but Cobalt Customer Support will not be able to assist if this mode does not operate, since it is highly dependent on the firewalls used on both sides of the connection.

SRT operation requires the +**SRT** optional license.

The user interface for SRT is found in the **Connections** tab and is displayed below:

- **Mode:** This selects between **Listener** (server), where the device will wait to be connected, **Caller** (client), where the device will explicitly connect to a sender, and

Rendezvous, where the device will attempt to connect to another device in rendezvous mode. If **Caller** or **Rendezvous** are selected, new fields will appear, as indicated below:
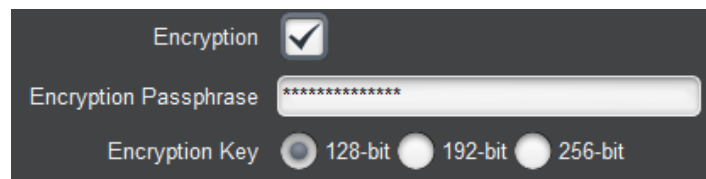
- o **Stream ID:** this is an arbitrary string sent from the caller to the listener, for identification purposes. In rendezvous mode, the Stream ID of one of the endpoints is arbitrarily selected for the connection.
- o **Server IP Address:** this is the IP address of the server ("listener") to be contacted.
- **UDP Port:** This is the UDP port to be used for the communication. If the decoder is a **Listener**, it will listen on this port for incoming connections. If it is a **Caller**, it will connect to this port in the server. In **Rendezvous** mode, the specified UDP port is used both to listen for connections and to contact the partner.
- **Interface:** The 9992-ENC has two streaming interfaces. You can restrict communication on one of them, or leave it to the 9992-ENC to choose the most suitable. In particular, if the decoder is a **Listener**, selecting **Any** will cause it to accept incoming connections on either one of the interfaces.
- **Connection Timeout:** This configures the amount of time the decoder will keep a connection open without any data. After the timeout, the connection is dropped and restarted.
- **Connection Latency:** This configures the incoming stream buffer. It should be a multiple of the round-trip time to the other endpoint.
- **FEC Enable:** If this box is checked, Forward Error Correction (FEC) is enabled. The following additional fields become available:

- o **FEC Mode:** the selections are **Row and Column**, **Column Only** and **Row Only**. **Row Only** FEC is only effective for occasional single packet losses. Column-based FEC (either **Row and Column** or **Column Only**) is effective for burst losses. Please refer to the SMPTE 2022 FEC discussion the 9992-ENC manual for more general details on FEC.
  - o **FEC Columns:** this selects the number of columns in the FEC matrix. The number of columns determines the maximum burst loss recoverable when column FEC is enabled.
  - o **FEC Rows:** this selects the number of rows in the FEC matrix. Note that this parameter is not displayed if **Row Only** is selected (because the number of rows is set to 1).
  - o **ARQ Type:** this selects how ARQ is combined with FEC. The options are **Enabled/Before FEC** (packet retransmissions are requested before FEC is applied), **Enabled/After FEC** (only packets not recovered by FEC are requested), and **Disabled** (the only packet recovery mechanism is FEC).
  - o **FEC Layout:** select between **Block Aligned** and **Non Block Aligned**. This parameter has a small impact in overall latency, but no impact in packet recovery.
- **Encryption:** Checking this box will enable encryption of the content. When the box is checked, additional fields appear:

- o **Encryption Passphrase:** Enter the encryption passphrase (minimum 10 characters). It must match the Passphrase at the receiver or communication will not be possible.
  - o **Encryption Key:** Select the encryption key length. Please note that encryption keys of more than 128 bits may not be legal in some countries.

Encoder Audio Configuration Tabs

Due to DashBoard limitations, audio configuration for each of the encoder channels is on a separate top tab. Each tab can contain up to two audio channels. These tabs automatically appear or disappear depending on the number of configured audio channels (see Basic Tab–Audio Parameters). This is illustrated below.

Encoder 2 Audio Channels 3 and 4

Encoder 1 Audio Channels 1 and 2   **Encoder 2 Audio Channels 1 and 2**

In this section, an "audio channel" is the same as an "audio PID", and it can be mono, stereo, or a 5.1 surround channel. The capabilities of the 9992-ENC are:

- Up to 16 total embedded audio pairs per card.
- Up to 8 total embedded audio pairs per video input.
- Up to 8 audio PIDs per encoder channel.

Note that a 5.1 Surround channel uses three embedded audio pairs.

The audio configuration tab is divided into two lower tabs, whose appearance is a function of the audio encoding standard. The 9992-ENC allows for any desired mix of audio encoding standards. The two lower tabs are the **Basic** tab, for the more common audio parameters, and the **Advanced** tab, for the audio advanced configuration parameters.

Audio Configuration Basic Tab

The appearance of the audio configuration basic tab is a function of the encoding standard, but some parts of it are common to all standards.

Audio Configuration Basic Tab – Common Parameters

The common parameters are shown below.
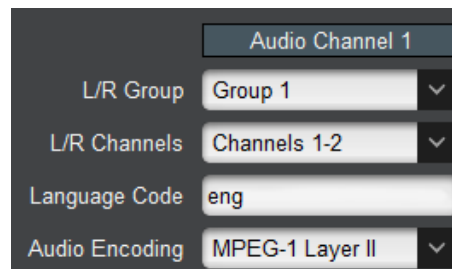
- **L/R Group, L/R Channels:** SDI embedded audio is typically divided into four groups (denoted by Group 1 to Group 4); each group has four mono channels (2 stereo pairs), denoted by Channels 1-2 and 3-4. These controls allow the selection of the desired group and channel pair. In the large majority of the cases, the first stereo pair is in Group 1, Channels 1-2, the second stereo pair is in Group 1, Channels 3-4, and so on. The **L/R Group** selection has one additional choice, labeled **Custom DID**. This allows the encoder to use a non-standard embedded audio DID (this quite uncommon). If **Custom**

73

DID is selected, a new configuration option becomes available, where the DID value can be entered:

- **L/R Group DID:** Enter the desired Group DID, in hexadecimal. As a reference, the table below contains the standard DIDs built into the system for Groups 1 to 4.
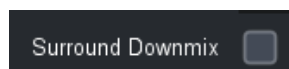
Group	SD-SDI DID	HD-SDI DID
Group 1	0x2FF	0x2E7
Group 2	0x1FD	0x1E6
Group 3	0x1FB	0x1E5
Group 4	0x2F9	0x2E4

Some compression standards support 5.1 Surround encoding. If these modes are selected, additional configuration options become available:

Each of the **Group/Channels** selectors operate as described above. The channels are identified as follows:
  - o **L/R:** Left/Right
  - o **C/LFE:** Center/Low Frequency Effects
  - o **Ls/Rs:** Left/Right Surround

- **Surround Downmix:** Surround Downmix to Stereo is offered for some audio encoding standards. If available, the following checkbox is presented:

If this box is checked, the 9992-ENC will downmix a 5.1 input into stereo prior to encoding, using LtRt.

- **Language Code:** This parameter represents the 3-letter ISO 639-2 language code for the audio, to be placed in the audio language descriptor in the PMT. For a complete list of the language codes, see this URL:
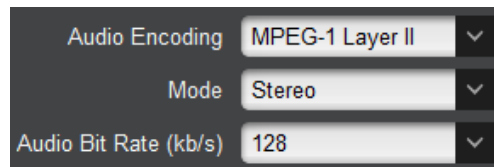
  http://www.loc.gov/standards/iso639-2/php/code_list.php

  If the Output Protocol in the Encoder Output Configuration Tab is set to RTMP, this field will not be displayed as RTMP does not use the transport stream container.

- **Audio Encoding:** This parameter selects the audio encoding algorithm. The choices are **MPEG-1 Layer II, AAC, Dolby, SMPTE-302M LPCM,** or **Dolby Pass-through.** Note that some options require additional licensing. If the Output Protocol in the Encoder Output Configuration Tab is set to RTMP, this field is forced to AAC-LC and becomes not editable. The reason is that the RTMP protocol has no support for MPEG-1 Layer II audio at 48 kHz sampling. It also has no support for Dolby or LPCM.

Audio Configuration Basic Tab – MPEG-1 Layer II
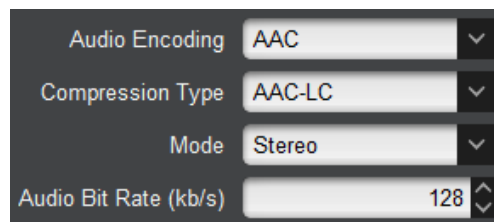
The MPEG-1 Layer II parameters are shown below.

- **Mode:** the choices are:
  - **Stereo:** standard stereo encoding.
  - **Mono:** mono encoding. The encoder only uses the left channel.
  - **Dual Channel:** works exactly the same as Stereo, but channels are internally labeled as 1 and 2 instead of Left and Right.
  - **Joint Stereo:** similar to stereo, but some frequency ranges are coded as mono to improve quality.
- **Audio Bit Rate (kb/s):** this is a drop-down menu of available rates. The choices will change between stereo and mono.

Audio Configuration Basic Tab – AAC
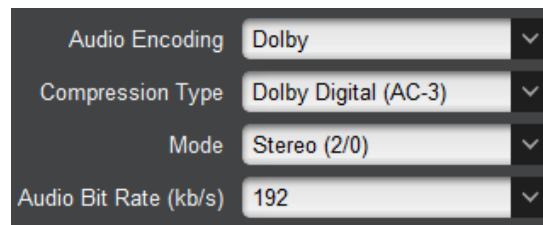
The AAC parameters are shown below.

- **Compression Type:** Select the type of AAC encoding. The options are **AAC-LC**, **HE-AAC V1** and **HE-AAC V2**.
- **Mode:** Select the number of channels. The options are **Mono**, **Stereo**, and **5.1 Surround**. Note that, if **Compression Type** is set to **HE-AAC V2**, this field becomes fixed at **Stereo**. In **Mono** mode, only the left channel is encoded.
- **Audio Bit Rate (kb/s):** Enter the desired bit rate. The encoder will not allow invalid bit rates to be entered.

Audio Configuration Basic Tab – Dolby
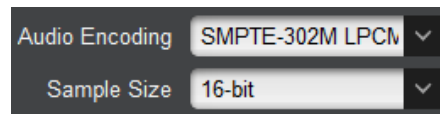
The Dolby parameters are shown below:

Audio Encoding	Dolby
Compression Type	Dolby Digital (AC-3)
Mode	Stereo (2/0)
Audio Bit Rate (kb/s)	192

- **Compression Type:** Select between **Dolby Digital (AC-3)** and **Dolby Digital Plus (EAC-3)**.
- **Mode:** Select the number of channels. The options are **Mono (1/0)**, **Stereo (2/0)**, and **5.1 Surround (3/2)**.
- **Audio Bit Rate (kb/s):** This is a drop-down of the valid bit rates for the selected mode.

Audio Configuration Basic Tab – SMPTE-302M LPCM

SMPTE-302M is technically not a compression standard – audio is carried as uncompressed Linear PCM samples. The options are:

Audio Encoding	SMPTE-302M LPCM
Sample Size	16-bit

- **Sample Size:** Select between 16-bit, 20-bit and 24-bit. The sample size defines the elementary stream audio bit rate, as follows:

Sample Size	Audio Bit Rate
16-bit	1,920 kb/s
20-bit	2,304 kb/s
24-bit	2,688 kb/s

Audio Configuration Basic Tab – Dolby Pass-through

Dolby Pass-through is a mode where audio comes pre-encoded in the SDI signal, and is simply passed on to the transport stream without any processing from the 9992-ENC, except for transport packetization. Dolby Pass-through does not have any additional parameters in the Basic tab. The 9992-ENC supports pass-through of the following signal types:
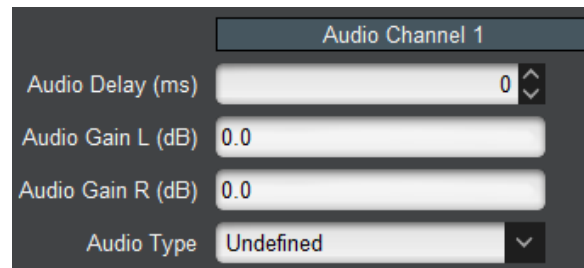
- Dolby AC-3
- Dolby EAC-3
- Dolby E

Audio Configuration Advanced Tab
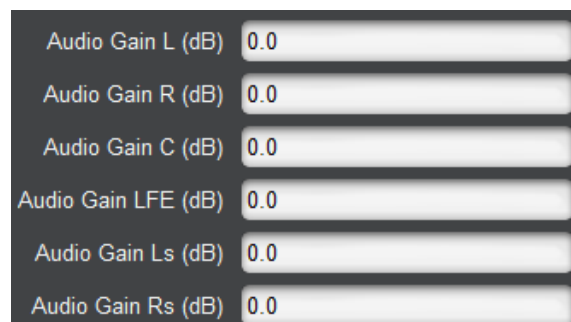
The appearance of the audio configuration advanced tab is a function of the encoding standard, but some parts of it are common to all standards.
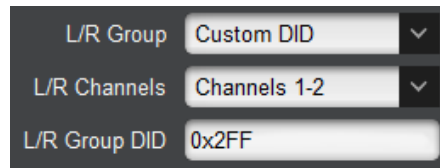
Audio Configuration Advanced Tab – Common Parameters

The common parameters are shown below.

- **Audio Delay (ms):** Use this to compensate for up to ±200 milliseconds of audio delay in the input signal. This setting will advance or delay the audio in relation to the video by the amount configured.
- **Audio Gain L/R (dB):** This control allows an independent gain adjustment for the left and right audio channels, from -18.0 dB to +18.0 dB, in steps of 0.5 dB. If this audio encoder channel is configured for 5.1 Surround operation, additional gain controls become available:

These controls are not available for Dolby Pass-through.

- **Audio Type:** determines the audio type in the PMT audio descriptor. This setting has no actual impact on how the audio is encoded; it only affects its description in the PMT. If the output protocol is RTMP, this control is not present since RTMP does not use the transport stream container. The choices are:
  - **Undefined:** no further information. This is the most common setting.
  - **Clean Effects:** indicates that the audio has no language.
  - **Hearing Impaired:** indicates that the audio is prepared for the hearing impaired.

77

o **Visual Impaired Commentary:** indicates that the audio is prepared for the visually impaired viewer.

Audio Configuration Advanced Tab – MPEG-1 Layer II

The MPEG-1 Layer II advanced parameters are shown below.
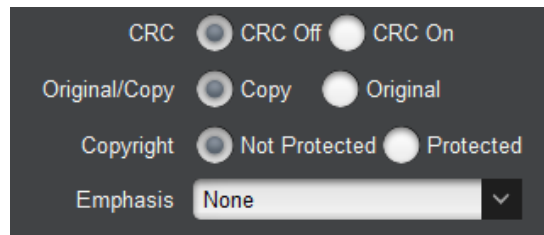
- **CRC:** Enables/Disables CRC insertion in the audio elementary stream. This is normally left disabled (CRC off).
- **Original/Copy:** Controls the state of the Original/Copy flag in the audio elementary stream. This setting does not affect the actual audio encoding.
- **Copyright:** Controls the state of the Copyright flag in the audio elementary stream. This setting does not affect the actual audio encoding.
- **Emphasis:** Controls the state of the Emphasis flags in the audio elementary stream. This setting does not affect the actual audio encoding. The available values are **None**, **50/15 us**, and **ITU-T J.17**.

Audio Configuration Advanced Tab – AAC

The AAC advanced parameters are shown below.
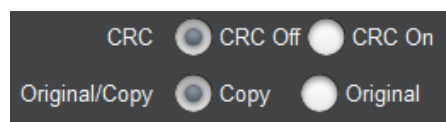
- **CRC:** Enables/Disables CRC insertion in the audio elementary stream. This is normally left disabled (CRC off).
- **Original/Copy:** Controls the state of the Original/Copy flag in the audio elementary stream. This setting does not affect the actual audio encoding.

Audio Configuration Advanced Tab – Dolby

The Dolby advanced parameters for Mono (1/0) and Stereo (2/0) operation are shown below.

- **Dolby PMT Type:** this parameter controls how Dolby AC-3/EAC-3 audio is signaled in the PMT. The two choices are:
  - **DVB:** Dolby Audio is signaled as per ETSI TS 101 154 Appendix C (stream_type 0x06 with the AC-3 or EAC-3 Descriptor from EN 300 468 annex D).
  - **ATSC:** Dolby Audio is signaled as per ATSC A/53 Part 3 (stream_type 0x81 for AC-3 and 0x87 for EAC-3). However, the 9992-ENC is currently unable to generate the ATSC AC-3 Descriptor; please contact Cobalt Digital if this is an issue in your network.
- **Dialog Normalization (dB):** Enter the value to align the average loudness to provide a consistent level. The default value for disc authoring or Internet is –31 dB and for broadcasting –24 dB (ATSC), –23 dB (EBU).
- **Line DRC:** Select the DRC (Dynamic range control) from drop-down menu; options are **None, Film Standard, Film Light, Music Standard, Music Light,** or **Speech**.
- **RF DRC:** Select from drop-down menu; options are **None, Film Standard, Film Light, Music Standard, Music Light,** or **Speech**.
- **Dolby Surround Mode:** Select from drop-down menu; options are **Not Indicated**, **Dolby Surround Disabled**, or **Dolby Surround Enabled**.
- **Original/Copy:** Controls the state of the Original/Copy flag in the audio elementary stream. This setting does not affect the actual audio encoding.
- **Copyright:** Controls the state of the Copyright flag in the audio elementary stream. This setting does not affect the actual audio encoding.

If the channel is configured for 5.1 Surround operation, the following additional parameters become available:

- **LFE Channel:** This control allows for the LFE channel to be disabled.
- **Dolby Surround EX Mode:** Select from drop-down menu; options are **Not Indicated, Dolby Surround EX Disabled,** or **Dolby Surround EX Enabled**.
- **LFE Low Pass Filter:** Select the check box to enable the LFE low-pass filter.
- **Surround 90-deg Phase Shift:** Select check box to enable a 90-degree phase shift in the surround channels.
- **Surround 3dB Attenuation:** Select check box to enable 3dB attenuation in the surround channels.
- **Downmix Preference:** Select from drop-down menu; options are **Not Indicated**, **Pro Logic**, and **Stereo**.
- **Lo/Ro Center Mix Level:** Enter the value of the left only/right only down-mix from a multi-channel to a two-channel output that is compatible for stereo or mono reproduction.
- **Lt/Rt Center Mix Level:** Enter the value of the left total/right total down-mix from a multi-channel to a two-channel output that is compatible for stereo or mono reproduction.
- **Lo/Ro Surround Mix Level:** Enter the value of the left only/right only down-mix from a multi-channel to a two-channel output that is Dolby Surround compatible.
- **Lt/Rt Surround Mix Level:** Enter the value of the left total/right total down-mix from a multi-channel to a two-channel output that is Dolby Surround compatible.

Audio Configuration Advanced Tab – SMPTE-302M LPCM

SMPTE-302M LPCM only includes the parameters indicated in Audio Configuration Advanced Tab – Common Parameters.

Audio Configuration Advanced Tab – Dolby Pass-Through

Since Dolby Pass-Through is pre-encoded, the audio level controls are not available. The only specific control is:

- **Dolby PMT Type:** this parameter controls how Dolby AC-3/EAC-3 audio is signaled in the PMT. The two choices are:
  - **DVB:** Dolby Audio is signaled as per ETSI TS 101 154 Appendix C (stream_type 0x06 with the AC-3 or EAC-3 Descriptor from EN 300 468 annex D).
  - **ATSC:** Dolby Audio is signaled as per ATSC A/53 Part 3 (stream_type 0x81 for AC-3 and 0x87 for EAC-3). However, the 9992-ENC is currently unable to generate the ATSC AC-3 Descriptor; please contact Cobalt Digital if this is an issue in your network.

The Apply/Cancel Buttons

The **Apply/Cancel** buttons are available at the bottom of the **Basic**, **Advanced**, and **Output** tabs, as well as every Audio **Basic** and **Advanced** tabs. These are not separate buttons – they are multiple instances of the same buttons, repeated on each screen for convenience. If no changes have been made to the settings, the **Apply/Cancel** buttons are grayed out; once any changes are made, they become available. Changes do not take effect until the **Apply** button is pressed. If you make changes but decide not to apply them, click on the **Cancel** button and the user interface reverts to where it was before. Once you click on the **Apply** button, the changes are implemented.

No changes to Apply   Configuration Changed

In general, most changes will cause the encoder channel to stop and start again, causing a brief (2-second) interruption to the stream. Changes to the following parameters are implemented on-the-fly, without stopping the encoder:

- Loss of Video Action and Flat Field settings in Basic Tab–Encoder Configuration.
- Any VBI/Ancillary data changes in Advanced Tab–VBI/Ancillary Data Insertion, except for enabling/disabling SMPTE-2038 or changing the SMTPE-2038 data rate.
- Audio Group, Channel, and Language Code in Audio Configuration Basic Tab – Common Parameters.
- Audio Gain and Audio Type in Audio Configuration Advanced Tab – Common Parameters.
- Transport Stream ID in Advanced Tab – Mux Parameters.
- Enable SDT and all the SDT parameters in Advanced Tab – Mux Parameters.
- Any connections made in the Output Tab–ASI/IP Streaming.

Encoder Statistics Tab

The Encoder Statistics Tab is divided into six lower tabs, as indicated below:

The Encoder Audio Statistics Tab is divided into two lower tabs, as indicated below:

The **Basic**, **Advanced** and **Output** tabs in the Encoder Statistics, as well as the **Basic** and **Advanced** tabs in the Encoder Audio Statistics, are direct equivalents of their configuration counterparts. They present the <u>current</u> value of each of the configuration parameters. When the **Apply/Cancel** buttons are grayed out, the contents of these tabs exactly match their configuration counterparts. When the **Apply/Cancel** buttons are active, configuration parameters have been changed. The current (running) encoder configuration can still be inspected in the statistics tabs, prior to clicking on the **Apply** button.

Encoder Statistics Status Tab

The **Status** Tab provides a summary of the status of the encoder. The variables displayed in this tab vary according to the encoder configuration.

Encoder Statistics Status Tab – Common Statistics

The following basic parameters are always displayed:

- **Encoder Status:** This gives the overall encoder status. Its values are:
  - 🟢 **OK**: The encoder is running normally.
  - 🟢 **Stopped:** The encoder has been manually stopped (see **Encoder State** in Basic Tab–Encoder Configuration).
  - 🔴 **Error:** The encoder should be running but it is not. This status will be briefly shown when the encoder is starting. The possible causes for this are:
    - The encoder has no input (check **Encoder Video Status**)
    - There is a mismatch between the video input signal and the encoder configuration. This can only happen if the encoder is configured for 4K and a non-4K signal is applied, or vice-versa.
- **Input Port:** This indicates the input port connected.

- **Encoder 1 Video Input:** This indicates whether the selected video input front-end is locked. This status is also reflected in the rear I/O panel LED next to the video input. The possible values are:
  - ⬤ **Locked**: The selected video input front-end is locked.
  - ⬤ **Unlocked:** The selected video input front-end is unlocked.
- **Signal:** If there is any recognizable video signal at the encoder video input, this field will indicate what type of signal the encoder is detecting. If no recognizable video signal is detected, this field will indicate **No signal**.
- **Transport Rate (b/s):** This indicates the overall transport rate, including NULL packets, coming out of the encoder subsystem. If you are connecting this encoder to an IP Output or ASI port in manual rate mode, the configured bit rate must be at least this value. If you are connecting this encoder to an IP Output with padding disabled, the actual rate will be lower than this value as the NULL packets will be stripped from it.
- **Video Rate (b/s):** This indicates the current video bit rate. It will normally match the configured video bit rate, except for when Adaptive Encoding is enabled in Output Tab–RIST settings. In this case, the video bit rate may change based on the reported network quality.

Encoder Statistics Status Tab – HLS Statistics

If the encoder channel is in HLS mode, the following additional statistics are displayed:

- **Output Rate:** this indicator reports the average transfer rate into the server, in bits/second, averaged over the last segment.
- **Encoder HLS Status:** this gives the overall status of the HLS connection. It has the following values:
  - ⬤ **OK**: The encoder pushing HLS segments normally to the server.
  - ⬤ **Waiting for Encoder:** The encoder is not attempting to connect to the HLS server because the encoding core is not running (i.e., the encoder is not generating bitstream). This can be because the encoder is explicitly stopped (**Encoder State** set to **Stopped** in Basic Tab–Encoder Configuration) or it has no valid input.
  - ⬤ **Transfer Error:** The encoder is running, but it is unable to transfer segments to the HLS server. Possible reasons are:
    - The encoder cannot contact the server.
    - The server is rejecting the segments due to misconfiguration.
    - There is a performance issue between the encoder and the server causing occasional transfer errors.
    - The server was specified as a host name, and the encoder cannot convert that to an IP address (i.e., no DNS, or server name misspelled).

Check the Admin Event Log Tab for more details.

- **HTTP Segments Transferred:** this indicator reports the number of bitstream segments successfully transferred so far.
- **HTTP Dropped Segments:** this indicator reports the number of segments dropped. A segment will be dropped if the previous segment has not been completely transferred when it becomes ready. A non-zero count here indicates that there is a performance problem between the encoder and the server – either in the network (not enough bandwidth) or in the server (not enough CPU power/disk bandwidth). If the segment size is small (3 seconds or less), increasing the segment size may improve the situation.
- **HTTP Transfer Errors:** this indicator reports the number of errors encountered while transferring segments. These may be network errors, or may be configuration errors.

Encoder Statistics Status Tab – RTMP Statistics

If the encoder channel is in RTMP mode, the following additional statistics are displayed:

- **Output Rate:** this field reports the average bit rate transferred to the server. It will be lower than the transport rate due to the lower container overhead used by RTMP. It is possible for the IP Output Rate to be less than the intrinsic bit rate of the encoder for short periods of time, depending on server and network conditions. The encoder will buffer the bitstream and attempt to "catch up" in these cases. If it cannot, audio/video bitstream data may be dropped.
- **Encoder RTMP Status:** This indicator reports the state of the RTMP connection to the server. The possible states are:
  - ○ 🟢 **Connected**: The encoder has established a connection with the RTMP server and is transferring data.
  - ○ 🟡 **Waiting for Encoder:** The encoder is not attempting to connect to the RTMP server. The reasons are:
    - The encoding core is not running (i.e., the encoder is not generating bitstream). This can be because the encoder is explicitly stopped (**Encoder State** set to **Stopped** in Basic Tab–Encoder Configuration) or it has no valid input.
    - The RTMP output is configured not to connect to the server (**Connect** set to **No** in the Output Tab–RTMP configuration section).
  - ○ 🔴 **Not Connected:** The encoder is running, but it is unable to connect to the RTMP server. Possible reasons are:

- The encoder cannot contact the server.
- The RTMP parameters are incorrect.
- The server was specified as a host name, and the encoder cannot convert that to an IP address (i.e., no DNS, or server name misspelled).

Check the Admin Event Log Tab for more details.

- **Server Connection:** RTMP can be optionally configured with a primary and a backup server. If the primary server cannot be contacted, the encoder will attempt to connect to the backup server. This field indicates which server (**Primary** or **Backup**) the encoder is currently connected or attempting to connect.
- **Video Buffer %, Audio Buffer %:** The encoder has separate buffers for audio and video. These buffers are used to temporarily store the bitstream if there is no enough network and/or server bandwidth. However, if this situation persists, the buffers start to fill up. These indicators report the current state of the buffers. If they overflow, data is dropped. Ideally, these buffers should stay empty (close to 0%).
- **Dropped Packets:** If the buffers overflow, data is dropped. The encoder will drop entire access units (an audio block or a video frame). This indicator has a count of the number of access units dropped for the current connection. This count resets when a new connection is established.

Encoder Statistics Status Tab – RIST Statistics

If the encoder channel is in RIST mode, the following additional statistics are displayed:

Field	Value
Output Rate (b/s)	4,986,512
Bitmask Requests	409
Range Requests	0
Retransmitted Packets	99
Packets Not Found	10381
Invalid NACK Requests	0
Requested Stream Not Found	1
Dropped Retransmissions	0
RTCP Received	2813
RTT Echo Received	41

- **Output Rate:** this field contains the measured total IP output payload bit rate, in bits/sec. It can be lower than the transport rate, if NULL packets are removed from the stream, or higher, if multiple destinations are enabled.
- **Bitmask Requests:** this field contains the number of bitmask retransmission requests received by the encoder.
- **Range Requests:** this field contains the number of range retransmission requests received by the encoder.

- **Retransmitted Packets:** this field contains the number of packets that have been retransmitted. It is possible that this number is higher than the number of retransmission requests because one request can ask for up to 17 packets.
- **Packets Not Found:** this field contains the number of packets whose retransmission has been requested, but are no longer in the encoder buffer. If this number grows, increase the NACK Window in the Output Tab–RIST configuration section.
- **Invalid NACK Requests:** this field contains the number of NACK requests deemed invalid or malformed. If this number is non-zero, please contact the receiver vendor.
- **Requested Stream Not Found:** each of the encoder output streams has its individual SSRC identifier. A non-zero count here indicates that the encoder received a request for an SSRC it does not have. The possible causes for this are:
  - The encoder has been rebooted, and received a request matching an old SSRC.
  - A network routing or forwarding problem caused the encoder to receive a request that was intended for a different encoder.
- **Dropped Retransmissions:** this field contains the number of packet retransmissions that were dropped due to the retransmission rate limit configured in the Output Tab–RIST section.
- **RTCP Received:** this field contains the number of RTCP packets received from the remote endpoints.
- **RTT Echo Received:** this field contains the number of RTCP RTT Echo requests received.

Encoder Statistics Status Tab – SRT Statistics

If the encoder channel is in SRT mode, the following additional statistics are displayed:

Transmit Rate (b/s)	6,628,213
Destination IP Address	10.10.9.12
Stream ID	Encoder 2
Encryption State	● Secured OK
Connection State	Connected
Encryption Key	192-bit
SRT Packets Sent	4610734
Retransmitted Packets	0
SRT Packets Lost	0
SRT Packets Dropped	0
RTT	0.5 ms
Estimated BW (b/s)	8,688,000

- **Transmit Rate (b/s):** this indicates the total output rate, including FEC overhead (if applicable).
- **Destination IP Address:** this indicated the IP address of the partner receiving the stream.
- **Stream ID:** indicates the current Stream ID. If the decoder is in **Caller** mode, this will be the Stream ID configured in the GUI. If it is in **Listener** mode, it will be the Stream

ID received from the remote end. If it is in **Rendezvous** mode, it will be the final selected Stream ID for the connection.

- **Connection State:** indicates the current connection state.
- **Encryption State:** indicates the current encryption state. This is an alarm and will be red in error conditions. The text indicates the exact condition.
- **Encryption Key:** indicates the current key size.
- **SRT Packets Sent:** indicates the number of data packets sent.
- **Retransmitted Packets:** indicates the number of retransmitted packets.
- **SRT Packets Lost:** indicates the number of packets lost reported by the receiver.
- **SRT Packets Dropped:** indicates the number of packets dropped at the sender.
- **RTT:** measured Round Trip Time to the receiver, in milliseconds.
- **Estimated Bandwidth (b/s):** indicates the bandwidth estimated by the SRT protocol. This is not the link bandwidth, which may be significantly larger.

Encoder Statistics Audio Tab

The **Audio** tab provides status information for the configured audio channels, as shown below:

- **Enc Audio Status:** this indicator will have the following values:
    - 🟢 **OK**: the selected audio is present and is being processed correctly.
    - 🟢 **Not Running**: the selected audio is not running yet. Audio does not run if the encoder is stopped. If the channel is configured for surround, it will show **LR Not Running.**
    - 🔴 **Not Present:** This indicates that the selected channel is not present in the SDI signal. If the channel is configured for surround, it may show **LR Not Present, CLFE Not Present,** or **LsRs Not Present.** If the channel is configured for Dolby Pass-Through, it may show **Invalid Passthru** if the signal is not recognized.
- **Info (dBFS):** this indicator shows additional information about the audio channel, as follows:
    - If the channel is a PCM channel, it will show the audio input level in dBFS. A silent channel will show -150 dBFS, as shown in Enc 1 Audio 3 above.
    - If the channel is a stereo PCM channel, it will show two levels, corresponding to L/R. If it is a surround channel, it will show six levels, corresponding to L/R/C/LFE/Ls/Rs.
    - If the channels is a pass-through channel and it is working correctly, it will show the signal type (AC-3, EAC-3 or Dolby-E) and the incoming bit rate, as shown in

Enc 1 Audio 2 above. If it there is no valid signal, it will show the word **Unlocked**.

Encoder Statistics Ancillary/VBI Tab

The **Ancillary/VBI** Tab provides the status of the ancillary data injection in the encoder. The variables displayed in this tab vary according to the encoder configuration; it will only include the ancillary data injection functions currently enabled (see Advanced Tab–VBI/Ancillary Data Insertion). Note that if no ancillary data processing is enabled, this tab will not be present.

- **Closed Captions:** This reports Closed Caption insertion. This field will report either **Present** or **Not Present**. If Closed Captions are reported as **Not Present**, the possible reasons are:
  - o If the caption source is EIA-608 Line 21, it means that the encoder cannot find a valid closed caption waveform on that line.
  - o If the caption source is SMPTE-334 VANC, it means that the encoder is either not receiving closed caption messages, or it is receiving EIA-708 messages without a caption field.

  Note that it is possible for the encoder to be receiving closed caption data that is empty (without actual captions). These will be reported as **Present**.
- **AFD:** This reports AFD insertion. This field will report either **Not Present** (if no AFD is being received) or **Code XXXX**, if AFD is being received; XXXX is the current AFD code being inserted. If AFD Source is set to Manual AFD Selection, this field will report the selected manual code.
- **HDR Metadata:** This field will report either **Present** or **Not Present**, depending on whether or not HDR metadata is being detect in the video signal.
- **SCTE 104 to SCTE 35 Injection:** this function includes the following three indicators in the tab:
  - o **SCTE 35 Packets Injected:** shows a count of how many SCTE 35 packets have been successfully injected in the transport stream for this encoder. Successful SCTE 35 injections are also logged, see the Admin Event Log Tab.
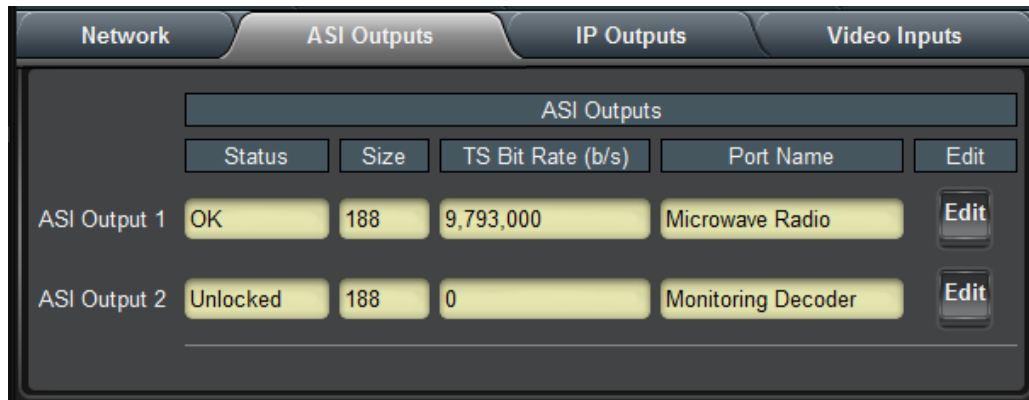
- o **SCTE 35 Packets Dropped:** if there are too many SCTE 104 messages, it may not be possible to insert all the SCTE 35 packets due to internal limitations in the 9992-ENC. The 9992-ENC can insert up to 10 SCTE 35 packets per second, which is sufficient for all usual ad insertion applications. If this indicator is nonzero, contact Cobalt Digital.
  - o **SCTE 104 Errors:** shows a count of SCTE 104 errors in the incoming signal. A nonzero count indicates that the device upstream of the 9992-ENC is non-compliant. Contact the vendor of that equipment.
- **SMPTE 2038:** this function includes the following two indicators in the tab:
  - o **SMPTE-2038 Injection Rate:** shows the current average injection rate for ANC packets carried using SMPTE-2038, over the last 2-second interval. This can be used to set the maximum injection rate.
  - o **SMPTE-2038 Packets Injected:** shows a running count of how many SMPTE-2038 transport packets have been injected since the encoder was last restarted.

ASI Outputs Tab

The 9992-ENC card has two ASI output ports that can be independently configured. Use this tab to configure and manage the ASI output ports.

ASI Ports: Configuration Tab

The default appearance of the Configuration tab is:

The **ASI Outputs** table contains the current configuration of the ports, as follows:
- **Status:** Indicates the port status. It can contain the following values:
  - **OK:** Port is operating normally.
  - **Unlocked:** Port is unlocked. This means that the port is in Automatic Bit Rate mode and it has no input.
  - **Overflow:** Transmit overflow. This means that the ASI Output is in Manual mode, and the configured bit rate is insufficient to carry the bitstreams connected to it. This situation will raise an alarm as packets are being dropped.
- **Size:** Indicates the configured transport packet size, in bytes.
- **TS Bit Rate (b/s):** This reports the actual transport stream bit rate, in bits/second.
- **Port Name:** This reports the user-configured Port Name.
- **Edit Button:** Clicking on this button allows configuration of the port. The ASI Output Configuration screen appears, with the settings for the selected port.

To configure an individual port, click on the **Edit** button for that port. The following configuration interface opens:

The configuration screen can be divided into two parts:
- ASI Output Parameters
- Input Selection Connection Parameters

The Connection Parameters are common to all outputs, and are described in the Connections Tab section, later in this document. The ASI Output Parameters are:
- **Port Name:** All 9992-ENC encoders and outputs can be assigned a user-defined **Port Name**. This name is used to identify the port later when making connections. Use any descriptive name suitable for your application, or accept the default.
- **Packet Size:** Select between 188 and 204 bytes.
- **ASI Rate:** The following two modes are available:
  - **Manual:** In this mode, the ASI output bit rate is set to the value entered in the **Bit Rate** field. The ASI output will maintain this rate at all times, as follows:
    - If there is no connection to the ASI port, or if the input connected to the ASI port is not active, the ASI port will transmit NULL packets.

- If the connected input bit rate is lower than the rate entered in the **Bit Rate** field, the ASI port will add NULL packets as required to pad it to the desired value. PCR packets will be re-stamped as required.
- If the connected input bit rate is higher than the rate entered in the **Bit Rate** field, the ASI port will attempt to remove NULL packets from the connected bitstream in order to achieve the desired value. PCR packets will be re-stamped as required. If there are not enough NULL packets to be deleted, packets will be dropped, and an alarm will be raised. This alarm will be indicated in the Dashboard™ **Card State** field, in the front Status LED, and in the ASI Statistics page.
  - o **Automatic:** If this mode is selected, the **Bit Rate** field disappears. The ASI output will exactly match the rate of the connected bit streams. However, if the connected ports have no data, or if there is no connection to the ASI port, there will be no output, and any connected downstream ASI device will indicate loss of sync. The ASI Statistics page will indicate this state, as well as the rear I/O panel indicator LED. Note that an alarm will only be raised if there is at least one connection to the ASI output.

- **Bit Rate:** This field is only available if the **ASI Rate** mode is set to **Manual**. Enter the desired ASI output bit rate here, in bits/second. The minimum value is 64,000 and the maximum value is 213,000,000.
- **Transport Stream ID:** This configures the Transport Stream ID field in the Program Association Table (PAT) coming out of this ASI port.
- **Original Network ID:** This field contains the Network ID code from which this program originated. This field accepts both hexadecimal (prefixed by 0x) and decimal values. Valid values are from 0 (0x0000) to 65535 (0xFFFF). The default value for this field is 0xFF01, which is in the range of values allocated for video over IP. The complete set of registered Network IDs can be downloaded from this URL:

    http://www.dvbservices.com/identifiers/export/original_network_id

    The Original Network ID field is carried in the Service Description Table (SDT). The SDT will be present in this ASI port only if any of the encoders connected to it have the SDT enabled.

Once the port is configured, click on the **Apply** button, and the configuration takes effect.

ASI Ports: Statistics Tab

The Statistics Tab for the ASI Ports provides a quick visual summary status for the ports. A sample, corresponding to the table example of the previous section, is depicted below.
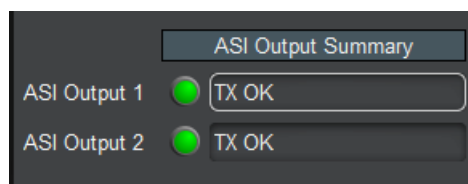
Each of the ASI Port indicators can have the following values:
- 🟢 **TX OK**: The port is operating normally in transmit mode (ASI Output).
- 🔴 **TX Overflow:** The connected bit rate is excessive. The Dashboard™ Card State will be red and the Status LED in the front of the board will also be red. To correct this problem, either reduce the connected bit rate, or increase the ASI output bit rate, or configure the port in Automatic mode. **If this alarm is active, data is being dropped.**
- 🔴 **TX Unlocked:** The port is in automatic bit rate, and there is no data rate coming to it. Any downstream ASI receivers will lose lock. Dashboard™ Card State and the Status LED will be red if there is a connection to this port.

IP Outputs Tab

IP Outputs receive data from connected inputs, format this data for transmission over UDP/IP, and send it with very precise timing over the Ethernet ports. The 9992-ENC card supports up to 4 transport stream outputs per Ethernet port. IP Outputs have the following specifications:
- Formats supported:
  - MPEG-2 Transport Packets over UDP/IP
  - MPEG-2 Transport Packets over RTP/UDP/IP
- Number of MPEG-2 Transport Packets per UDP datagram: fixed at 7.
- Addressing support: unicast, multicast and broadcast.
- Advanced control over the IP header fields available.
- SMPTE 2022 FEC available with the optional **+SMPTE2022** license. The 9992-ENC supports one FEC session per Ethernet port.

IP Outputs: Configuration Tab

IP output stream can be created, configured, and removed using this configuration area. Before any streams are created, the Configuration Tab appears as depicted below:
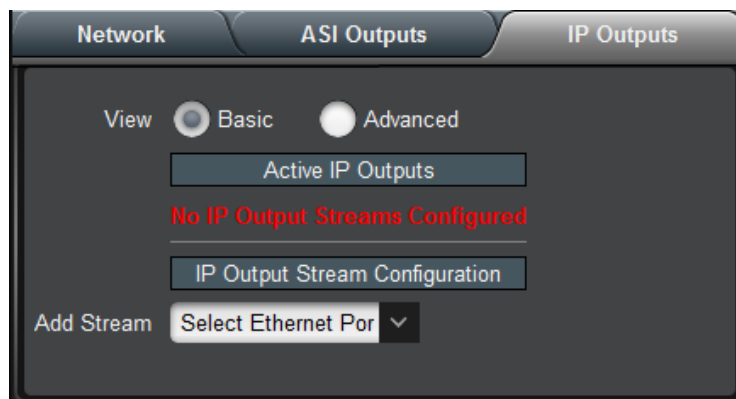
To create an IP Output stream, first select the desired Ethernet port in the **Add Stream** drop-down box. Once that selection is made, the IP Output Stream Configuration is displayed, as depicted below (Basic View). The configuration screen has two areas:
- **IP Output Parameters:** these are the parameters specific to the IP Output configuration. The set of parameters available for configuration depends on the **View** selection. In the **Basic** view, suitable default values are entered for the advanced parameters.
- **Input Selection Connection Parameters:** these allow a connection to be made to the output stream.
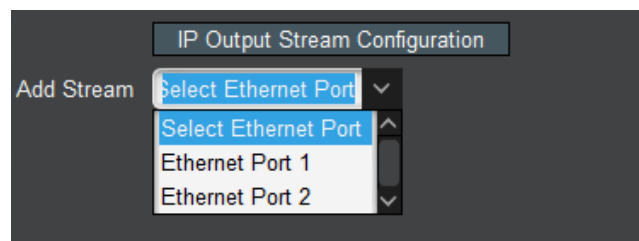
The Connection Parameters are common to all outputs and will be described in the Connections Tab section, later in this document.

The Basic View configuration parameters are as follows:
- **Enabled:** This allows the output stream to be enabled or disabled. If it is disabled, no packet transmission takes place. This feature is provided for testing purposes (i.e., temporarily disable an output for fault-finding). Most users will leave the stream enabled.
- **UDP Port:** Selects the UDP destination port. Valid values are between 1 and 65535. Note that, in traditional IP networks, UDP ports between 1 and 1023 are reserved for administrative uses. It is recommended to use UDP ports 1024 and higher. The 9992-ENC, however, will accept any legal value. Note that if the port is configured for RTP, the UDP port must be an even number, and the 9992-ENC interface will enforce this restriction – odd numbers will be automatically rounded up.
- **Destination Address:** Selects the IP address to transmit to. Any unicast or multicast address can be entered here, with the exception of the loopback range (127.0.0.0 to 127.255.255.255). The 9992-ENC will also accept the broadcast IP address of

255.255.255.255, and will transmit the packets as Ethernet broadcasts. Use of broadcasts, however, is strongly discouraged.

- **Stream Name:** All 9992-ENC input and output ports can be assigned a user-defined name. This name is used to identify the stream later when making connections. Use any descriptive name suitable for your application, or accept the default.
- **RTP:** If this box is checked, the device will include RTP (Real Time Protocol) headers in the output flow. If it is not checked, the transport stream will be sent over UDP/IP without any additional headers. Note that RTP requires the use of even UDP port numbers; when this box is checked, the user interface will enforce this restriction. The device will not generate RTCP packets.
- **SMPTE 2022 FEC:** The device supports SMPTE 2022 FEC in one stream per Ethernet interface. If no streams are currently configured for SMPTE 2022 FEC, this box will be displayed. If it is not displayed, then another stream is already using the feature. Check this box to enable transmission of SMPTE 2022 FEC packets for this stream. Note that SMPTE 2022 requires the use of RTP; checking this box will cause the RTP box to be checked as well.
- **NULL Padding:** This setting controls whether or not NULL packets are transmitted, making the stream completely CBR. IP networks are inherently VBR, and do not require NULL packets (which carry no information). However, the decoders may need them. The following is a good set of rules for deciding whether or not to send NULL packets:
    - If all your decoders are consumer IP set-top boxes or PCs running software decoders, NULL packets can be disabled.
    - If your decoders include professional IRDs, NULL packets must be enabled. The great majority of professional IRDs will not work without them.
    - If you are generating an MPTS (routing both encoders to the stream), enable NULL packets. An MPTS without NULL packets is technically illegal as per ISO/IEC 13818-1, but some systems support it.
    - If you are not sure about what kind of decoder will be receiving the stream, enable NULL packets.

This control offers the following options:

- **Disabled:** NULL packets are disabled and will not be transmitted. This will cause the stream to be somewhat VBR, even if the encoder is set to CBR mode.
- **Enabled – Automatic Rate:** This setting enables NULL packets, but the bit rate is automatically set by the 9992-ENC to the minimum suitable value. This is the recommended setting. If you later reconfigure an encoder connected to this stream, the rate will be automatically adjusted.
- **Enabled – Manual Rate**: This setting allows you to specify the overall stream bit rate. If you specify the bit rate, it must be high enough to support the connected encoders (i.e., it must be at least equal to the sum of the connected encoders' **Transport Rate**, found in each encoder **Status** tab). Specifying a rate that is not high enough will cause the IP Output to drop packets. Note that if this option is selected, the IP Output will be transmitting continuously at the selected bit rate, regardless of connections or the state of the encoders. If there is no connection to the IP Output, it will transmit only NULL packets; if there are connections and the encoders are stopped, it will transmit NULL packets plus (P)SI tables.

If the Advanced View is selected, additional parameters are available for configuration:

- **UDP Source Port Mode:** This parameter allows the UDP Source Port to be configured. The UDP Source Port is typically irrelevant for operation, as the 9992-ENC will not be listening for return traffic. This control is provided for traffic identification purposes if that is required. The options are:
  - **Same as Dest Port:** If this is selected, the UDP source port will be set to the same value as the destination port. This is the behavior of previous 9992-ENC firmware versions.
  - **Manual Selection:** This setting allows for configuration of the UDP source port. If this option is selected, the following entry becomes available:

- **UDP Source Port:** Enter the desired value for the UDP Source Port. Valid values are between 0^5 and 65535.
- **TOS:** This parameter allows the configuration of the Type-Of-Service (TOS) byte in the IP header (also known as the Differentiated Services – DS – field). Valid values are between 0 and 255. Configuring this is only useful if the downstream router is configured to honor the field.
- **TTL:** This parameter allows the configuration of the Time-To-Live (TTL) byte in the IP header. Valid values are between 0 and 255. If not explicitly configured, it defaults to 128. This field controls how many hops the packet can traverse before it is dropped by a router. The default value of 128 is suitable for virtually all applications.
- **DF Bit:** This parameter allows the configuration of the Do-not-Fragment (DF) bit in the IP header. The 9992-ENC will never produce fragmented packets, and with the UDP payload set to 7 transport packets, the IP packets are guaranteed to fit inside the Ethernet MTU. This control is provided for compatibility with legacy switches/routers. Some legacy equipment may exhibit performance problems if this bit is not set. This is not an issue with current network equipment.

SMPTE 2022 FEC Support

The 9992-ENC supports one FEC session per Ethernet port. A checkbox for **SMPTE 2022 FEC** will be displayed if the feature is available. Once this feature is enabled for one of the streams in a given Ethernet port, the checkbox will no longer be displayed.

Once the **SMPTE 2022 FEC** box is checked, additional parameters become available for configuration:

- **FEC Mode:** If you select **Column Only**, the 9992-ENC will send a single FEC flow, corresponding to the column protection data, using a UDP port number corresponding to the media UDP port number plus 2. If you select **Row and Column**, the 9992-ENCwill send two FEC flows, the first corresponding to the column protection data, and the

---

[5] RFC 768 allows the UDP Source Port to be zero, in cases where the device does not expect replies to the packet.

second corresponding to the row protection data. The row protection data will be sent using a UDP port number corresponding to the media UDP port number plus 4. Note that not all receivers support Row and Column mode; such receivers will only use the FEC Column data and discard the FEC Row data.

- **Columns:** Number of columns in the FEC matrix. This variable must be between 1 and 20 if **FEC Mode** is set to **Column Only**, and between 4 and 20 if it is set to **Row and Column**.
- **Rows:** Number of rows in the FEC matrix. This variable must be between 4 and 20.
- **FEC Overhead:** This field is updated as configuration is entered, and contains the overhead for the selected FEC configuration. Note that not all parameter changes cause the overhead to change. The FEC overhead is the sum of a Column overhead and a Row overhead (which is zero if **FEC Mode** is **Column Only**). The overhead is a function of the settings, as follows:
    - o **Increasing** the number of columns **decreases** the Row overhead (if enabled) and **does not change** the Column overhead.
    - o **Increasing** the number of rows **does not change** the Row overhead and **decreases** the Column overhead.
    - o **Decreasing** the number of rows and columns has the opposite effect as the previous items.

The following constraints apply to the FEC function:
- The number of rows must be between 4 and 20.
- The number of columns must be between 1 and 20 for Column Only mode, or between 4 and 20 in Row and Column mode.
- The size of the FEC matrix (product of the number of rows and the number of columns) must not exceed 100.

The user interface will not allow invalid configurations to be entered, and will automatically make parameter adjustments as required. Examples:
- If you select Row and Column, and the number of columns is less than 4, it will be automatically adjusted to 4.
- If your number of rows is 10, and you set the number of columns to 20, the number of rows will be automatically reduced to 5.

The number of rows and columns should be selected based on some understanding of the packet loss characteristics of the network between the 9992-ENC and the receivers. If you have no statistics on packet loss, the recommended setting is 20 columns and 5 rows to maximize the correction capabilities. Most receivers that support SMPTE 2022 FEC provide packet loss/recovery statistics. After running for a while, if the network is found to be clean, consider reducing the matrix to 10 rows and 10 columns, which will reduce the overhead.

Completing the Configuration

Once the configuration information is filled in, click on the **Apply** button to make it active. If there are no errors, the stream will be created, and the configuration area disappears. If any errors are detected, they will be displayed at the top of the **Apply** button.
The following configuration-related errors are flagged:

- ***Error: UDP Port/Address conflict with Port X/Y***: you have configured two IP Output streams with the same destination IP Address and UDP port, on the same Ethernet interface. Please review your settings. Note that ports with FEC enabled will use either two or three UDP ports (depending on the FEC settings) – these are checked as well.
- ***Maximum number of streams exceeded on this port***: you will receive this message if you attempt to create more than 4 IP outputs on a given Ethernet port.
- ***Error: No SMPTE 2022 FEC License Available***: the SMPTE 2022 function requires licensing. Please contact Cobalt Digital to obtain a license.

If the configuration is successful, the output stream will be added to the Active IP Outputs table.

Active IP Outputs Table

Once the output is created, it is added to the **Active IP Outputs** table, which has **Basic** and **Advanced** views. This table provides a summary of the configuration and status of the output stream. An example of this table, in the Basic view, is depicted below.

	Enabled	TS Bit Rate(b/s)	UDP Port	Destination Address	RTP	FEC	Stream Name	Edit Stream	Delete Stream
Stream 1/1	Yes	7,897,000	1026	225.1.1.1	Yes	20X5 R-C	MPTS Multicast FEC	Edit	Delete
Stream 1/2	Yes	0	1025	10.10.9.55	No	Off	Disconnected Port	Edit	Delete
Stream 2/1	Yes	3,412,000	5502	10.10.9.29	No	Off	SPTS Unicast From Enc1	Edit	Delete
Stream 2/2	No	0	1025	225.1.2.2	No	Off	Disabled Port	Edit	Delete
Stream 2/3	Yes	4,485,000	1026	225.1.2.3	Yes	4X4 C	Column-Only FEC	Edit	Delete

The Basic view includes the following:
- **Enabled:** The configured value of this parameter.
- **TS Bit Rate (b/s):** This column provides the current bit rate of the output transport stream. This does not include UDP and IP overhead, nor RTP/FEC overhead.
- **UDP Port:** The configured value of this parameter.
- **Destination Address:** The configured value of this parameter.
- **RTP:** The configured value of this parameter
- **FEC:** Summary of the FEC configuration. If FEC is disabled, this field will indicate it as **Off**. If FEC is enabled, this field will indicate the FEC matrix size as Columns × Rows, and the protection mode as **C** for Column Only or **R-C** for Row and Column. In the example above, Stream 2/3 has Column Only FEC with 4 Columns and 4 Rows, and Stream 1/1 has Row and Column FEC with 20 Columns and 5 Rows.
- **Stream Name:** The configured stream name.

- **Edit Stream:** If you click on this button, you can modify all the parameters for this output. The configuration area will re-open with the current output settings.
- **Delete Stream:** If you click on this button, the stream is deleted and removed from the table.

When the Advanced view is selected, additional fields appear in the table, as depicted below:

	Enabled	Line Bit Rate(b/s)	Null Padding	UDP Port	Src Port	Destination Address	TOS	TTL	DF	RTP	FEC	Destination MAC	Stream Name	Edit Stream	Delete Stream
Stream 1/1	Yes	10,390,315	Auto	1026	1026	225.1.1.1	0	128	Set	Yes	20X5 R-C	01005e010101	MPTS Multicast FEC	Edit	Delete
Stream 1/2	Yes	0	Auto	1025	3000	10.10.9.55	0	128	Set	No	Off	Unknown	Disconnected Port	Edit	Delete
Stream 2/1	Yes	3,552,006	Auto	5502	5502	10.10.9.29	0	128	Set	No	Off	ac83f00203ff	SPTS Unicast From Enc1	Edit	Delete
Stream 2/2	No	0	Auto	1025	1025	225.1.2.2	0	128	Set	No	Off	Disabled	Disabled Port	Edit	Delete
Stream 2/3	Yes	5,901,046	Auto	1026	6600	225.1.2.3	25	128	Set	Yes	4X4 C	01005e010203	Column-Only FEC	Edit	Delete

The Advanced view includes all items in the Basic view plus the following:
- **Src Port:** The current UDP Source Port being used for transmission.
- **Line Rate:** This column replaces the **TS Rate** column in the Advanced view. It indicates the actual Ethernet line rate for the stream, including the MAC, IP, UDP, RTP and FEC overheads.
- **Null Padding:** The configured value of this parameter (shown as **No**, **Auto**, or **Manual**).
- **TOS:** The configured value of this parameter.
- **TTL:** The configured value of this parameter.
- **DF:** The configured value of this parameter.
- **Destination MAC:** The destination MAC address for this IP Output. For multicast destination addresses, this is derived from the destination IP address using the rules from RFC 1112. For unicast destination addresses, this is obtained using ARP. If this entry is the word **Unknown**, the 9992-ENC has failed to obtain a destination MAC address. The IP Output is **not** streaming. A more detailed description of the unicast MAC address algorithms used in the 9992-ENC is presented below.

Managing Unicast MAC Addresses

When the 9992-ENC is configured with a unicast destination address, it needs to obtain a corresponding MAC address (corresponding to either the final destination, if it is in the same subnet, or to the default gateway). These MAC addresses are obtained using ARP. The 9992-ENC uses a custom MAC address management algorithm, designed specifically for MPEG operation.

When an IP Output stream with a unicast destination address is created, the 9992-ENC immediately starts attempting to obtain a MAC address for it, using standard ARP requests. These requests are issued every two seconds until answered. No packets will be transmitted on

that IP Output until a MAC address can be obtained. Note that this process will happen even if the stream is configured to be in the disabled state.

Once a MAC address is obtained, the 9992-ENC will cache it for about 5 minutes, as is usual for IP devices. Unlike other IP devices, the 9992-ENC will keep on using the MAC address until a response is received, to avoid stream interruptions. If no response is received at that time, the 9992-ENC will raise a yellow alarm. This alarm can be seen in the IP Output Statistics tab, described in detail below.
The current state of the 9992-ENC current streaming ARP cache is available in the Advanced View of the Active IP Outputs table, described above.

IP Outputs: Statistics Tab

The Statistics tab for the IP output ports contains a summary of each stream status. There are two sub-tabs: one for Port 1, and another for Port 2. The tab is depicted below:

Ethernet Port 1   **Ethernet Port 2**
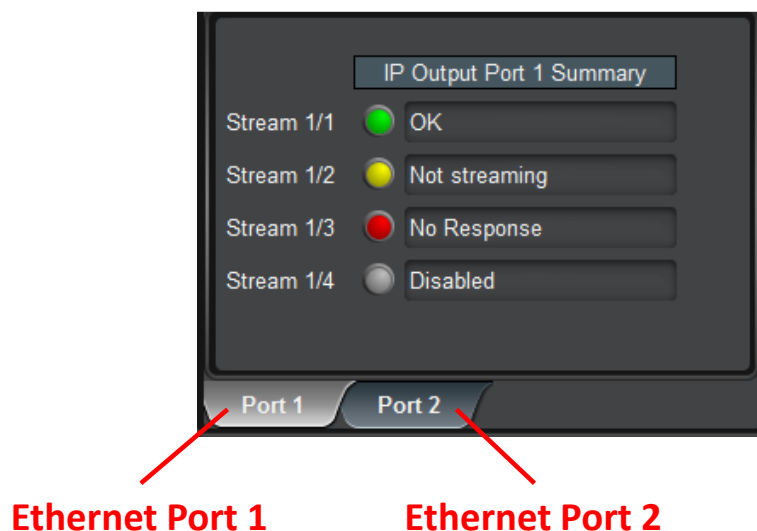
The indicators can have the following values:
- 🟢 **OK**: The IP Output is operating normally (either streaming or ready to stream).
- 🔴 **No Response:** The IP Output is configured for unicast operation, but it does not have a destination MAC address. If there is a connection to this output, Dashboard™ Card State and the Status LED will be red.
- 🔴 **Overflow:** The IP Output is configured for NULL Padding with a manual rate, and the connected bitstream(s) exceed that configured manual rate. If this alarm is asserted, *packets are being dropped*. The Dashboard™ Card State and the Status LED will be red.
- 🟡 **No Response:** The IP Output is configured for unicast operation, and the destination stopped responding to ARP. The IP Output is using an old cached MAC address. If there is a connection to this output, the Dashboard™ Card State will be yellow (but packets are being transmitted).

- ● **Not Streaming:** The IP Output is in automatic rate mode, and the connected encoder channel(s) are not running. The port is ready to transmit, but there is no stream available. No transmission is currently happening.
- ● **Disabled:** The IP Output has been disabled (by setting **Enable** to **No**).

Connections Tab

The Connections allows the creation, deletion, and management of input-output connections. The Statistics tab includes all connected input/output status indicators and an overall summary status indicator, which allows the operator to immediately pinpoint errors.

Connections Configuration Tab

The Connections configuration tab is depicted below. The message "No Connections" will be displayed if there are no configured input/output connections in the 9992-ENC.
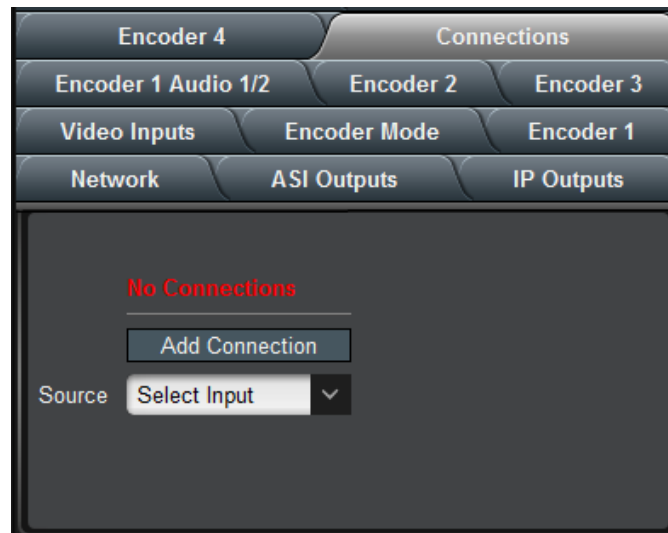
To establish a connection, simply select a source and a destination, and then click on Apply.

Source Selection

There are six sources in the 9992-ENC:

- Up to four Encoder channels (described in the Encoder 1-4 Tabs section)
- Two Test Packet Generators (described in the Admin Test Packet Generator Tab section)

The connection process starts by selecting one of these data sources, using the **Source** drop-down menu:
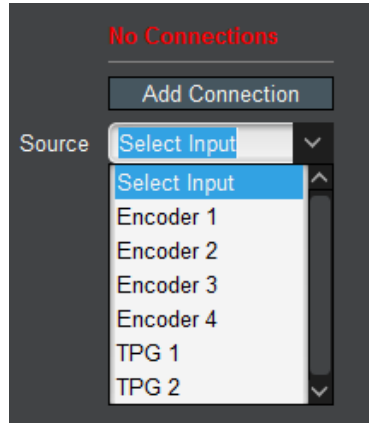
Once a source is selected, a list of available destinations is presented.

Destination Selection

The list of available destinations always includes all the defined IP Output ports, as well as the two ASI ports. This interface is also available if you select ASI/IP Streaming in the Output Tab–ASI/IP Streaming, and in the Admin Test Packet Generator Tab. If **Stream Display** is set to **Stream Names**, the user-defined names are presented. This is displayed below.
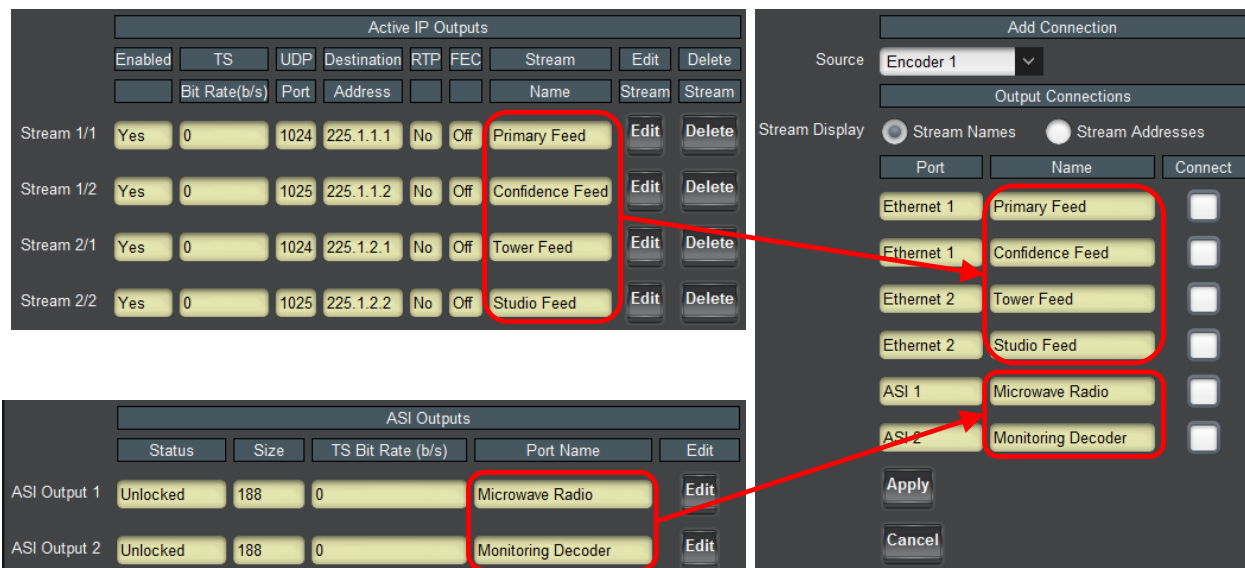
If you would prefer to make the output selection by Destination Address and UDP Port, set **Stream Display** to **Stream Addresses**; this option is illustrated below.
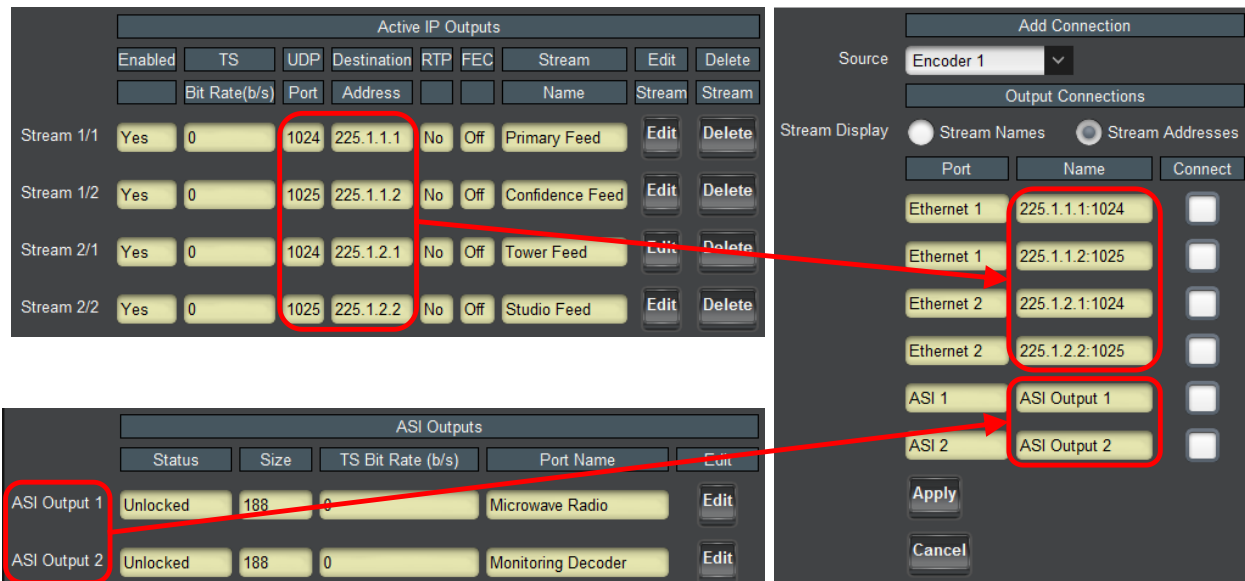
To make the connections, simply check the **Connect** box in front of the input you wish to use. You can connect any source to as many outputs as you wish. Conversely, unchecking the box disconnects that particular source-destination pair. Two examples are shown below:
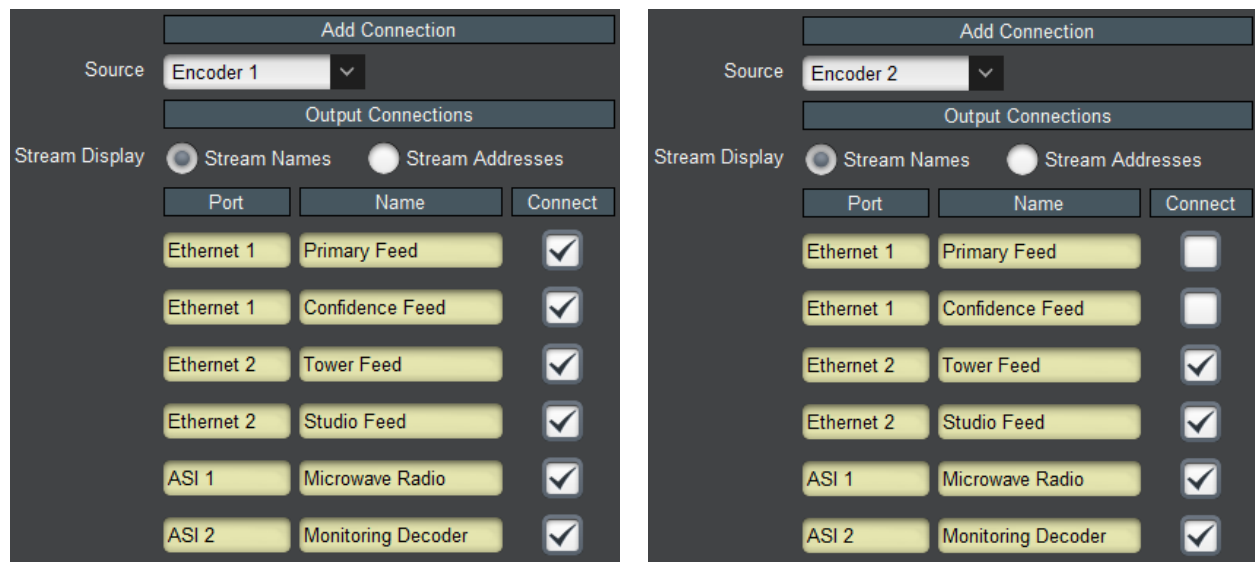
Source Selection in the Output Ports

When configuring an output (ASI or IP), connections can be immediately made as well, in that output's configuration interface (see ASI Ports: Configuration Tab and IP Outputs: Configuration Tab). The selection parameters are depicted below. The user-defined names for the Encoders (and Test Packet Generators) are displayed in the user interface to facilitate identification. To make the connection, just click on the corresponding checkbox under **Connect**. Encoders configured for RIST, RTMP and HLS are not available for connection and will not be shown in the list.
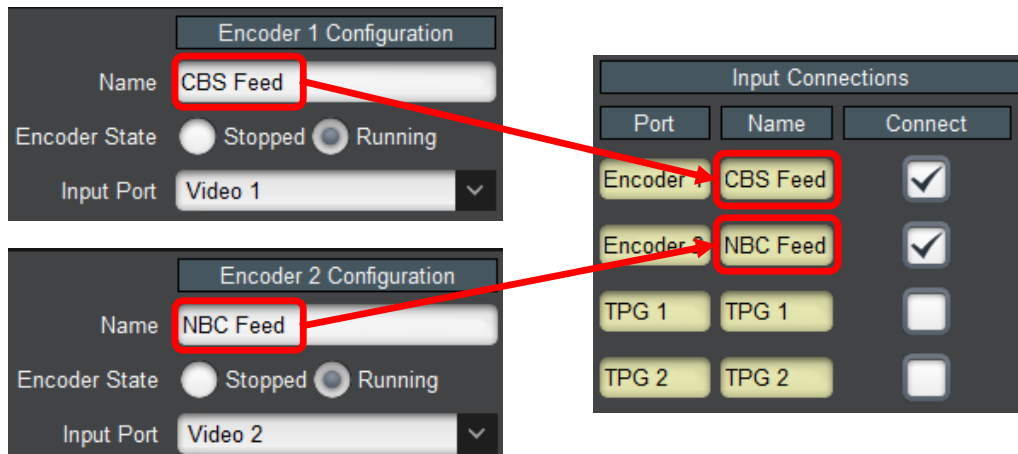
The Established Connections Table

As connections are established (either in the Connections tab, or as part of the source or output configuration), they are added to the Current Connections table. Regardless of how they got added, the connections can be managed using the functions in this table. A sample is depicted below.

The following columns are available in this table:
- **Source Port:** this column indicates the physical port of the connection. The possible values are **Encoder 1** through **Encoder 4**, **TPG 1** and **TPG 2**.
- **Source Name:** this column contains the user-defined name for the source.
- **Output Port:** this column indicates the physical output port for the connection. The possible values are **Ethernet 1**, **Ethernet 2**, **ASI 1** and **ASI 2**.
- **Output Name:** If the **Stream Display** control at the top of the table is set to **Stream Names**, this column will have the user-defined name for the output. If it is set to **Stream Addresses**, it will have the destination IP address and UDP port for IP Outputs, and the values **ASI Output 1** and **ASI Output 2** for the ASI ports.
- **Delete:** if you click on this button, the corresponding connection will be deleted.

Notes on Multi-Program Transport Stream Creation

If multiple encoders are connected to a given input, the 9992-ENC will automatically produce a Multi-Program Transport Stream (MPTS). Since the PIDs and Program Numbers can be set arbitrarily in each encoder, it is possible to select the same values for one or more of these parameters between the various encoder instances. However, when the bitstream from the encoders is multiplexed into one MPTS, these values have to be distinct.

When building the MPTS, the 9992-ENC will use the configured values for each encoder if possible. However, if there are any conflicts, the following rules are employed:

1. Whenever here is a PID or program number conflict, the settings for the lowest-numbered encoder connected to the MPTS take precedence. For example, if all four encoder instances are connected to a given port, the following will happen:
   - Settings for Encoder 1 will be taken unchanged.
   - Settings for Encoder 2 that do not conflict with Encoder 1 will be taken unchanged. Settings that conflict will be changed as little as possible so that they do not conflict. For example, if both encoders use PID 0x100 for video and 0x101 for PCR, Encoder 1 will retain PIDs 0x100 and 0x101, and Encoder 2 will use 0x102 and 0x103 (as long as these are not used by Encoder 1).
   - Same process is then applied to Encoder 3, and then Encoder 4.
2. Program number conflicts are resolved in the same manner.
3. These changes are specific to the particular output. They do not affect the PID mappings for other outputs. For example, if the four encoders go out on some output, and the PIDs for Encoder 4 are remapped on that MPTS, if Encoder 4 goes out on an SPTS in another port, its original PIDs are used.
4. The four encoder instances default to non-conflicting PID and program assignments. If full control of the PIDs is desired, non-conflicting PID sets should be selected. Encoder PID assignments are found in the Advanced Tab – Mux Parameters.
5. The MPTS will have an SDT if any of the connected encoders have the SDT enabled. The resulting SDT will only have entries for encoders that have SDT enabled.

Connection Statistics Tab

The Connection Statistics Tab presents the combined status of all the established connections, in one table. It includes the Source Port, Source Name, Output Port and Output Name fields to identify the connections, and the rows are in the same order as the table in the Configuration Tab. The Statistics tab contains two additional fields, the **Source Status** and the **Output Status**. Since these are color-coded, it is simple to quickly identify any problems. If any of the **Source Status** or **Output Status** indicators are red, the Dashboard™ Card State will be red as well, and the Status LED in the front of the card will also be red.

The meaning of the indicators is as follows:

- **OK**: The stream is operating normally. If it is an encoder, it means that it is operating normally; if it is an output, it means that it is either transmitting or ready to transmit.
- **Warn:** The stream is configured but disabled. Simply enabling the stream may clear this situation.
- **Error:** The stream is configured but has detected a problem. If it is an encoder, it is not running. If this is an output, it normally means that the output is either unable to send (e.g., an IP output configured for unicast but unable to find the destination MAC address) or dropping packets (e.g., an oversubscribed ASI or IP output in manual rate mode). ASI Outputs with Automatic Rate will be in this state if they do not have data to transmit. A sample of the Connection Statistics Tab is depicted below.

Established Connections					
Source Port	Source Name	Source Status	Output Port	Output Name	Output Status
Encoder 1	CBS Feed	🟢 OK	Ethernet 1	Primary Feed	🟢 OK
Encoder 1	CBS Feed	🟢 OK	Ethernet 1	Confidence Feed	🟢 OK
Encoder 1	CBS Feed	🟢 OK	Ethernet 2	Tower Feed	🟢 OK
Encoder 2	NBC Feed	🟡 Warn	Ethernet 2	Tower Feed	🟢 OK
Encoder 1	CBS Feed	🟢 OK	Ethernet 2	Studio Feed	🟢 OK
Encoder 2	NBC Feed	🟡 Warn	Ethernet 2	Studio Feed	🟢 OK
Encoder 1	CBS Feed	🟢 OK	ASI 1	Microwave Radio	🔴 Error
Encoder 2	NBC Feed	🟡 Warn	ASI 1	Microwave Radio	🔴 Error
Encoder 1	CBS Feed	🟢 OK	ASI 2	Monitoring Decoder	🟢 OK
Encoder 2	NBC Feed	🟡 Warn	ASI 2	Monitoring Decoder	🟢 OK

Admin Tab

The Admin tab contains several general administrative functions, each on its own tab.

The Admin tabs are:
- **General:** Manages a number of general card parameters; provides an SNMP MIB download.
- **Firmware:** Manages firmware images.
- **Config Files:** The 9992-ENC can store multiple configurations. These are managed in this tab.
- **Test Packet Generator:** Manages the Test Packet Generators.
- **License Keys:** Contains the current licensing state of the 9992-ENC and allows new license keys to be entered.
- **Event Log:** The 9992-ENC contains a non-volatile event log. It can be inspected and downloaded from this tab.

The Admin Statistics tabs are simplified read-only versions of the corresponding Admin Configuration tabs.

Admin General Configuration Tab

The Admin General Tab is depicted below:

The Admin General Tab includes the following parameters:
- **Card Name:** This field defaults to "9992-ENC" but can be set to any descriptive name. The name provided here also appears in the DashBoard™ Tree View.

- **SNMP Traps:** This allows SNMP traps to be enabled or disabled[6]. You must click the **Reboot** button for the changes to take effect (image shown below).
- **Enable Parameter Blast:** This feature that speeds up DashBoard startup over high-latency links (i.e., when the computer running DashBoard has a WAN connection to the encoder or the frame housing the encoder). This feature requires DashBoard version 8.2 or later.
- **MIB File Download:** The 9992-ENC provides an up-to-date copy of its MIBs. If you click on the **Save** button, a zip file with the relevant MIBs will be downloaded to your computer. This zip file contains the card MIBs, as well as the Ross Video and openGear MIBs required to compile the card MIBs.

Admin General Statistics Tab

The Admin General Statistics Tab is shown below. It shows the current configuration for the **Card Name, SNMP Traps** and **Enable Parameter Blast** controls.

This tab also includes one additional item, **Temperature Alarm,** which shows the current state of the 9992-ENC thermal protection system. The possible values are:
- ⬤ **None**: There is no temperature alarm and the 9992-ENC is operating normally.
- ⬤ **Chassis Door Open:** The 9992-ENC has detected that the chassis door is open. The ventilation fans are built into the chassis door; opening the door disengages the fans and cuts the airflow. While the 9992-ENC can operate for short periods of time without this airflow, such operation is not guaranteed over long periods of time (more than a few minutes). The 9992-ENC will remain in yellow alarm for as long as the chassis door is open. Depending on the chassis loading and ambient temperature, operating with the door open for more than a few minutes can cause the 9992-ENC to overheat and shut down.
- ⬤ **FPGA Temperature Warning:** The 9992-ENC has detected that its internal temperature has exceeded 70°C. The exact value can be found in the Product Statistics Tab. While the 9992-ENC can operate indefinitely in this condition without any damage, it is recommended that the situation be corrected as the thermal operation margin is reduced.
- ⬤ **FPGA Temperature Critical:** The 9992-ENC has detected that its internal temperature has exceeded 80°C. The exact value can be found in the Product Statistics Tab. While the 9992-ENC can operate indefinitely in this condition without any damage, the situation **MUST** be corrected immediately. If the internal temperature reaches 85°C, the 9992-ENC will **shut down** without any further notice to protect itself from damage.

---

[6] SNMP is an optional feature in the openGear™ frame controller. The 9992-ENC SNMP functions are only available if SNMP is licensed in the frame controller.

After a thermal shutdown, the 9992-ENC automatically starts again when the temperature is reduced to a safe operational value.

Admin Firmware Tab

The 9992-ENC can hold up to three distinct firmware images: a **Factory** image and two upgrade images, called **Image 1** and **Image 2**. The Factory image can never be overwritten, and will always be available as a fallback in case of problems or failed updates. Image 1 and Image 2 can be updated at will. Since the card offers two upgrade images, it is always possible to fall back to the previous image if there are any problems with the current one. The card will also automatically fall back to the factory image if it detects a corrupted firmware image. Finally, the push buttons on the front of the card allow for a forced override to the factory image, as described in the Front Switches section.

## Uploading a Firmware Upgrade

When applicable, Cobalt Digital Inc. provides for continual product enhancements through software updates. As such, functions described in this manual may pertain specifically to cards loaded with a particular software build. You can update your card by downloading the new Update software by going to the Support → Firmware link at www.cobaltdigital.com. Download "Firmware Update Guide", which provides simple instructions for downloading the latest firmware for your card onto your computer, and then downloading it to your card through DashBoard™. When you have the firmware upgrade file placed, in the desired location, on your computer click on the **Upload** button at the bottom of the user interface.
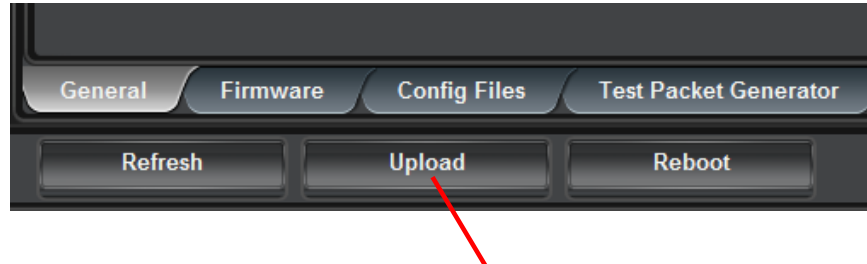
Click here to start firmware update

A classic dialog box allows you to browse your computer to select the upgrade file. You can simultaneously upgrade all of your 9992-ENC cards over multiple chassis as well. Uploading firmware to the 9992-ENC does not affect its operation in any way and does not introduce any glitches in the inputs/outputs.

Note: To allow for a controlled transition to operation when upgrading firmware, reboot the card to engage the new firmware. The card will go off-line while rebooting.
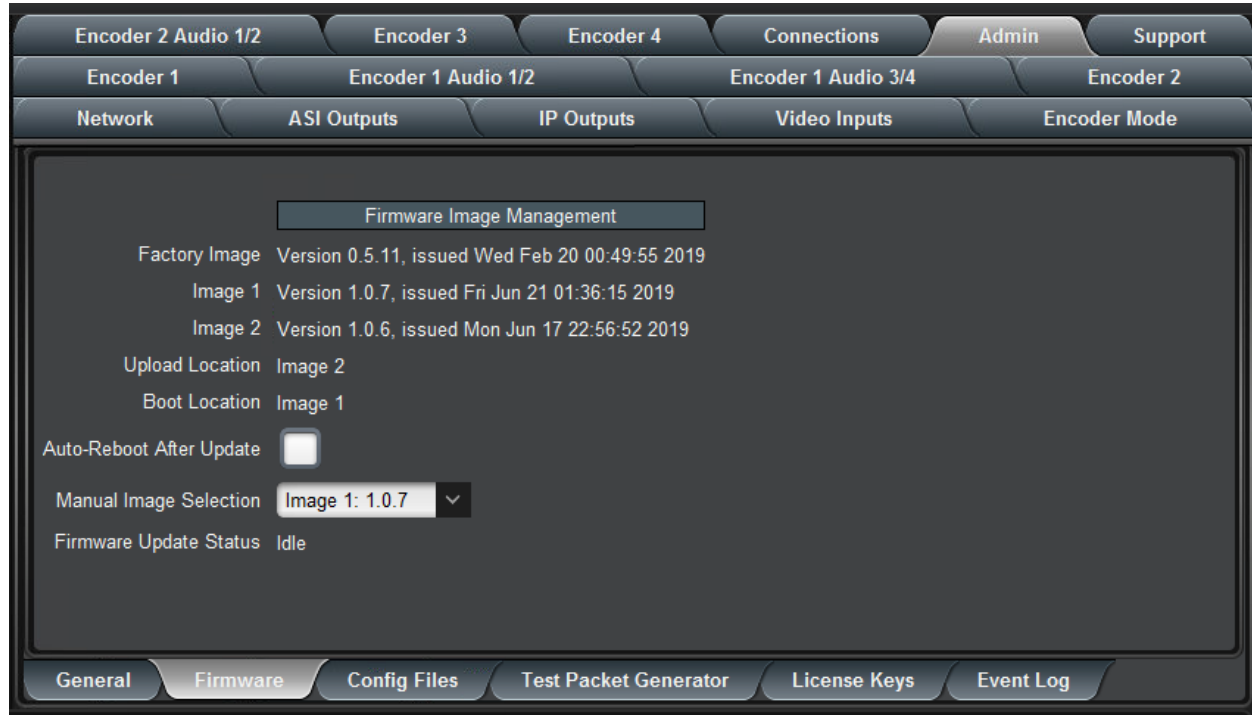
The fields in the Firmware Image Management tab are:

- **Factory Image, Image 1, and Image 2:** These contain version and release date information for the corresponding firmware images. If no valid image is present, this field will indicate **No Image**.
- **Upload Location:** This field contains the location where the image upload will go. The 9992-ENC automatically chooses a location that will not overwrite the currently running image.
- **Boot Location:** This field indicates which image will be used in the next boot. If an image is successfully uploaded through Dashboard, this automatically changes to point to that image. It can also be manually changed.
- **Auto-Reboot After Update:** This field controls whether the 9992-ENC will automatically reboot after a successful firmware upload through Dashboard. By default, the 9992-ENC will **not** reboot after an update. You can upload the firmware at any time, and reboot later during a maintenance window.
- **Manual Image Selection:** Select one of the previously uploaded images from the drop-down list and click the **Reboot** button to make the changes.
- **Firmware Update Status:** This describes the status of the Firmware running on the encoder.

Admin Config Files Tab

As you make configuration changes to the 9992-ENC, they are automatically persisted in non-volatile storage. If you reboot or power-cycle the card, it will come back in the same configuration.

In addition to automatic configuration persistency, the 9992-ENC also offers the ability to save up to 50 complete configurations, load them, and even export them. This can be used to quickly configure it for different scenarios, or for saving configuration "checkpoints" as a complex configuration is built. Since configurations can be exported, they can be archived outside the card as well.

The layout of the Admin Config Files tab is shown below.
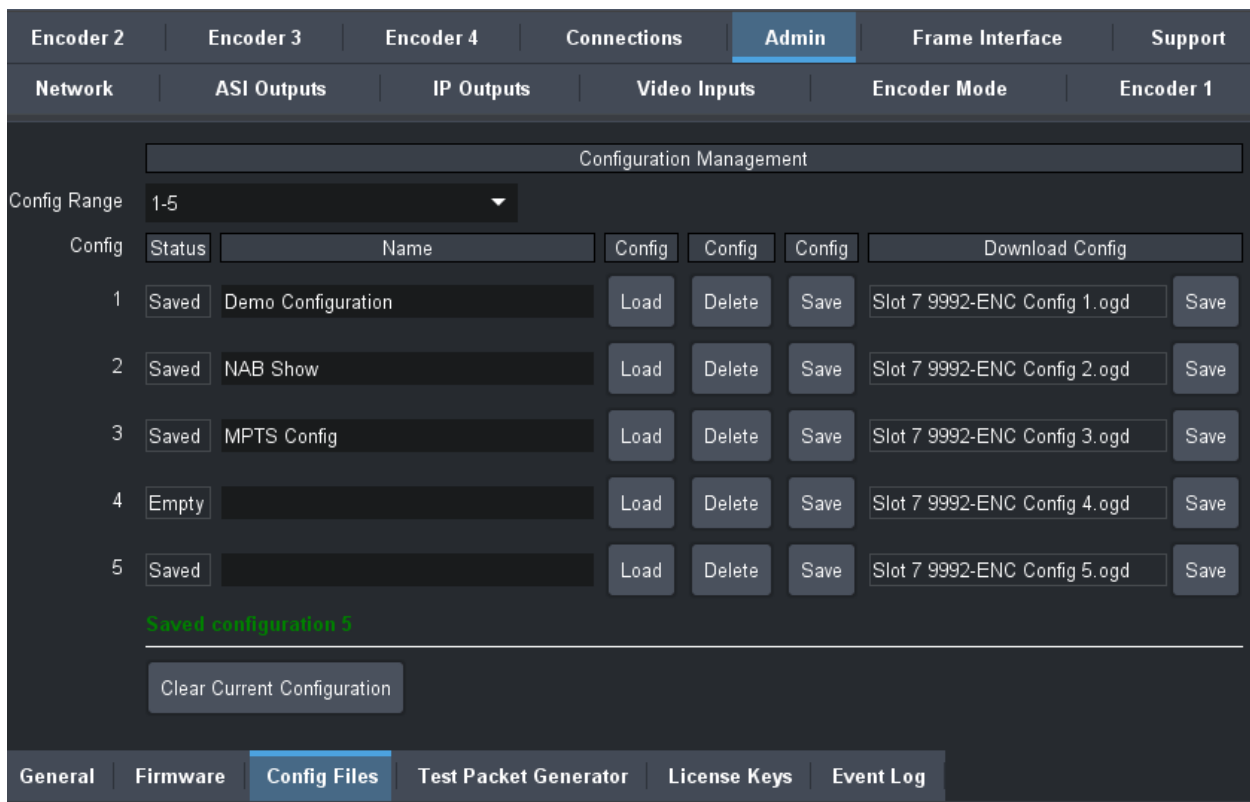
The Config Files tab only displays five configurations at a time. Use the **Config Range** control to select a range of configurations to display:
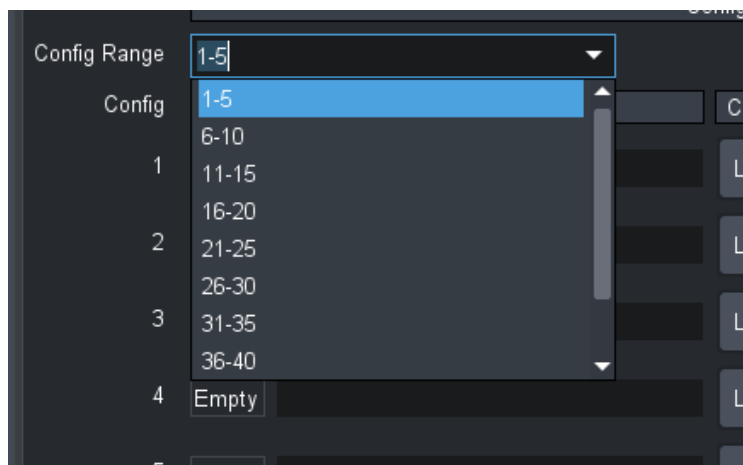
User-Saved Configurations

The fields in the user-saved configuration are:

- **Status:** This indicates whether there is a saved configuration on that particular slot. It will contain the words **Saved** or **Empty**.
- **Name:** This is an optional name for the configuration. It is not required but highly advisable. The name can be edited at any time (even when there is no saved configuration).
- **Config Load Button:** Click on this button and the corresponding configuration is loaded on the 9992-ENC card. It will replace the currently running configuration. Dashboard™ will take a few seconds to reload (longer if you are accessing over a wide-area network), but the actual configuration in the 9992-ENC is virtually instantaneous. The Status Message Area will indicate the result of the operation.
- **Config Delete Button:** If you click on this button, the corresponding configuration and its description are deleted.
- **Config Save Button:** If you click on this button, the current card configuration is saved on the corresponding slot, possibly replacing the configuration saved there if it is not empty.
- **Download Config:** If you click on the **Save** button, the corresponding file is downloaded to your computer. This feature is provided to allow configuration backups.

If you save a configuration to your computer, and later wish to restore it to the 9992-ENC, use the following procedure:

1. On Dashboard™, open the user interface for the frame controller (slot 0).
2. Select the **Data Safe** tab in the configuration area.
3. Uncheck the **Disable** checkbox corresponding to the card you wish to restore the configuration. This step is depicted below.
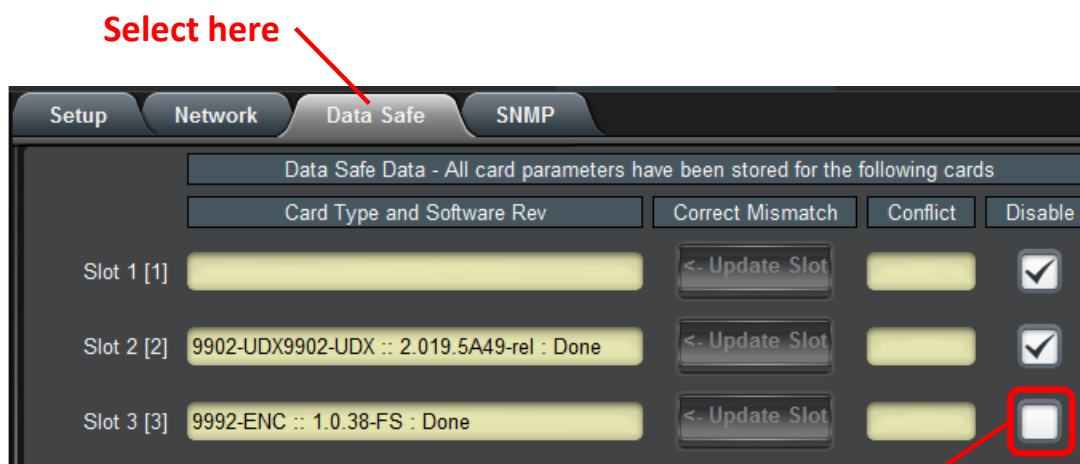
4. On the Dashboard™ Tree View, right-click on the card, and select **Restore Configuration.** Follow the prompts and navigate to the file you wish to restore. This process is illustrated below
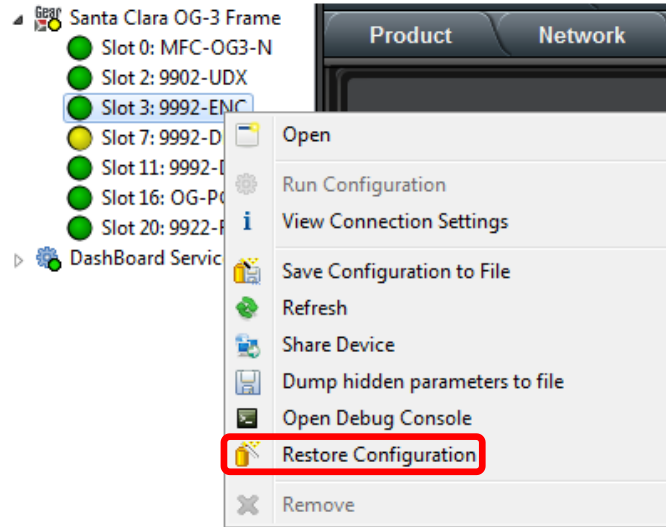
This process is discussed in further detail in the **DashBoard User Manual** – Chapter 5 – **Restoring Configurations to Devices**.

Clear Current Configuration Button

The **Clear Current Configuration** button clears all the configured ports and streams as follows:

- All ASI Ports are set to manual configuration, 20 Mb/s, 188-byte packets.
- All Encoders are stopped and configured with a default set of parameters.
- All IP Outputs are deleted.
- All Connections are removed.
- The Test Packet Generators are disabled.

The button does not affect the following areas:

- The settings in the **Network** tab are not changed.
- The settings in the **Admin General** tab are not changed.
- Saved configurations are not modified in any way.

Dashboard™ will take a few seconds to reload (longer if you are accessing over a wide-area network), but the actual configuration in the 9992-ENC is virtually instantaneous. The Status Message Area will indicate the result of the operation.

Admin Test Packet Generator Tab

The 9992-ENC includes two Test Packet Generators (TPGs) that are capable of generating a configurable constant bit rate sequence of MPEG-2 Transport Packets with very strict timing. The TPGs are considered a source (input), and are available to be connected to any output. The user interface for the TPGs includes a status table, which reports the current configuration of the generators.

To configure one of the TPGs, click on the **Edit** button on its row. The following configuration parameters are displayed:

The configuration interface is divided into two areas:

- **TPG Configuration Parameters**, described in this section.
- **Output Selection Connection Parameters,** described in the Destination Selection section of the Connections Tab chapter.

The TPG Configuration Parameters are:
- **Port Name:** All 9992-ENCports have a user-defined name, to facilitate routing. Enter any suitable name.
- **Mode:** controls the type of MPEG-2 transport packets generated. The options are:
    - **Disabled:** TPG is disabled. No packets are being generated.
    - **NULL Packets:** TPG is generating NULL packets. If you select this option, the **PID** parameter becomes read-only with the value 1FFF.
    - **Ramp48 Packets:** TPG is generating packets with a "Ramp48 Payload". A "Ramp48 Payload" is composed of the bytes 0x48, 0x49, 0x4A, …, 0xFF. Generated packets have the Payload bit set, no Adaptation Field, and a valid Continuity Counter field.
    - **PCR Packets:** TPG is generating packets with a valid PCR field (stamped corresponding to the packet's departure time at the configured bit rate). The packets have a small payload with random data, so the Continuity Counter field is valid and counting.
- **PID:** controls the PID of the generated packets. This field accepts both decimal and hexadecimal values (prefixed with 0x).
- **Bit Rate (bps):** controls the bit rate of the generated packets. The minimum value is 64,000 bps and the maximum value is 213,000,000 bps.

Admin License Keys Tab

The 9992-ENC has several optional licensable features. The Admin License Keys Tab is used to manage these features. Using this tab, you can see how many licenses you have for each optional feature, and how many you are currently using.

The Admin License Keys Tab includes a License Status table, and a configuration area, as shown below. The table rows are license counts, and the columns correspond to different licensable features. The rows are:
- **Permanent Licenses:** This is the number of non-expiring licenses for each feature.
- **Temporary Licenses:** This is the number of temporary licenses for each feature. Once the license period expires, they are removed.
- **Total Licenses:** This is the total number of licenses for each feature. It is simply the sum of the permanent and temporary licenses.
- **Used Licenses:** This is the number of licenses in use for each feature by the current card configuration.

If you have temporary licenses, the **Time Remaining** field indicates how long until they expire. If you do not have temporary licenses, this field has the message "No active temporary licenses". The table columns correspond to the licensable features, as follows:
- **4K Encode:** This enables 4K encoding for the board. If you have the 9992-ENC-4K-HEVC model, this license was pre-installed in the factory.
- **UL Latency:** This enables Ultra-Low Latency encoding in HEVC. This is not a counted feature and applies to the board as a whole.

- **SMPTE 2022 FEC**: This enables FEC for the board. This is not a counted feature; if FEC is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one FEC instance in use.
- **RIST**: This enables RIST for the board. This is not a counted feature; if RIST is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one RIST instance in use.
- **4:2:2**: This enables 4:2:2 encoder for the board. This is not a counted feature; if 4:2:2 is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one 4:2:2 instance in use.
- **AVC**: This is the maximum number of AVC/MPEG-2 encode instances licensed for the board. If you have the 9992-ENC-4K-HEVC model, four instances of this license were pre-installed in the factory.
- **HEVC**: This is the maximum number of HEVC encode instances licensed for the board. If you have the 9992-ENC-4K-HEVC model, four instances of this license were pre-installed in the factory.
- **MP2/AAC**: This is the maximum number of combined MPEG-1 Layer II and AAC encode sessions licensed for this board. Each AVC or HEVC license comes with 2 encode sessions. An AAC 5.1 surround encode session requires 3 licenses.
- **Dolby 2/0**: This is the maximum number of Dolby stereo encoding sessions licensed for this board. Each license can be used either for AC-3 stereo or EAC-3 stereo.
- **Dolby 3/2**: This is the maximum number of Dolby 5.1 surround sessions licensed for this board. Each license can be used either for AC-3 or EAC-3. Surround licenses can also be used for Dolby 2/0 stereo operation.
- **Encryption**: This enables RIST Main Profile Encryption and Authentication for the board. This is not a counted feature; if encryption is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one encryption instance in use.
- **SRT**: This enables SRT for the board. This is not a counted feature; if SRT is enabled, the corresponding number is 1; if it is disabled, the corresponding number is 0. The Used Licenses field will be set to 1 if there is at least one SRT instance in use.

	License Status											
Feature	4K Encode	UL Latency	ST-2022 FEC	RIST	4:2:2	AVC	HEVC	MP2/AAC	Dolby 2/0	Dolby 3/2	Encryption	SRT
Permanent Licenses	1	1	1	1	1	4	4	16	16	5	1	1
Temporary Licenses	1	1	1	1	1	3	4	14	16	5	1	0
Total Licenses	1	1	1	1	1	4	4	16	16	5	1	1
Used Licenses	0	0	1	0	0	2	2	0	0	0	0	0

Time Remaining: 3 weeks, 6 days, 23 hours

License Key Installed OK

License Key:

Apply License Key

Serial Number: ac83f0010034

To request a license key from Cobalt, you will need to provide the card serial number. It can be found in the Product Tab and in the Admin License Key Tab as well. Once you receive the key from us, enter it in the **License Key** field shown above, and click on the **Apply License Key** button. If the key is accepted, you will see the message *License Key Installed OK*, as illustrated above. If there are any problems, you will see an error message in the same location. The following are the possible error messages:

- *Invalid key: missing characters*: the key you entered is too short. Double-check that you entered all the characters.
- *Invalid/Corrupted Key*: the key you entered has the correct number of characters, but it is invalid. Double check what you entered.
- *Serial number mismatch: this key is for serial xxxxxxxxxxx*: 9992-ENC license keys are specific to a card. You entered a valid license key, but it is intended for a different card, whose serial number is displayed in the message. You must use this key on the correct card.
- *This key has already been applied*: License keys can only be applied once. This is a valid key for this card, but you have already applied it, and its features are already available.
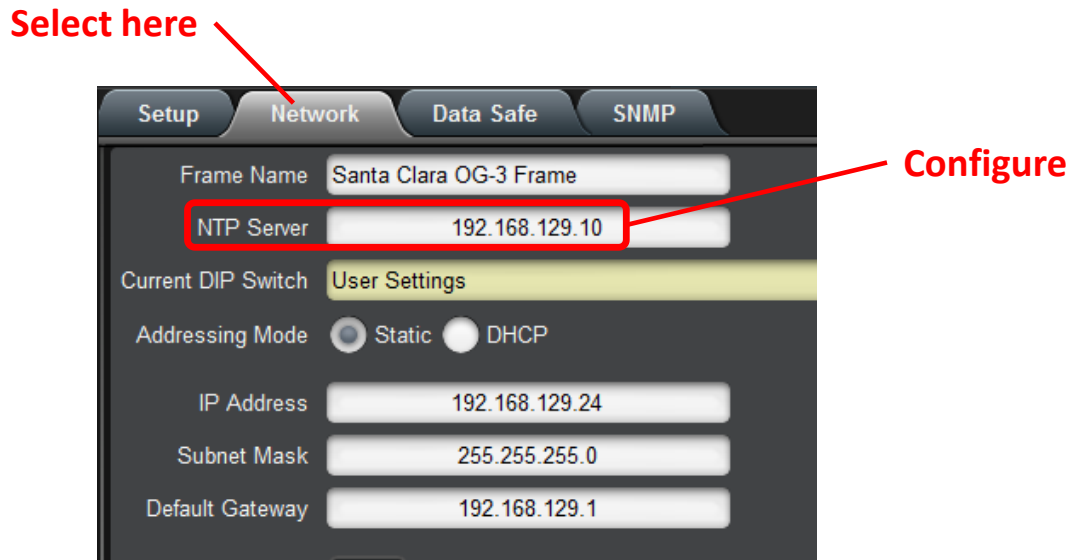
Admin Event Log Tab

The 9992-ENC includes an Event Log in non-volatile storage. This event log can be used for fault finding and to check for error conditions. The following information is included in each 9992-ENC event in the log:

- **Date:** The calendar date in which the event occurred.
- **Time:** The time at which the event occurred.
- **Severity:** The severity of the event. The 9992-ENCdefines three severity levels:
    - **Error:** Any events that affect the operation of the device. For example, an ASI Input losing lock or an IP Input no longer receives packets. An error will impact service until addressed.
    - **Warning:** Any events that may produce visible glitches, but they do not have a continuous service impact. Examples of warnings are automatic redundancy switches and ARP renewal failures.
    - **Info:** These are informational events. All configuration actions are logged with this severity. When an error is cleared (for example, an ASI Input regains lock), the event is logged with this severity as well.
- **Subsystem:** The subsystem affected by the event. This may be a port, a stream, or the card itself.
- **Event:** This is a textual description of the event.

The 9992-ENC does not have a battery-backed real-time clock. It depends on the frame controller to obtain the current date and time, and the frame controller depends on an external Network Time Protocol (NTP) server to obtain current date and time. By default, the 9992-ENC will initialize its internal time-of-day clock to January 1, 2018, GMT. If the frame controller is NTP-synchronized, the 9992-ENC will then accept time from it and set it's time-of-day clock accordingly.

In order to configure the frame controller for NTP, open its configuration screen on Dashboard™, select the **Network** Tab, and enter the IP address of an available NTP server:

If your frame controller has access to the Internet, you can point it to one of the public NTP servers for your region. You can find more details on this link: **http://psp2.ntp.org/bin/view/Servers/WebHome**

The full Admin Event Log tab is displayed below:
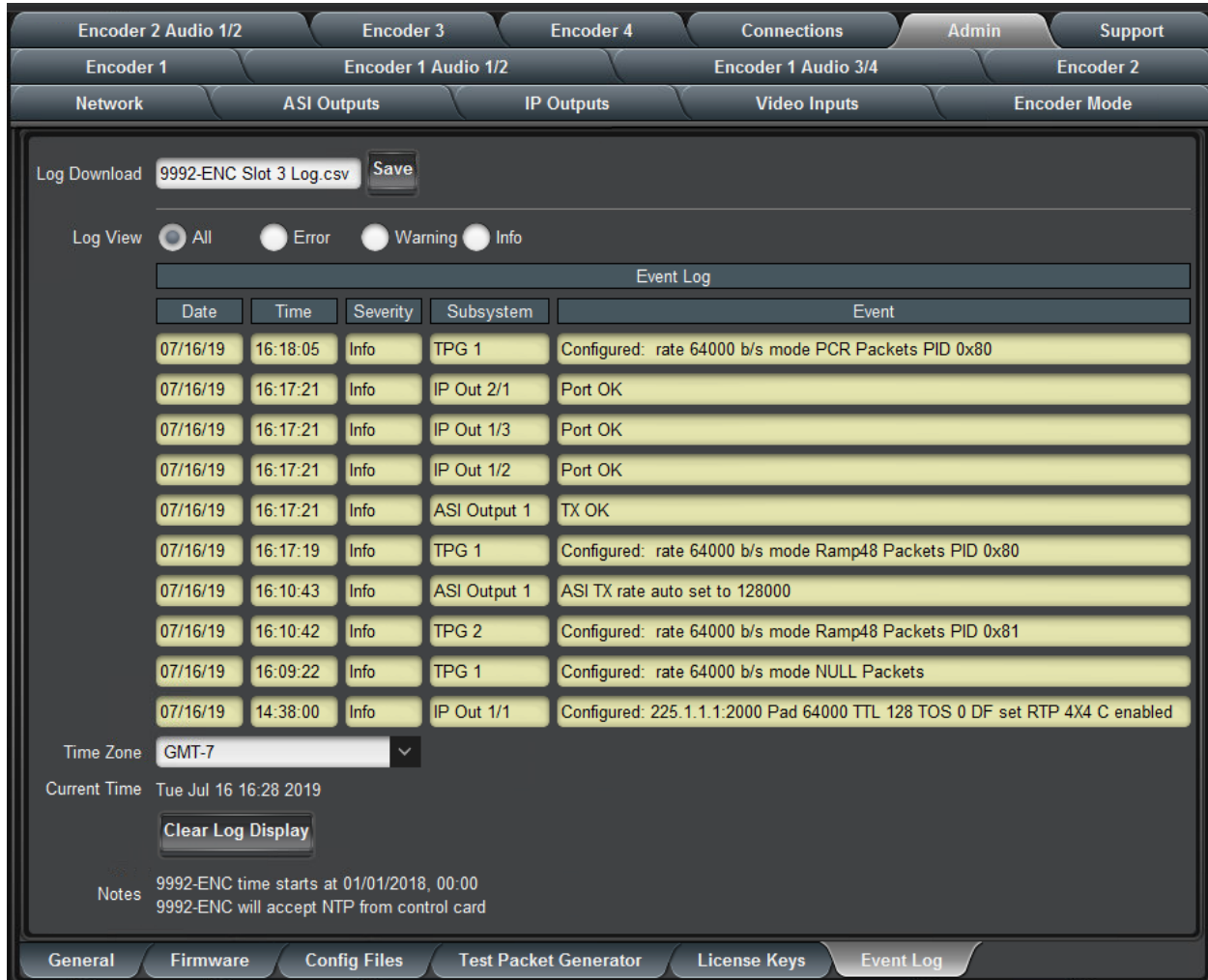
The fields are:

- **Log Download:** The user interface only displays the last 10 events of each type. If you would like to see the whole event log, it can be downloaded to your computer by clicking on the **Save** button. The log will be in CSV format, and it can be opened by any utility that can read text files; ideally, you should use a spreadsheet program such as Microsoft Excel or similar, so it is presented in tabular format. The log will be in chronological order, oldest entry to newest.
- **Log View:** The user interface can display the last 10 events. You can choose to see the last 10 events of any kind by selecting **All** or you can restrict the view only to **Info**, **Warning**, or **Error**.
- **Event Log:** This table presents the last 10 events of the selected type.
- **Time Zone:** To simplify the correlation of the events with your local time, you can set your time zone using this drop-down menu. Note that the 9992-ENC presents a simplified list, with standard GMT offsets. Note that standard GMT offsets do not change back and forth with Daylight Savings; you will need to make this adjustment manually if it is relevant to you.

- **Current Time:** This field indicates the 9992-ENC view of what the current date and time is. If your frame is not NTP-synchronized, this is useful to figure out "how long ago did this event happen".
- **Clear Log Display:** If you click on this button, it clears all log views. This is useful to quickly identify any new events after the unit has been set up. Note that this action does not clear the logs stored in non-volatile memory.

The 9992-ENC will store up to about 400 Kbytes of logs in non-volatile memory. When that limit is reached, the oldest half of the stored logs will be deleted to make space for new logs.

Frame Interface Tab

Some openGear frames, such as the Cobalt BBG-1300-FR and the Ross OG-3/OG-X frames include a midplane Gigabit Ethernet layer-2 switch, connected to the frame control network. The 9992-ENC can be configured to connect to this network. The advantages of enabling this connection are as follows:

1. Firmware updates will use this interface instead of the frame's CAN bus. This will significantly reduce the download time, from several minutes (or more if the computer running DashBoard is remote from the frame) to a few seconds.
2. Initial DashBoard connection to the card or card refreshes will be significantly faster, typically taking a few seconds, even if the computer running DashBoard is remote from the frame.
3. The frame interface is available for unicast RIST, HLS, SRT and RTMP operation. In some situations, it may not be necessary to connect the I/O panel streaming ports.

Frame Interface Configuration Tab
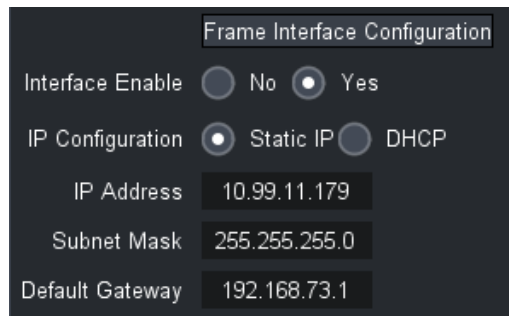
The Frame Interface Configuration Tab is shown below:

- **Interface Enable:** This control is used to enable/disable the Frame Interface. If it is set to **Yes**, additional options are displayed:

- **IP Configuration:** This control selects between DHCP and Static IP configuration. If **Static IP** is selected, the following additional configuration options are displayed:
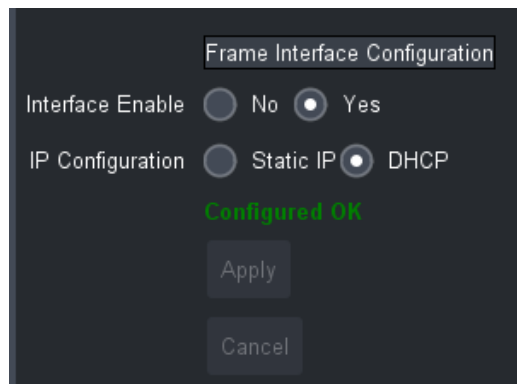
- **IP Address:** Enter the desired interface IP address.
- **Subnet Mask:** Enter the desired interface subnet mask.
- **Default Gateway:** Enter the desired default gateway. The default gateway must be consistent with the IP address and subnet mask.

Hit the **Apply** button to accept the configuration. If the configuration is valid, the message **Configured OK** will be presented:

Notes:
- The 9992-ENC will only use the Frame Interface if it has Ethernet link and a valid IP address. Enabling the frame interface on a frame that does not have the Gigabit backplane will have no effect. The status of the Frame Interface is reported in the Frame Interface Statistics Tab.
- If the computer running DashBoard does not have IP connectivity to the 9992-ENC frame interface, **firmware updates will fail**. In such cases, either correct the network connectivity or disable the Frame Interface.

Frame Interface Statistics Tab

The Frame Interface Statistics Tab shows the current configuration and status of the Frame Interface:

The parameters are:

- **Interface Enable:** shows the current value of this parameter. If the interface is not enabled, the IP address, Subnet Mask, and Default Gateway will be shown as 0.0.0.0.
- **IP Configuration:** shows the current value of this parameter.
- **IP Address:** shows the interface IP Address, which may have been obtained through DHCP.
- **Subnet Mask:** shows the interface Subnet Mask, which may have been obtained through DHCP.
- **Default Gateway:** shows the interface Default Gateway, which may have been obtained through DHCP.
- **Interface Link:** this indicator has the following two values:
  - ● **Link OK**: The Frame Interface has established link with the frame.
  - ● **No Link:** The Frame Interface has not established link with the frame. This should only happen in frames without the Gigabit backplane.
- **Control Speed:** this indicates the data rate at which the Frame Interface has achieved link. It should always be **1 Gb/s Ful Duplex**. Any other value is an indication of a physical issue, either with the 9992-ENC or the frame.
- **MAC Address:** this reports the MAC address of the Frame Interface.

Support Tab

If you need support with your product, you can contact Cobalt Digital Inc. by phone or e-mail:
- Phone number: +1 217 344-1243, Monday-Friday 8:00AM – 5:00PM Central Time
- E-mail:

If you need to contact Technical Support, please be prepared to provide the following information:
1. A detailed description of the problem, and any actions taken to solve it.
2. A detailed description of the environment around the encoder. This includes the make and model of any connected devices being used, as well as the connection network (IP or ASI) between the encoder and any other devices.
3. The Technical Support information from the decoder itself. This is downloaded from the **Support** tab:
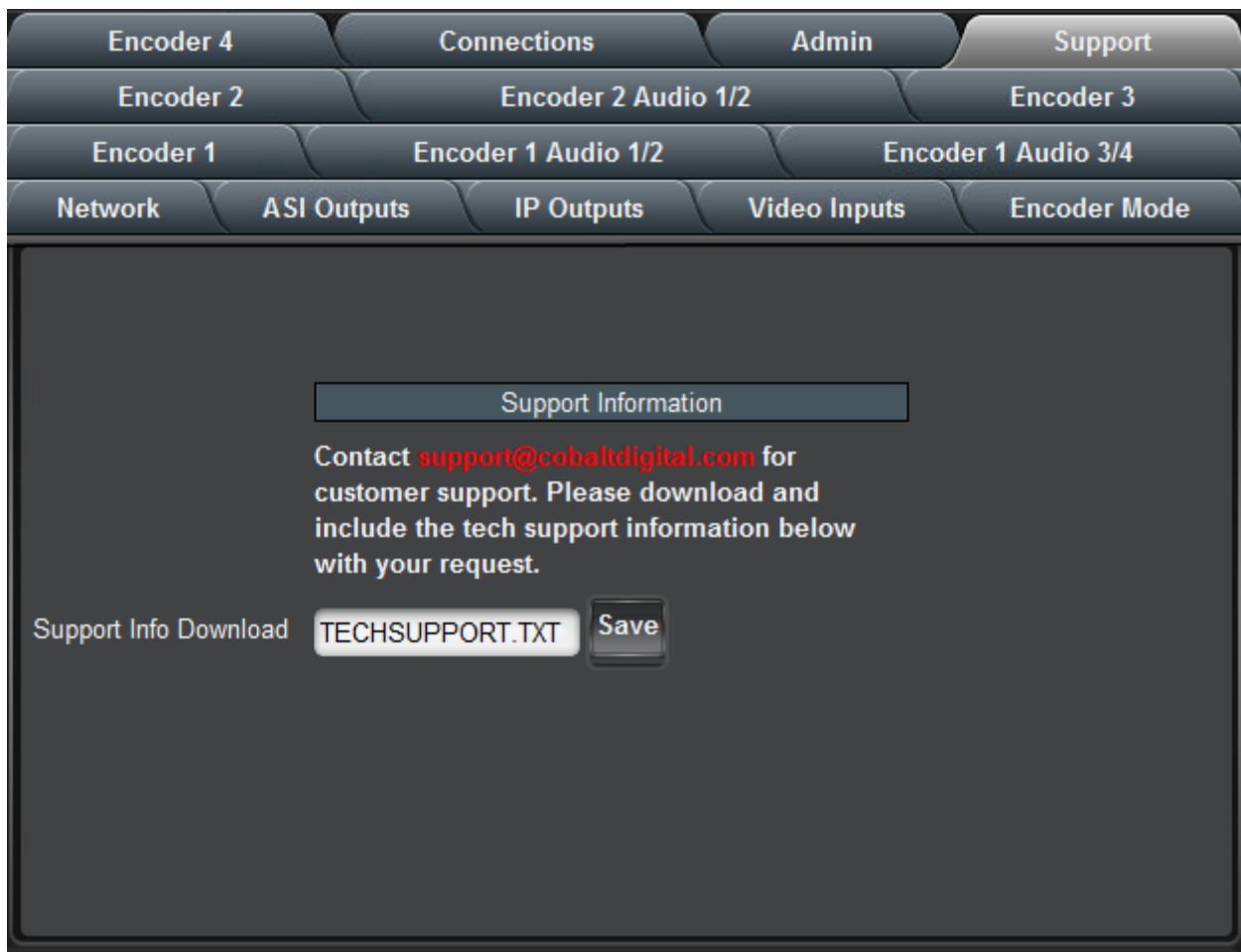
Select the **Support** Tab, and click on the **Save** button next to **Support Info Download**. This will create a file called **TECHSUPPORT.TXT** in the computer running DashBoard. Please e-mail this file to address shown.

The **TECHSUPPORT.TXT** file contains the following information:

- The current configuration of the unit
- A copy of the Event Log (which can also be obtained via the Admin Event Log Tab)

This file does not contain any information that would allow remote access to the unit.

RIST Main Profile Authentication

Technology Overview

RIST Main Profile security (encryption and authentication) is provided by DTLS, which is the datagram version of the TLS functionality used to secure web sites. This technology is mature and widely deployed.

DTLS authentication is based on the concept of **Key/Certificate** pairs. A **Key** must be kept secret. A **Certificate** is derived from the **Key** and is public. A certificate allows secure communication, but only with the device that holds the corresponding key.

A certificate may be signed by a third party called a **Certificate Authority (CA)**. This is a third party that is trusted; if a device is prepared to trust the Certificate Authority, that trust extends to the certificates signed by it.

The certificate-based authentication process is illustrated in Figure 1. In this figure, Device B is deciding whether or not it trusts Device A. The same process can happen independently in the other direction. Device B has decided to trust certificates signed by a certain CA, so it has a copy of its CA Certificate, which was transferred to it through some secure means. Device B then receives a certificate from Device A. Unless that certificate matches the key stored in Device A, communication cannot even start. Device B can locally check the CA signature in the certificate coming from Device A against the CA Certificate it has. It that signature matches, and if Device B is prepared to trust the CA, then it will agree to communicate with Device A.
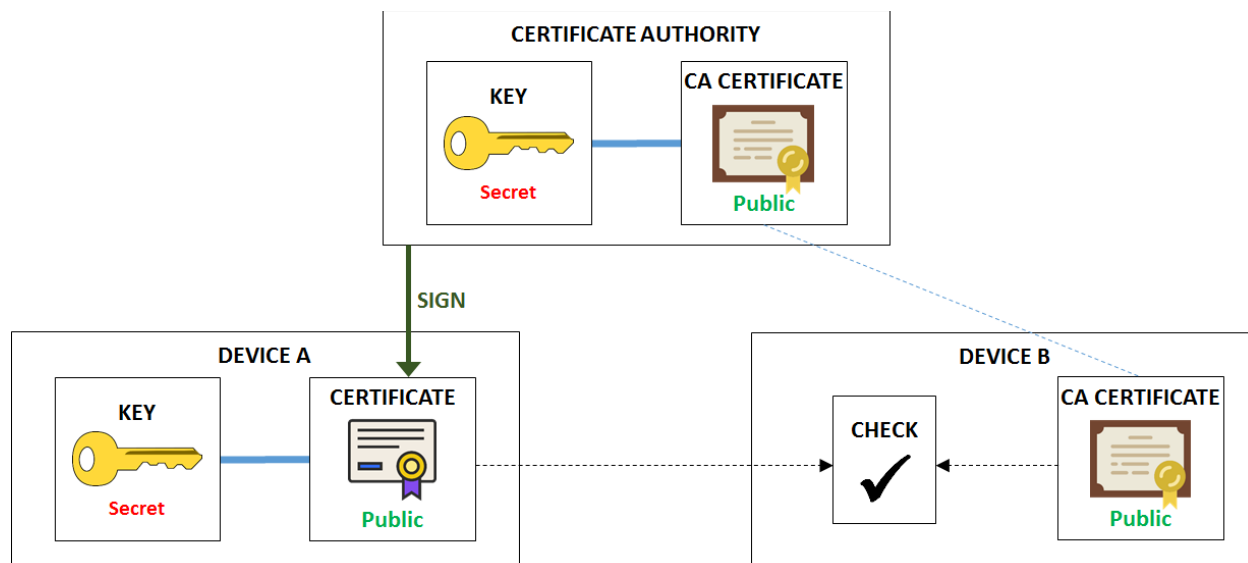

Figure 1: Certificate Checking

Security is maintained since:

- Even though the certificate from Device A is public, an unauthorized device cannot use it to establish communication because it does not have the corresponding key. Communication will not start.
- An unauthorized device may have a consistent certificate/key pair, but it will not be able to use it to start communication because the certificate is not signed by the CA trusted by Device B.

129

Certificate Validity and Expiration

All certificates have two dates built in:
- A starting date and time, before which the certificate is not valid.
- An ending date and time, after which the certificate is not valid.

When the certificate is generated, the user/device/process that is generating it decides on the certificate validity. There is no practical limitation on how long a certificate may be valid for. Administrators can decide on this as a tradeoff between security and convenience.
If certificate-based authentication is being used, it is important that the devices involved have a way to determine "what time is it now". NTP synchronization is highly recommended.

Blocklists

It is possible that a device goes "rogue" – in other words, it used to be authorized, but for whatever reason, it should not be accepted anymore. In Cobalt devices, this functionality is implemented using a list of **blocked devices**. One important field in the certificate is the **Common Name** – i.e., the name of the device. In a web site, this is usually the address of the site, e.g., www.cobaltdigital.com, but it can be any text string. For Cobalt devices, the blocking is done based on the Common Name of the device. Referring back to Figure 1, Device B will execute an additional step after it verifies that the certificate from Device A is valid – it will check that the Common Name is not in a list of blocked devices. If it is, Device B will refuse to communicate, even though the certificate checks out.
Due to the nature of how certificates are generated, it is not possible to take a valid certificate and modify the Common Name (or any of the other fields encoded in it, including the validity date). Such an alteration will cause the certificate to become invalid (it is protected by a hash).

Signing a Certificate

Figure 1 shows a certificate that has been signed by a Certificate Authority. In order to be secure, the signing process must not expose the device's secret key, not the CA's secret key. The process uses an intermediate file called a **Certificate Signing Request**, or **CSR**. The process is illustrated in Figure 2.
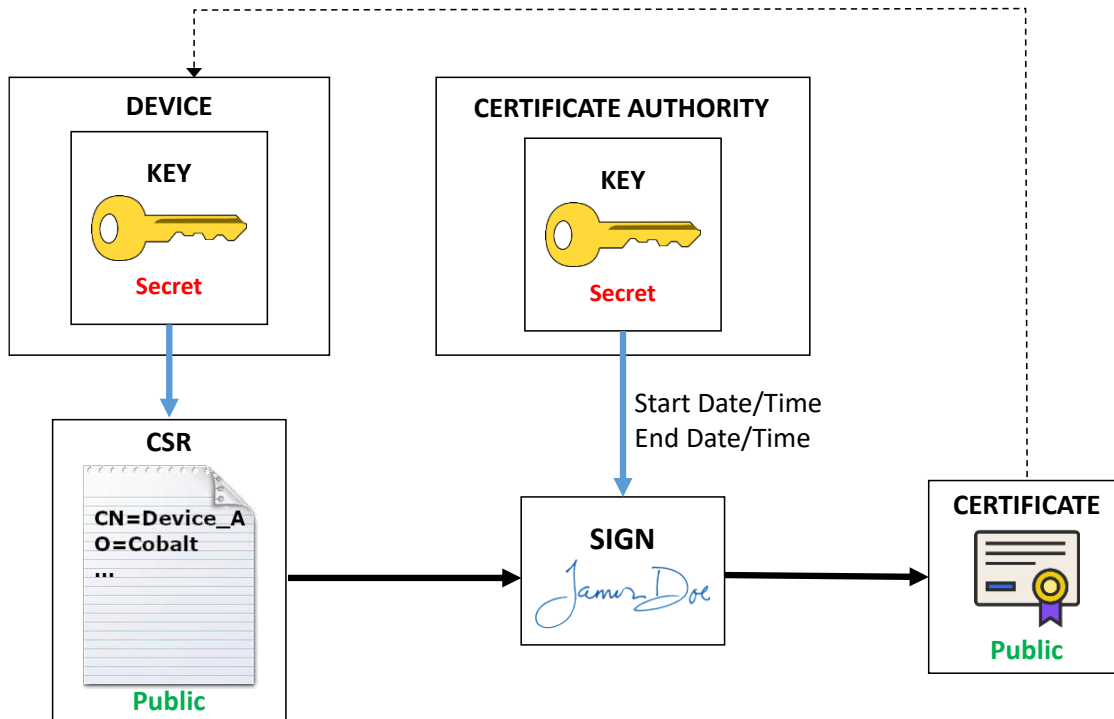
Figure 2: Certificate Signing Process

As indicated in Figure 2, the process includes the following steps:

1. A CSR is generated based on the device key (either by the device itself or by someone with access to the key). The CSR has a number of configurable items that will be transferred to the final certificate. The most important item is the Common Name, which later can be used to block access. Other fields include Organization, locality, etc. These items are not checked by Cobalt devices.

2. The CSR file (which does not need to be kept confidential) is then given to the Certificate Authority, which then "signs", generating the desired certificate. The configurable items in the CSR are copied into the certificate. At this step, the validity dates of the certificate are also set. Normally, the start date/time is whatever the local time is at the CA, and a duration (normally expressed in days) is specified.

3. The signed certificate needs to be given back to the device, to be used when it communicates with other devices.

Cipher Suites

RIST Main Profile defines two classes of cipher suites, with different key types:

- Cipher suites that use RSA keys.
- Cipher suites that use ECDSA keys.

Cobalt devices support both types of cipher suites. Since each type has a different key, each type needs its own certificate. The whole process described in the previous sections applies to each type of key. When a RIST Main Profile device connects to another RIST Main Profile device, it will negotiate a common cipher suite that is supported on both sides. For maximum compatibility with third-party devices, install both RSA and ECDSA keys and/or certificates in

131

the Cobalt device. However, if you know that one type or another is not in use, you can skip the authentication files for that type.

ECDSA ciphers are considered more secure than RSA ciphers. A Cobalt device will preferably select ECDSA ciphers if supported.

RIST Main Profile Encryption and Authentication in Cobalt Devices

This section provides an overview of the encryption and authentication capabilities built into Cobalt devices. These are provided in the context of RIST Main Profile tunnels. Encryption and authentication are implemented using the DTLS protocol, which is the datagram version of the standard TLS protocol used to secure web sites in the Internet.

Encryption options

RIST Tunnels are configured in the **Network** top tab, **RIST Tunnels** bottom tab. The number of tunnels offered varies by device, and is set to the maximum number of channels that device can support. For example, since the 9992-ENC encoder can support 4 simultaneous encoding sessions, it can support up to 4 RIST Tunnels. Encryption is invoked simply by checking the **Encryption** box. Once that box is checked, other options appear, as illustrated in Figure 3. The device will offer a list of available cipher suites. When negotiating the DTLS connection, it will accept any of the allowed ciphers. The full name of the offered cipher suites is:

- **AES128-RSA:**   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- **AES128-ECDSA:**   TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- **AES256-RSA:**   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- **AES256-ECDSA:**   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- **NULL:**   TLS_RSA_WITH_NULL_SHA256

The **NULL** cipher provides no encryption, only optional authentication, and is disabled by default. It is provided for testing purposes and its use in production is strongly discouraged.

Figure 3: Configuring Encryption

The –RSA ciphers (and the NULL cipher) use RSA keys and certificates, and the –ECDSA ciphers use ECDSA keys and certificates.

The actual cipher to be finally used when the tunnel is established is negotiated at connection time, and is reported in the DashBoard GUI. Please note that if the tunnel endpoints are configured in such a way that there is no allowed common cipher, the tunnel will fail to connect. If the **Authentication** checkbox in Figure 3 is not checked, the device will agree to connect to any other device (regardless of whether it actively starts the connection as a client, or it waits to be contacted as a server). The communication will still be encrypted.

Authentication Options

All Cobalt devices with RIST Main Profile support include the following:
- A built-in Certificate Authority (CA), which includes a key and the corresponding certificate.
- A built-in RSA key and corresponding certificate, signed by the built-in CA.
- A built-in ECDSA key and corresponding certificate, signed by the built-in CA.

Internal certificates are generated with a 10-year duration. At boot time, the device will always check if the certificates are expired or not yet valid, and will re-generate new certificates if this is the case. However, when using authentication, it is very important to have a valid date/time in the device. All Cobalt devices support NTP synchronization.

Cobalt devices offer the following features (available independently for RSA and ECDSA modes):
- Users can upload new key/certificate pairs for the device to use.
- Users can obtain CSRs derived from the built-in device keys.
- Users can upload a CSR, have it signed by the local CA, and download the corresponding certificates.
- Users can upload new certificates matching the built-in keys.
- Users can back-up and restore the local CA key.
- Users can download the local CA and encryption certificates.

While authentication can be individually enabled/disabled in a per-tunnel basis (by using the **Authentication** checkbox shown in Figure 3), the keys and certificates are shared between all tunnels.

Authentication Security Model

Authentication involves the use of two interfaces:
- The DashBoard GUI is used to configure the authentication parameters.
- A web interface is used to move files in and out of the device.

The security model assumes that the DashBoard interface is secured – i.e., the network where DashBoard communication is happening is a secure network and no further security measures are needed.

The web interface requires a password to complete all operations that involve uploading a file to the device. The web interface can also be enabled or disabled on individual network interfaces. If the device has a management port, the web interface is always available on this port.

All common authentication functions are available in the **Network** top tab, **Authentication** bottom tab. The relevant configuration items are shown in Figure 4.
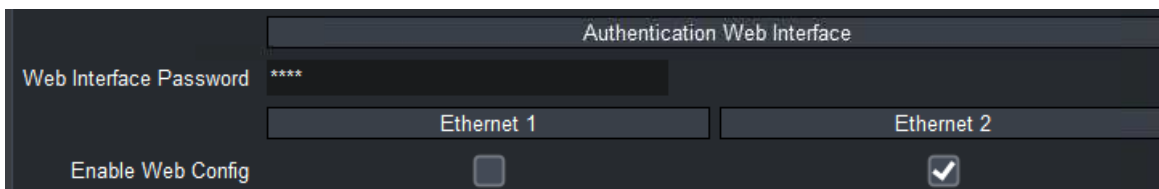

Figure 4: Web Interface Security Control

The configuration items are as follows:
- **Web Interface Password:** some web interface actions require a password. The password is set here. If the password is lost simply set another one. The default password is **Admin** and it should be changed if this function is to be used.
- **Enable Web Config:** Cobalt devices have streaming ports (usually in the openGear card I/O panel). If a streaming port is directly connected to the Internet, it is insecure to have the authentication web interface available on it, even with the password. This control allows the user to enable or disable the web interface on specific Ethernet interfaces. The number of interfaces presented here is device-dependent.

The **Authentication** tab has Apply/Cancel buttons at the bottom. Changes become effective only after the Apply button is clicked.
If the web interface is enabled for a given network interface, the following links will be available in the web page served from that interface:

Click here for RIST Key/Certificate Management

Click here for RIST Authentication Management

Configuring the Local Credentials in the Device

As illustrated in Figure 1, the device needs a matched key/certificate pair to operate. The device's certificate is its identity, presented to remote devices when connecting. Using the DashBoard interface, in the **Authentication** tab, the device can be configured to use either its built-in credentials, or credentials that have been uploaded by the user through the web interface. This is shown in Figure 5.
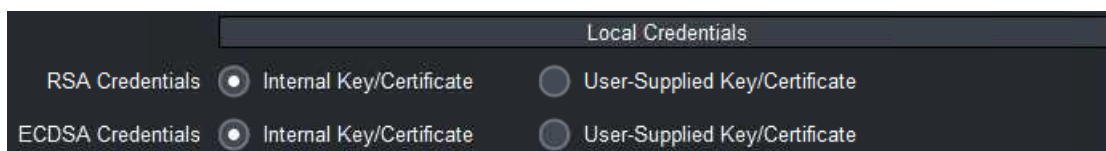

Figure 5: Configuring the Local Credentials

Note that selecting "User-Supplied Key/Certificate" prior to actually uploading a Key/Certificate will fail when the Apply button is clicked. Use the web interface to upload the files.

Uploading Keys and Certificates

In order to upload Keys and Certificates, follow the <u>Click here for RIST Key/Certificate Management</u> link in the web interface, as illustrated in Figure 6. For each type of encryption, you have two options:

1. Upload a matched key/certificate pair together

   or

2. Upload only a certificate that is matched to the internal built-in key. In order to do this, you will need to obtain a CSR from the device itself and get it signed, as illustrated in Figure 2. This process is described in more detail below.

You do not need to provide all four files. For example, if you are only interested in ECDSA operation, you just need to provide the ECDSA Certificate (matched to the internal key) or a certificate/key pair. Certificates and keys must be in PEM format.

The **Device Password** must match the password entered in the DashBoard interface.

Click on **Upload Files** to push the selected files into the device. Note that the device will only accept the files if they are consistent, i.e.:

- Files must be in the proper format.
- If only a certificate is provided, it must match the built-in key.
- If a key and certificate are provided, they must be of the correct type (RSA or ECDSA) and must match each other.
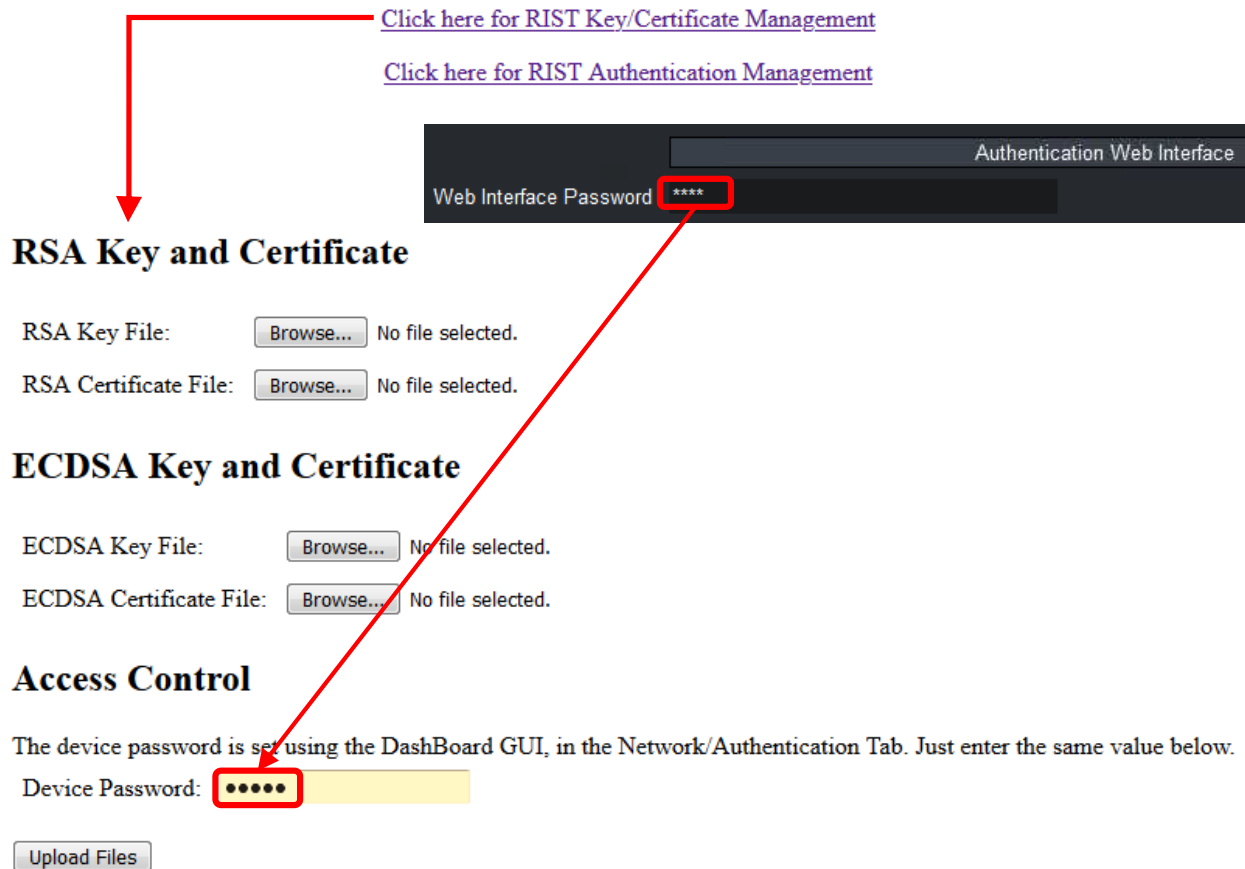
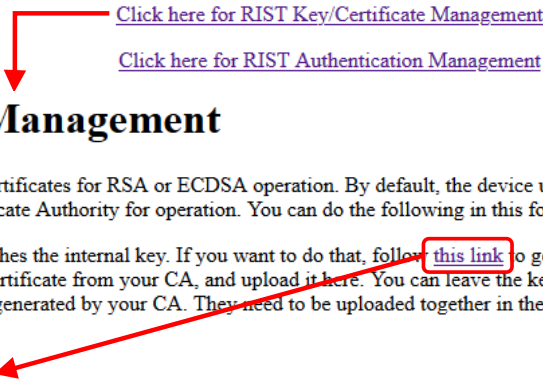*Figure 6: Uploading Keys and Certificates*

Obtaining a CSR for the Built-In Keys

Figure 7 shows the process to generate a CSR for one of the built-in keys. Fill in the form and click on **Generate CSR.** A link will be provided to download the CSR, which then can be signed by an external CA, generating a certificate. The certificate will be uploaded to the device as described in the previous section.

Most fields in Figure 7 are informational and will become part of the CSR, but have no further use. The two relevant fields in this form are:

- **Key Type:** the CSR will be for either the RSA or the ECDSA key. Select which key here. If you need to generate CSRs for both keys, use this form twice.
- **Common Name:** this is what identifies the device. If later you need to block this device, the blocking will be done based on the Common Name field. It is recommended that you use unique names per device if you are generating CSRs.

No password is necessary to generate a CSR since they do not need to be kept confidential.

Figure 7: Generating a CSR

Authenticating Remote Devices

The previous sections described how to set the credentials for the local device, which are presented to the remote device at connection time. In other words, they are the answer to the "*who are you?*" question.

The other side of the authentication is, upon reception of the credentials, to decide if the local device is willing to communicate with the remote device. For Cobalt devices, the answer to this question is "*any device whose certificate has been signed by my trusted CA is allowed to connect, unless explicitly banned*".

All Cobalt devices have a built-in CA, and by default will authenticate against this built-in CA. This means that if you simply enable authentication in two Cobalt devices, **they will fail to communicate** because each one is using its internal built-in CA credentials. They will need to be configured with the proper CA and credentials.   There are multiple options to do so, described below.

Option 1: Use an External Certificate Authority

This is the most secure option, but it is also the most involved to set up. The steps are:
1. Create a Certificate Authority on a computer separate from the Cobalt devices, and generate a CA Certificate. An example of how to do this can be found in the section entitled "Creating a Certificate Authority with OpenSSL" later in this document.

2. Load the CA Certificate in every Cobalt device. Figure 9 shows how to do this.
3. Do one of the following:
    a. Generate matched Key/Certificate pairs (signed by the CA) for each Cobalt device, and upload these using the process shown in Figure 6.
        or
    b. Generate a CSR in each Cobalt device using the process shown in Figure 7. Have the CA process the CSR to generate a certificate. Upload the certificate back into the Cobalt device using the process shown in Figure 6.
4. Configure the Cobalt device to use the user-supplied credentials, as shown in Figure 5.

The most secure is 3(3.b) above, since keys are never transmitted anywhere. However, it is the most labor-intensive. This process is illustrated in Figure 8.
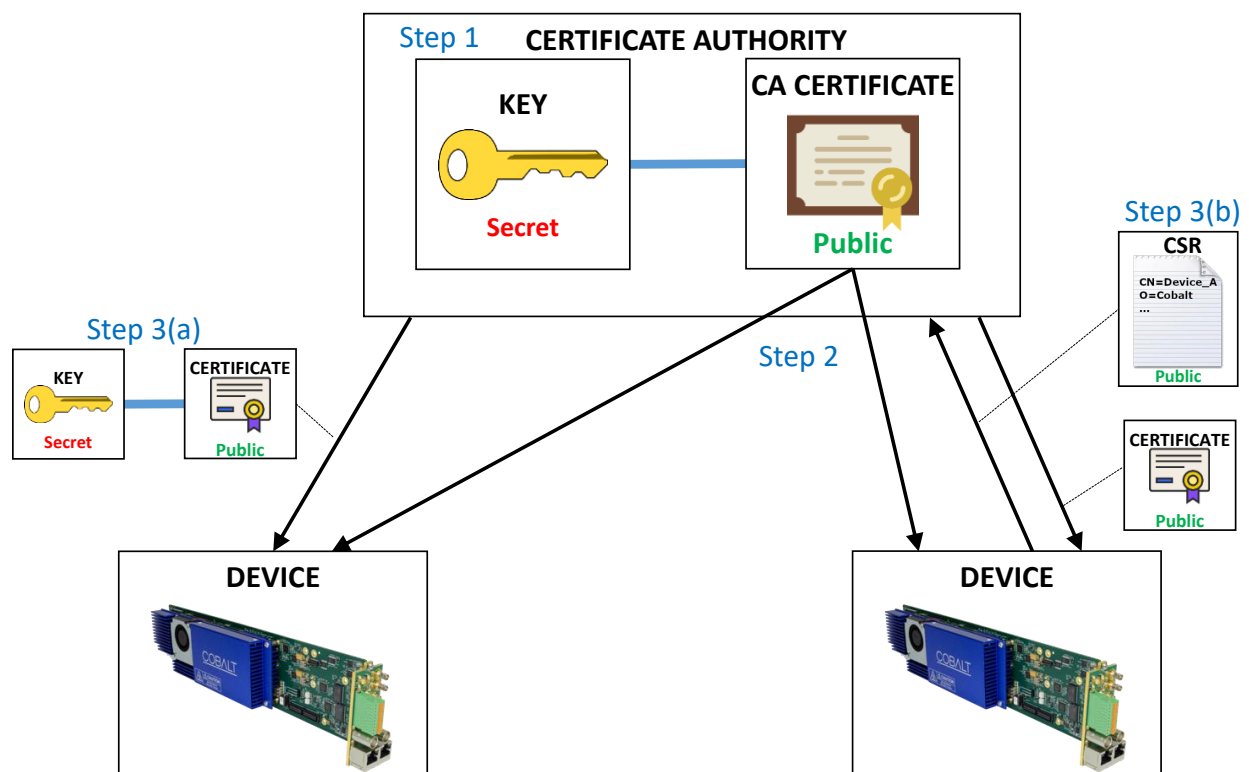

Figure 8: Using an external Certificate Authority

The process of loading an external CA certificate in the Cobalt device (Step 2) is shown in Figure 9:

- Open the device's web page and select <u>Click here for RIST Authentication Management</u>.
- In the **Uploading an External CA Certificate**, use the **Browse** button to find the PEM file with the certificate.
- Enter the device password and click on the **Upload CA Certificate** button.

The device will check out the certificate for correctness and validity, and, if accepted, will save it. If the certificate is accepted, it can now be selected in DashBoard, as shown in Figure 9.
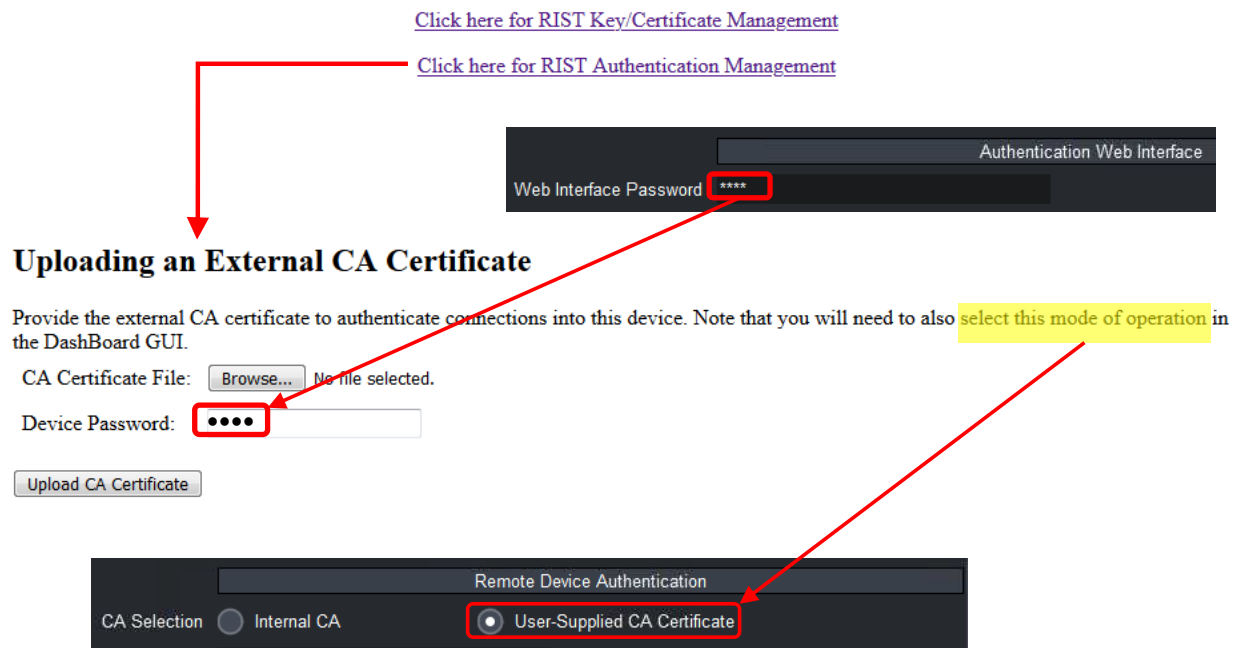
Figure 9: Uploading an External CA Certificate

Option 2: Using one of the Cobalt Devices as the Certificate Authority

This is similar to Option 1, but instead of a separate CA, one of the Cobalt devices is used as the CA. This option is less secure than Option since the CA is one of the devices participating in the network. The steps are:

1. Pick one of the Cobalt devices as the CA for your network. This device will be configured to use the internal CA and internal credentials. The CA key for this device **<u>MUST</u>** be downloaded and backed up.
2. Copy the CA certificate from the device chosen as the CA into all the other devices in the network. Configure all other devices to use this CA certificate.
3. Generate a CSR from each device in the network, have it signed by the CA device, and install the resulting certificate back in the device. Cobalt devices working as a CA can only sign certificates – client key generation is not supported.
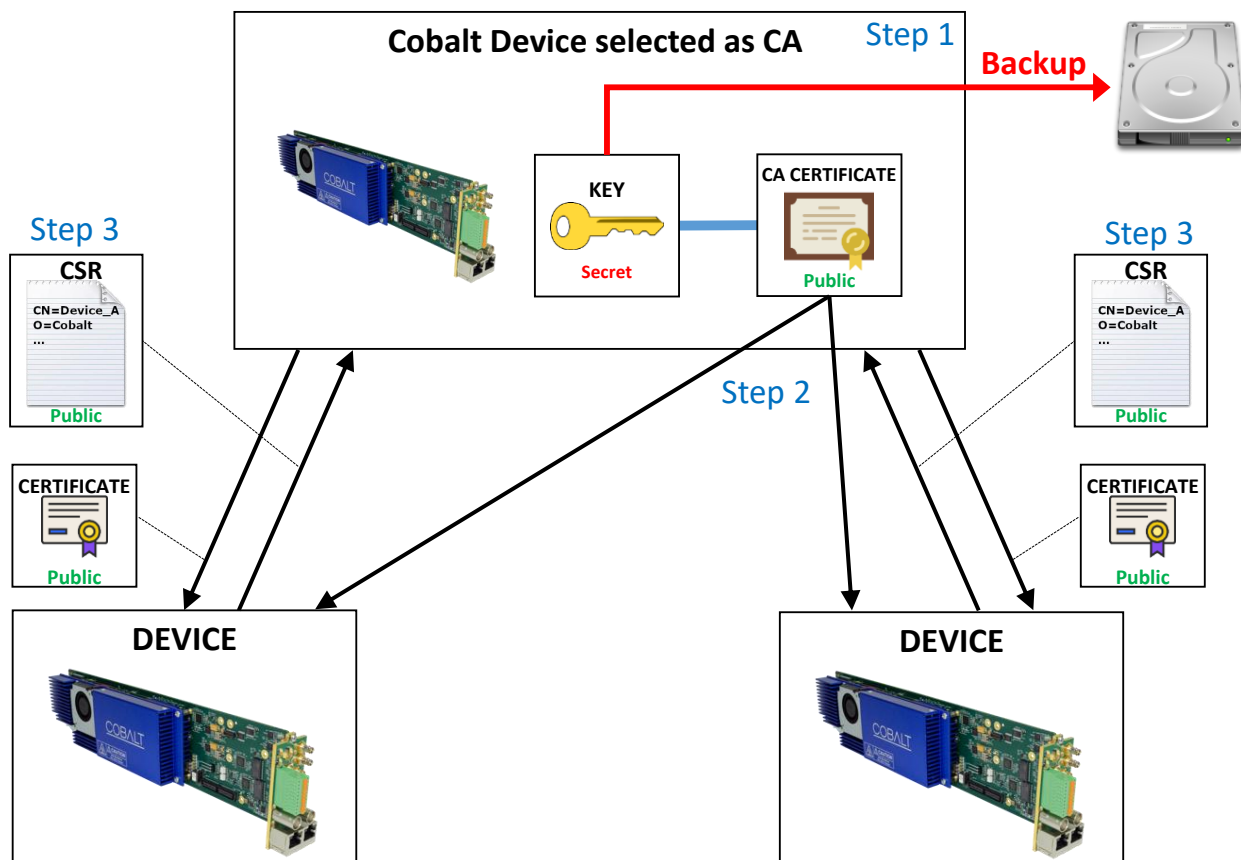
Figure 10 illustrates the whole process.

Figure 10: Using a Cobalt Device as the CA

Step 1 indicates that the CA Key for the device selected as CA must be downloaded for backup purposes. If that device is ever damaged or lost, the key can be installed on an alternate device. The CA Key can be downloaded in the DashBoard **Authentication** tab, as shown in Figure 11, by clicking on the **Save** button. Note the following:

- The default filename is **CA_KEY.BIN**, but it can be renamed as desired. Keep the extension as .BIN so as it is recognized by DashBoard.
- The file should be copied to a secure location.
- The file is encrypted and uses a proprietary format.   It is not compatible with any of the usual TLS software packages.   This is done as an additional level of security in case an unauthorized third-party obtains a copy of the file. However, any supported Cobalt device can use this file, so the best strategy is to keep the backup secure.

Uploading a saved key file to a Cobalt device is done through DashBoard, in a similar fashion as a firmware update. Open the device, click on the **Upload** button at the bottom of the screen, and navigate to the CA_KEY.BIN. Once the file is uploaded, the Cobalt device will automatically re-generate all the internal certificates.
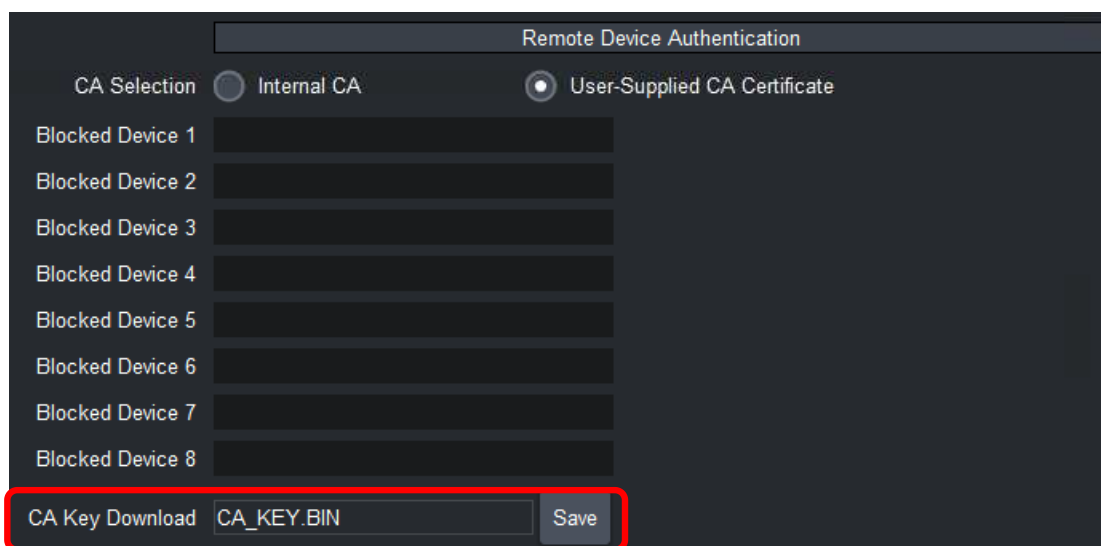
Figure 11: Downloading the device's internal CA key

The original device CA key is saved when a new key is uploaded. It can be restored at any time using the **Restore CA Key** button in the **Authentication** tab in DashBoard. This is illustrated in Figure 12.
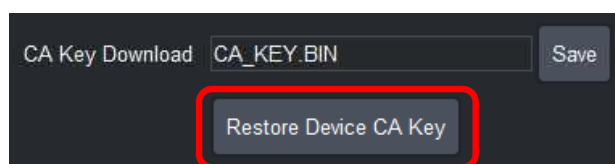

Figure 12: Restoring the original CA key

Figure 13 shows how to obtain the device's internal CA certificate for Step 2. No password is needed because the certificate does not need to be kept confidential. Use the process shown in Figure 9 to install the CA certificate in each Cobalt device.
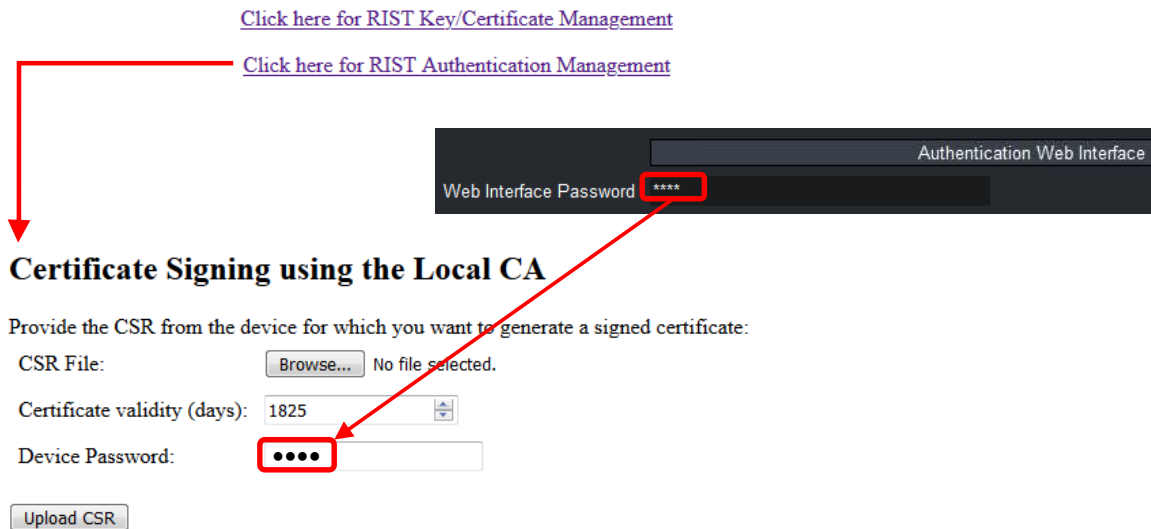
Figure 13: Downloading the internal CA Certificate

In Step 3 a CSR is generated for each device and signed by the CA device. The CSR generation for Cobalt devices is covered in the section entitled "Obtaining a CSR for the Built-In Keys". Figure 14 shows the process of signing a certificate, which is done through the web interface.

141

Provide the CSR file, fill in the desired certificate duration (the default is 5 years), provide the device password, and click on the **Upload CSR** button. The CSR must be in PEM format and is validated. If the CSR is valid, a certificate will be generated and a link to download it from the device will be provided. The process of uploading a certificate back to the device was described in the section entitled "Uploading Keys and Certificates".

Figure 14: Signing a Certificate

Option 3: Using the same CA Key in all Cobalt Devices

As with Option 2, one of the Cobalt devices is arbitrarily picked as the CA. The CA Key for this device is downloaded and installed in all the other devices, so they all become copies of the same CA. When a new CA Key is uploaded into the Cobalt device, it automatically re-generates its internal certificates to match this key. In this mode, all devices use internal credentials and internal CA, and this works because all the internal CAs are the same. This process is illustrated in Figure 15. It is still recommended that key be backed up in a secure location.

As indicated before, uploading a key to a Cobalt device is done through DashBoard. It should be noted that DashBoard can upload a file to multiple devices in parallel. This is a convenient way to distribute a key to multiple devices. DashBoard will automatically show all compatible devices to which the key can be uploaded.

This option is the least secure since a copy of the CA is in each device.
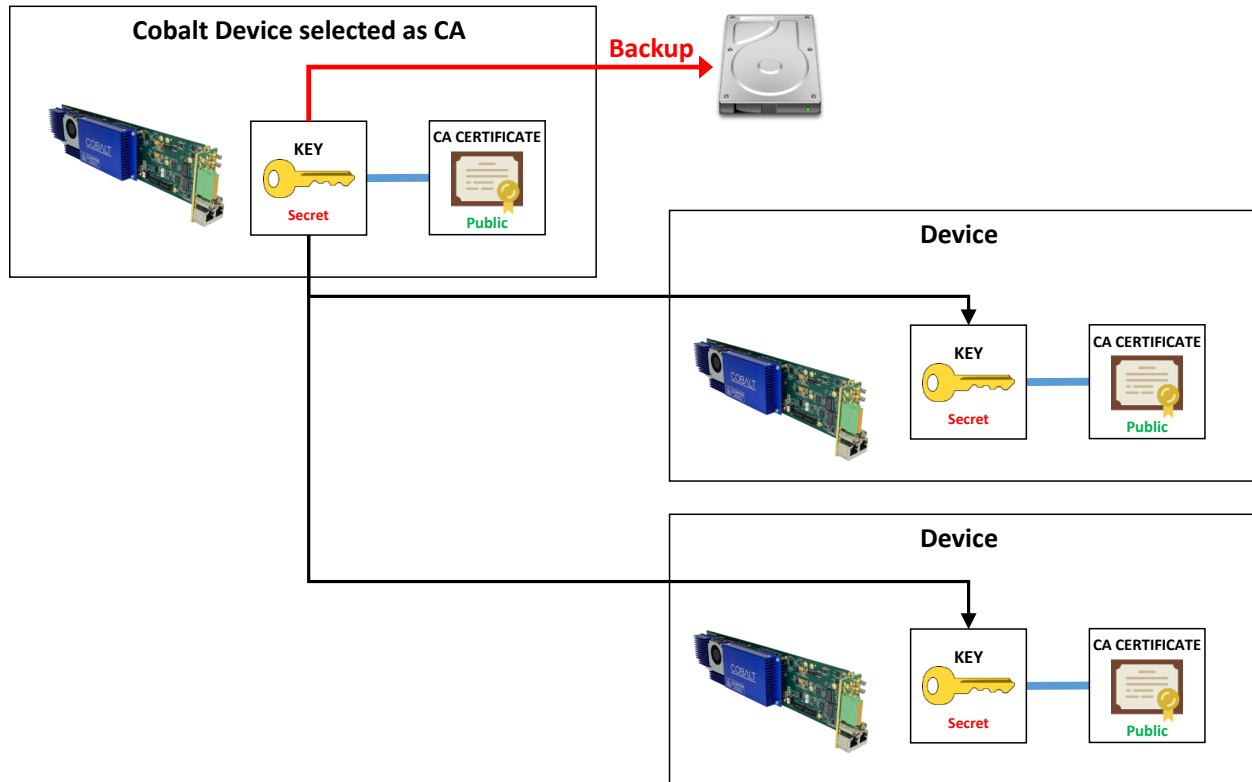
Figure 15: Copying the CA Key to all devices

Creating a Blocklist

In some situations, it may be necessary to block a device that was previously authorized to connect. The device presents valid credentials (i.e., a certificate signed by the trusted CA) but it should not be allowed to connect anymore.

This can be done in the Blocked Device list in the **Authentication** tab in DashBoard, show in Figure 16.

Up to 8 devices not allowed to connect
Devices identified by **Common Name**

Figure 16: Blocked Device List

Devices are identified by the **Common Name (CN)** field in the certificate tied to the RSA or ECDSA keys. The Common Name is set as follows:

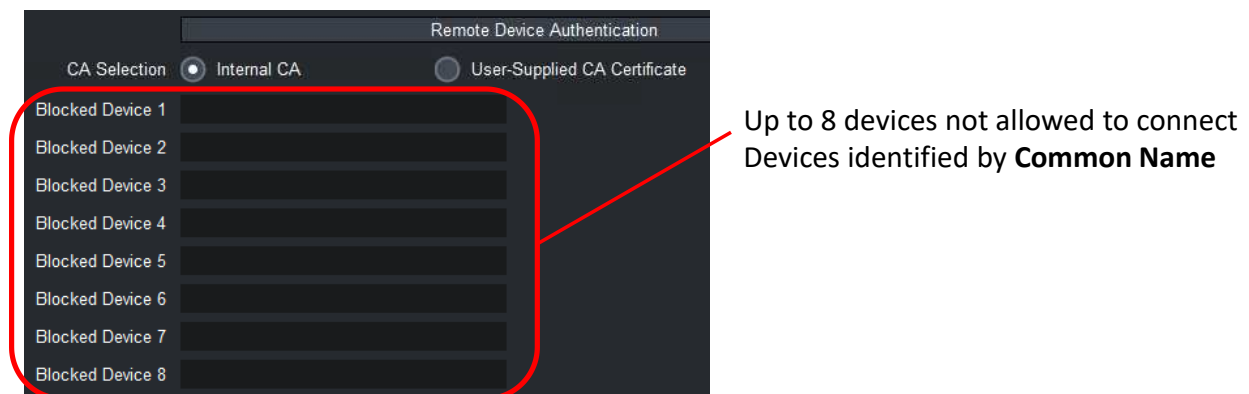- If the device is using the built-in credentials, the Common Name is set to **Product_MACAddress**. For example, **9992-ENC_AC:83:F0:01:03:18.**
- If the device is using a certificate derived from a CSR from the device itself, the Common Name was set in the CSR, as described in the section "Obtaining a CSR for the Built-In Keys" and illustrated in Figure 7.
- If the device is using an externally-generated key/certificate pair, the Common Name is part of that certificate.

When a connection succeeds, the Common Name of the remote end is reported in the Statistics area, **Network** top tab, **Tunnel Stats** bottom tab, as indicated in Figure 17.

Figure 17: CN Reporting in the Statistics GUI

Creating a Certificate Authority with OpenSSL

This section shows how to create a private Certificate Authority with OpenSSL. Please note that Cobalt Digital cannot provide support for OpenSSL, these instructions are provided as-is. If you are using Linux, most distributions include OpenSSL, either by default or as an additional package. If you are using Windows, there are a number of ports available in the Internet. One such port can be found in this link. Note that OpenSSL is a command-line utility that needs to run in a terminal (or a "cmd" shell in Windows).
In the sections below, commands to be typed are in **black** and responses are in **purple**.

Generating the CA Key and Certificate

The first step is to generate the CA key, which must be kept secret. In this example, the key will be written to **CA_KEY.PEM**:
```
openssl genrsa -des3 -out CA_KEY.PEM 2048
```

144

```
Generating RSA private key, 2048 bit long modulus (2 primes)
...........................+++++
...+++++
e is 65537 (0x010001)
Enter pass phrase for CA_KEY.PEM:  (password is entered here)
Verifying - Enter pass phrase for CA_KEY.PEM:  (password is entered here)
```

The program will ask for a passphrase (password) for the key. Enter at least 4 characters and make a note of it, because this password will be needed for signing certificates.

The next step is to generate the CA Certificate from the key. One important parameter is long the certificate validity will be. In this example, the certificate will be written to **CA_CERT.PEM**, and the certificate validity will be set to 3650 days (10 years):

```
openssl req -x509 -new -nodes -key CA_KEY.PEM -sha256 -days 3650 -out CA_CERT.PEM
Enter pass phrase for CA_KEY.PEM:  (password is entered here)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Illinois
Locality Name (eg, city) []:Champaign
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cobalt Digital
Organizational Unit Name (eg, section) []:Compression
Common Name (e.g. server FQDN or YOUR name) []:CA-SERVER
Email Address []:support@cobaltdigital.com
```

You can fill the fields as you wish but do not leave the Common Name blank. The Email Address field can be left blank.

If you intend to use this as the CA for Cobalt devices, upload the **CA_CERT.PEM** file using the procedure illustrated in Figure 9.

Generating Device Keys

The following command generates an RSA key and writes it to **RSA_KEY.PEM**:

```
openssl genrsa -out RSA_KEY.PEM 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
........+++++
...........+++++
e is 65537 (0x010001)
```

The following command generates an ECDSA key and writes it to **ECDSA_KEY.PEM:**

```
openssl ecparam -name secp521r1 -genkey -param_enc explicit -out ECDSA_KEY.PEM
```

(No output is generated in the terminal.)

Generating CSRs

In order to have certificates signed by your CA, you will need to generate a CSR for each key. The CSR generation procedure is the same for RSA and ECDSA keys. In the example below, we are generating a CSR for the key in **RSA_KEY.PEM** and writing it to **RSA_CERT.CSR:**

```
openssl req -new -key RSA_KEY.PEM -out RSA_CERT.CSR
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
```

```
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Illinois
Locality Name (eg, city) []:Champaign
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cobalt Digital
Organizational Unit Name (eg, section) []:Compression
Common Name (e.g. server FQDN or YOUR name) []:Encoder-Device
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

The most important parameter is the **Common Name**. Select something unique for each device. Also, leave the challenge password empty.

Repeat the same steps to generate a CSR for the ECDSA key if desired.

Generating Signed Certificates from the CSRs

The procedure here is the same regardless of where the CSRs come from. You can use CSRs from your keys generated in the previous step, or you can get CSRs from the Cobalt device as described in the section "Obtaining a CSR for the Built-In Keys".

In the example below, we take the CSR in **RSA_CERT.CSR** and sign it with the CA Key in **CA_KEY.PEM** and the CA Certificate in **CA_CERT.PEM**, generating a certificate that is good for 3650 days (10 years), and write to **RSA_CERT.PEM**:

```
openssl x509 -req -in RSA_CERT.CSR -CA CA_CERT.PEM -CAkey CA_KEY.PEM -CAcreateserial -
out RSA_CERT.PEM -days 3650 -sha256
Signature ok
subject=C = US, ST = Illinois, L = Champaign, O = Cobalt Digital, OU = Compression, CN
= Encoder-Device
Getting CA Private Key
Enter pass phrase for CA_KEY.PEM: (password is entered here)
```

At this point, the file **RSA_CERT.CSR** is no longer necessary and can be deleted. Repeat the same step for the ECDSA CSR if desired.

You can now upload the keys and certificates to the Cobalt devices using the procedure described in section "Uploading Keys and Certificates".