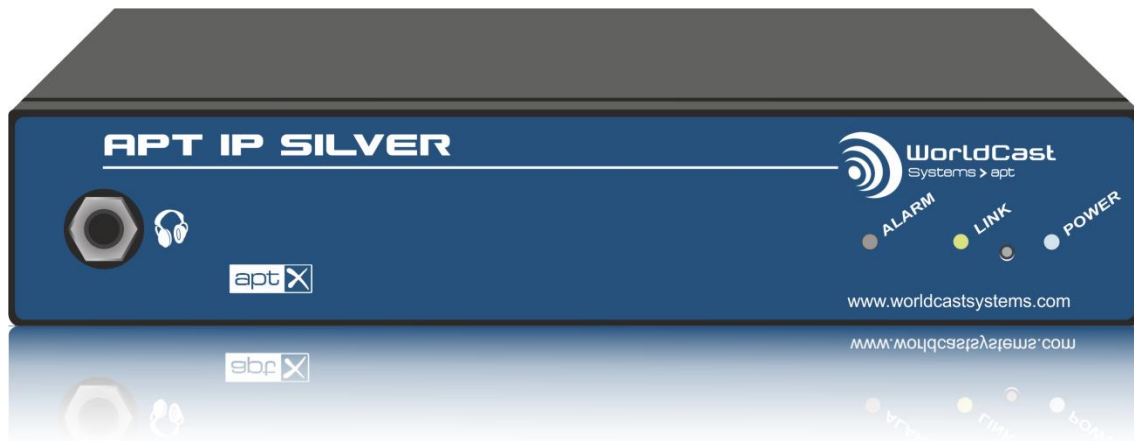


# WorldCast Systems APT IP Silver Encoder/ Decoder User manual



System Release 3.0.x | Document Version 2.2 | release/update: May 2018

## DECLARATION OF CONFORMANCE

Established following the Directives 99/5/EC and 2006/95/EC



We, hereby, certify that APT IP Silver Encoder/Decoder complies with the dispositions of the European Community Directive for harmonized standards within the Member States related to radio equipment and telecommunications terminal equipment (Directive 99/5/EC) and low voltage (Directive 2006/95/EC).

**i** *This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.*

**⚠** The APT IP Silver Streamer is available only with XLR connectors. The RCA version has been discontinued.

### Installation and Operational Manual:

#### **APT IP Streamer Encoder/Decoder**

System Release 3.0.x / May 2018

© Copyright 2011/2018 by WorldCast Systems. All rights reserved.

No part of this publication is permitted to be reproduced, stored in a retrieval system, transmitted by any means, electronically, mechanically or otherwise, without written consent of WorldCast Systems.

#### **Warranty**

All information is believed to be true and correct at time of print. WorldCast Systems reserves the right to make any changes, without notification, to their products and manual. WorldCast Systems makes no warranty of any kind with regards to this material, including the implied warranties of merchantability and fitness for a particular purpose.

WorldCast Systems shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance or use of this material.

#### **Trademarks**

aptX® and aptX® Enhanced are registered trademarks of Qualcomm/CSR. Other trademarks are the property of their respective owners.

### **How to contact us:**



#### **WorldCast Systems Head Office**

20, avenue Neil Armstrong - Parc d'Activités J.F. Kennedy  
33700 BORDEAUX – MERIGNAC  
FRANCE  
Tel: +33 (5)57 928 928 | Fax: +33 (5)57 928 929

#### **Americas Office**

19595 NE 10th Ave, Suite A  
Miami FL 33179  
USA  
Tel: +1 (305)249 31 10 | Fax: +1 (305) 249 31 13

#### **How to get support**

If you have a technical question or issue with your APT equipment, please consult the support section of our website at:

<http://www.worldcastsystems.com> or

[apt-cust-support@worldcastsystems.com](mailto:apt-cust-support@worldcastsystems.com)

## Table of Contents

<b>Table of Contents</b>	<b>4</b>
<b>Safety &amp; Disposing Information</b>	<b>6</b>
<b>Precautions regarding the lithium battery present in the device</b>	<b>6</b>
2.1.1.1 Monitoring	16
2.1.1.2 Power- Connection - and Alarm Status	16
2.1.1.3 Reset Switch – Default IP Addresses	16
3.1.1.1 Browser Cache	20
3.2.3.1 CPU Utilization	24
3.3.2.1 Audio Alarms Section	30
3.3.2.2 Transport Alarms	31
3.3.2.3 Loss of Physical Connection	31
3.3.2.4 Dynamic DNS Alarms	31
3.3.2.5 NTP Alarm	31
3.3.3.2 IP Statistics - Details	33
3.3.3.3 Packet Re-Sequencer	33
3.3.3.4 About Stream Tables (general)	34
3.4.5.1 Embedded AUX Data (Using Serial Port)	38
3.4.6.1 Auto Detection of Incoming Streams	39
3.4.9.1 About Stream Types	44
3.4.10.1 IP Forwarding - UDP Forwarding	45
3.4.10.2 Media Forwarding - RTP Forwarding	47
3.4.10.3 UDP/RTP Re-Encapsulation	49
3.4.11.1 Transmit (Tx) Encoder	50
3.4.11.2 About Packet Sizes	53
3.4.11.3 Packet Sizes of Framed Algorithms	53
3.4.11.4 Receive (Rx) Decoder	54
3.4.12.1 About Packet Size of AUX Data treams	57
3.4.13.1 Audio Stream Receive, decode and prepare Forwarding	58
3.4.13.2 Forwarding an Audio Stream (Tx)	59
3.4.13.3 IP Stream Forwarding (UDP)	60
3.4.13.4 Combination of UDP/RTP Forwarding	61
3.4.14.1 Configuration Validation	64
3.5.1.1 NTP Client Settings	67
3.5.1.2 NTP Synchronization Alarm	67
3.5.1.3 NTP Server general Considerations	67
3.5.2.1 User Accounts	68
3.5.2.2 FTP Accounts	69
3.5.2.3 Alarms / MasterView 2.0 Recipients Accounts	69



3.5.3.1	Network - Network	70
3.5.3.2	Advanced Network Configuration	73
3.5.3.3	UPnP - NAT Traversal Mode	73
3.5.3.4	Dynamic DNS	74
3.5.3.5	DNS Look Up - mDNS	76
3.5.3.6	Virtual IP Interfaces	76
3.5.3.7	VLAN Tagging – Virtual LAN	77
3.5.3.8	Firewall	78
3.5.6.1	SNMP Agent	81
3.5.6.2	SNMP MIB Files	81
3.5.6.3	SNMP Remote Manager	82
3.5.7.1	Application Builder	83
3.5.7.2	Application	84
3.5.7.3	MasterView	85
3.5.7.4	MasterView Dashboard Designer	86
3.5.7.5	ScriptEasy Control	87
3.5.7.6	ScriptEasy Remove a Script	87
3.5.8.1	Event Log File Export	88
3.5.9.1	Backup/Restore Unit Configuration	89
3.5.9.2	Firmware Update	91
3.5.11.1	SSL Certificate Authority	94
3.5.11.2	Chat Box	95
3.6.1.1	Audio Configuration Options	99
3.6.1.2	Analog I/O Clip Levels (XLR)	100
3.6.1.3	Low Latency Mode	100
3.6.1.4	Encoder and Decoder Mono Modes	100
3.6.2.1	Sync. Alarm Fail Time (Decoder only)	101
3.6.2.2	Unit Clock Mode	101
3.6.2.3	Advanced Routing (Decoder only)	102
3.6.7.1	How to Create a Custom Alarm ( <i>continued</i> )	108
4.3.1.1	Reading performance information from the component streams	116
4.3.1.2	Creating a Monitor Stream	117
4.3.1.3	Performance Information with a Monitor Stream	118

## Safety & Disposing Information

The APT IP Silver Encoder / Decoder Audio devices are powered by an external switching power adapter. If a product defect occurs on the power adapter this adapter must be replaced. There are no user-serviceable parts inside.





TO PREVENT THE RISK OF ELECTRIC SHOCK, DO NOT OPEN THE COVER OF THE POWER ADAPTER THERE ARE NO USER-SERVICEABLE PARTS INSIDE THIS UNIT. PLEASE REFER SERVICING TO QUALIFIED APT SERVICE PERSONNEL.



According to local laws and regulations, this product should not be disposed of in the household waste but sent for recycling.

## Precautions regarding the lithium battery present in the device

This device includes a rechargeable Lithium Vanadium Pentoxide battery. If the battery is not correctly replaced, there is a risk of explosion. Only replace it with a battery of the same type. Contact us before attempting to use another type.

-  Do not puncture the battery
-  Do not throw the battery in fire
-  Do not immerse the battery in water
-  Do not throw away the used battery, recycle it instead. You may send it back to us if needed.

## 1.0 About this Manual

Thank you for purchasing the APT IP Silver Audio Codec from APT. We have developed these units to be as user friendly as possible, and they contain many advanced features which are designed to make the use of this product simple and straightforward.

This operations manual is intended for operators of the APT IP Silver audio network transmission link. This manual describes the function, the installation and use of the unit.

It is recommended that new users of the APT IP Silver should read the full manual before switching it on for the first time, to get a better feel for the functionality and to eliminate any possible area of confusion.

### 1.1 Release Notes


This manual is the primary reference covering the configuration, installation, operation and troubleshooting of the APT IP Silver.

As of this publication date, this document is the current manual revision. We recommend that you check with your distributor or on the APT website for updates to firmware and this manual.

 *This Manual refers to System Release 3.0.x – May 2018*

#### 1.1.1 System Options for SR.3.0.x:

 **ScriptEasy version 2.8.7.001**

 **MasterView 2.1.0 web application** (desktop version not supported anymore)


### 1.2 Important Network Security Advice


#### 1.2.1 This IP Audio Codec is a network device!

As a network appliance, the APT IP Silver can create security vulnerability between your internal LAN and the WAN domain. The IP Silver units provide built-in firewall and policy routing capabilities, but you should make sure that your security installation is suitable to protect your LAN domain from possible attackers.

For further information, please also refer to section 1.7.



 *Before commissioning, we strongly recommend changing the default LogIn on the WEB GUI (refer to section 3.5.2)!*

 *Before connecting to your Network, please check the SNMP community strings. Don't use the trivial default names (refer to section 3.5.6.1).*

### 1.3 About WorldCast Systems

WorldCast Systems is a highly respected provider of professional, reliable and innovative solutions to the Radio & TV industry worldwide.

Encompassing the industry-leading brands of APT, Ecreso and Audemat, WorldCast Systems offers high-performing broadcast systems including audio codecs, FM transmitters and RF signal monitoring designed to meet the needs of both large international broadcast networks and small private stations alike. WorldCast Systems' products are deployed throughout the networks of many major public and commercial broadcasters such as the BBC, ARD, the EBU, RTE, TDF, RNE, Teracom, RAI, ORF and Clear Channel Radio

- ➔ **APT** codecs deliver audio over IP, T1, ISDN & Leased Lines. Our award-winning SureStream technology enables high quality audio transport over cost-effective IP links.
- ➔ **Ecreso** offers highly efficient FM transmitters with extensive inbuilt functionality, highly competitive Total Cost of Ownership and an industry-leading 10-year warranty.
- ➔ **Audemat** provides a range of professional monitoring and measurement tools for Radio & TV, complemented by an extensive range of remote control systems for management, configuration and monitoring of broadcast networks.

Three core values have shaped the growth and direction of WorldCast Systems

1. **Product innovation:**

Audemat places a key emphasis on Research & Development and its innovative approach has been repeatedly recognized by the industry. WorldCast Systems has won awards for innovation at consecutive NAB Shows for over 10 years.

2. **Customer satisfaction:**

Audemat is dedicated to ensuring the best quality, value and service for its customers and has achieved ISO 9001 certification.

3. **Sustainable Development:**

Audemat is committed to sustainable development and demonstrates this commitment in several ways: it has been ISO 14001 certified since 2007, adheres to the UN Global Compact project and all new products are developed in keeping with an eco-design philosophy and built within Audemat's low energy consumption factory.

Headquartered in Bordeaux-Merignac, France, WorldCast Systems employs nearly 100 people worldwide with an R&D center in Northern Ireland and sales offices in the UK, Germany, India and the US. A global distributor network works together with our international sales and support staff to offer local assistance to our international customer base.

## 1.4 Unpacking and Inspection

After unpacking:

- ➔ Check the unit for damage during shipping. Immediately report any damage back to the distributor or APT.
- ➔ Check that the list of contents is complete as follows:

### APT IP Silver

Serial Number located on the rear panel:

**APT IP Silver Encoder: K200-**  
**APT IP Silver Decoder: R200-**

(please complete)

### External Power Adapter

Please confirm that the local power supply voltage matches the required voltage levels of 100-240VAC.

### CD Box

A CD box including a Quick Start guide and a CD where you will find the documentation for this product.

Ethernet Port	Default IP Address	Port	DHCP / Static
ETH	192.168.100.110	http 80, https 443	Static



**ⓘ** *If the equipment supplied does not match the items requested please contact APT or your local distributor immediately and report any shortages.*

## 1.5 Introduction

The Apt IP Silver range (Encoder/Decoder) is based on the APT core engine for Codecs. This engine is designed to be as flexible and versatile in use as possible. The core is powerful and addresses the needs of professional IP audio transmissions.

The set of APT IP Silver Encoder/Decoder can be used to setup a full duplex link. The Silver Codec range consists of the Encoder and the Decoder as separate units in a ½ 1U format.

As a multi-algorithm audio Encoder or Decoder, it is offering standard analog left and right audio connections operating through IP. These analog audio connections are carried out for semi-professional phone jacks (legacy) or as professional XLR connectors.

The new Codec generation incorporates the enhanced versions of the aptX® Enhanced algorithm (real time transmission on the network with data reduction by factor 4:1) Linear PCM 16 and 24 bit as well as MPEG 2/4 HE-AACv1/2.

The units can deliver high-quality audio used for inter-studio networking, remote/outside broadcasts, and STL/TSL monitor applications.

Audio modes and bandwidths are dependent on the network bit rate, the algorithm, mode and frequency response selected and the bit resolution of the desired audio.

The Silver Codec range runs an embedded WEB GUI which can be accessed from a web browser or via the WorldCast Codec Management System which runs on a PC connected via LAN or WAN. A headphone socket provides for additional monitoring of the audio input (Encoder) or the output (Decoder)

An Additional interface allows for the connection of auxiliary data terminated on a DB-9-way connector. Regardless of using the Encoder or the Decoder the AUX Data link is always provided as a duplex link (while the audio is always simplex).

The APT IP Silver is delivered with the SureStream option applied as standard.

Both units are very similar with the exception that the Decoder offers an additional USB port for future use (e.g. playing out stored audio files).

Script Easy is an application builder for enhanced management and control of a Codec device. In addition, ScriptEasy applications allow the user to communicate and control external equipment using SNMP protocol GET/SET commands. MasterView allows creating customized dashboards of an application to be able to check the equipment status and to perform user actions remotely with a web browser.

Script Easy and MasterView are implemented as standard.

## 1.6 Getting Connected

This chapter outlines how you can quickly connect your IP Silver Streamer and start sending audio. Begin by connecting the power adapter to the unit.

### Making a connection and send audio:

- ➔ Set up the Encoder and the transmitting IP stream
- ➔ apply this configuration to the unit
- ➔ Set up the Decoder and the receiving IP stream
- ➔ Apply these settings to the unit

The audio connections are made on the rear panel using RCA phone jacks (legacy) or XLR type connectors.

### APT IP Silver Encoder / RCA (legacy)



Figure 1-1: IP Silver Encoder (legacy RCA version) rear panel view

### APT IP Silver Decoder / XLR

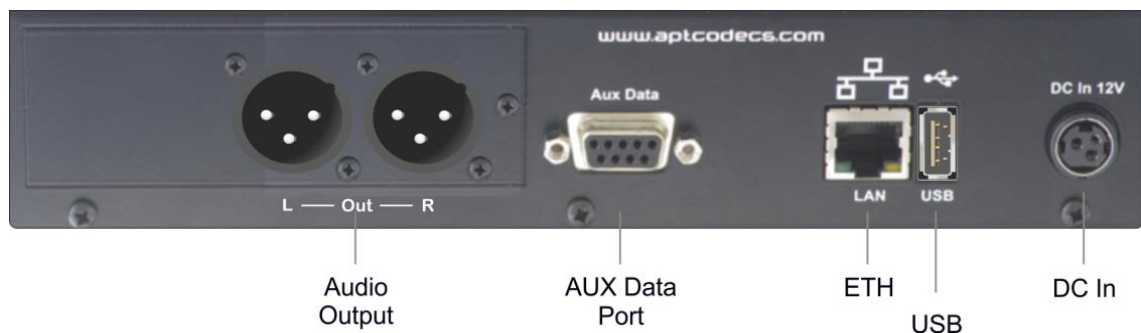


Figure 1-2: IP Silver Decoder (Decoder XLR version) rear panel view

## 1.7 IT Security Recommendations

### 1.7.1 APT IP Silver – Network Connection

IP codecs are network devices; therefore, they should be seen as such. An IP audio Codec must be connected to the IP network via a switch or router providing sufficient firewall mechanisms to protect the audio service and the connected network against external attacks. All network related security rules are valid for an IP codec as well.

The image below shows the principle of the network connection via the ETH port. The ETH port must be used for management access and audio streaming. Therefore, care must be taken that the management TCP/UDP ports are inaccessible on the streaming network (the external network).

APT IP Silver devices are VLAN aware and provide a sufficient network separation.

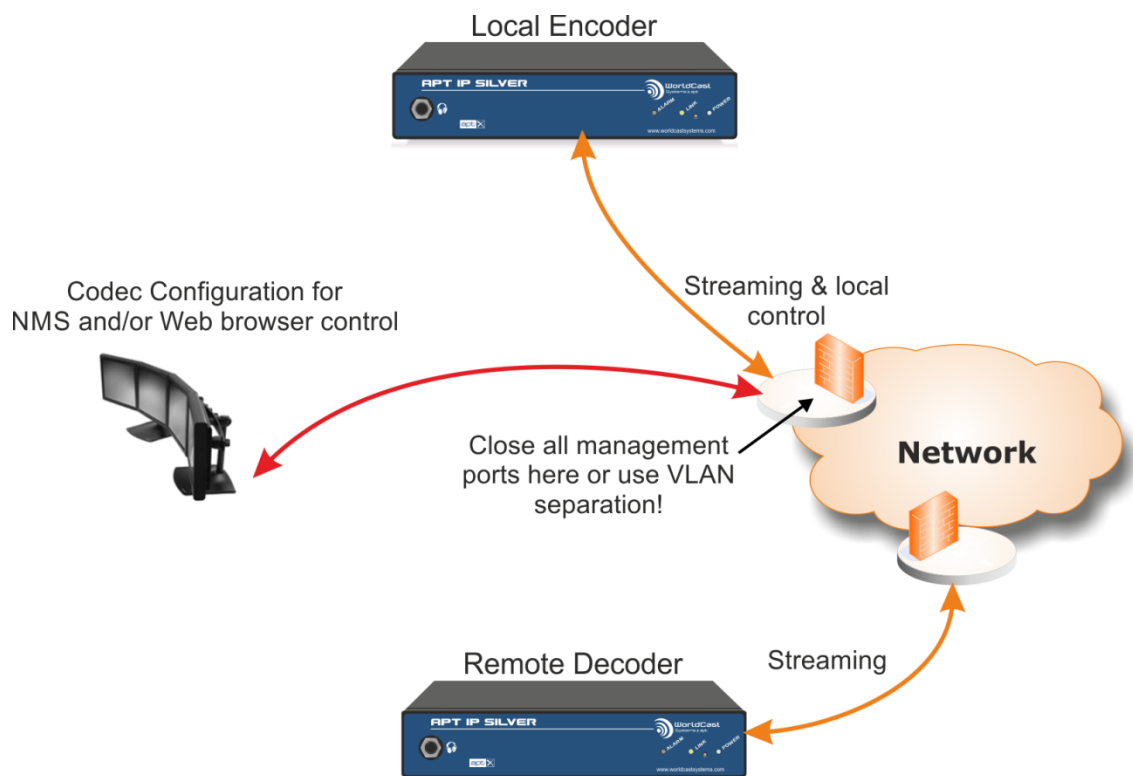



Figure 1-3: This figure shows the recommended network installation: IP Silver connected to a switch with firewall mechanism (or VLAN aware switch).

 Make sure that the firewall configuration of the Codec device suits your security policy.



## 1.8 Connecting via Web Browser

In most cases, the device is controlled and managed using a standard web browser. On default, no service filter is enabled with the factory default configuration.

Ethernet Port	Default IP Address	Port	DHCP / Static
ETH0	192.168.100.110	http 80, https 443	Static

### 1.8.1 Firewall Service Filter – internally managed Ports

The following table shows the TCP/UDP ports that should be taken into consideration while planning your security. The internal firewall allows some port management on the ETH interface.

Port	Service	Protection
TCP 80	HTTP, WEB Services (rerouted to 443)	Internal firewall
TCP 443	HTTPS, Web Services	Internal firewall
TCP/UDP 111	RPC	External
TCP 21	FTP	Internally protected
UDP 161	SNMP	Internal firewall
UDP 162	SNMP TRAP	Internal firewall
UDP 5577	Internally used	External
UDP 7777	APT NMS communication	External
UDP 7778	APT NMS communication	External

#### Notes:

---



---



---



---



---



---



---




---

## 1.8.2 Default LogIn and Services

### **Passwords**

The Web GUI and the NMS are protected by a user login. The default passwords are trivial password only, like “admin” or “password”. It is evident, that these passwords are insufficient for regular use. Furthermore, it is a negligent behavior if this default login has not been changed before connecting to a network. Please refer to section 3.5.2 about how to replace the Web GUI login.

 Before commissioning the unit, we firmly recommend changing the default LogIn on the WEB GUI. Never use the default login for regular operation on an open network segment.

### **SNMP**

The default names of the community strings must not be used for the regular operation. The default names of community strings, especially the Private Community, are widely used and therefore commonly known. Because SNMPv2c does not support password protection of the strings, the recommendation is clearly to create the names as “cryptic” as possible. Refer to section 3.5.6.1 about how to change the community string name.

 *The names of the SNMP community strings must be changed even if SNMP is not used!*

### **FTP Account**

The FTP service is only used by ScriptEasy when a new script is loaded into the unit. The user can manage the FTP login (user management), and on the Firewall, the FTP service can be disabled on any or all ports.

#### Notes:

---

---

---

---

---

---

---

---

---

---

## 2.0 Installation and Wiring

This chapter describes the general installation procedure and the wiring of the Silver unit's rear panel connectors. This section consists of two parts:

- ➔ Preparing for installation of the APT IP Silver Encoder and Decoder
- ➔ Wiring power and signal connectors

### 2.1 Tools and Cables Required

In addition to the content of the packing list, the following items are necessary to complete the installation.

 **Network/Management connection cables**

For Ethernet connections, you need one or more CAT5 cables. The ETH ports are **Auto MDI-X\*** capable; this allows using any Ethernet cable (crossover or straight-through).

 **Ethernet switch:**

Providing an Ethernet switch facilitate the audio IP link and the management connection simultaneously

 **Cables for each Audio signals:**

At least one standard audio cable equipped with RCA or XLR connectors (depends on the version of the unit)

 **Power Adapter:**

AC power adapter as supplied with the Silver unit

*\* In the past, the general convention for network hubs and switches was to use the MDI-X (Media Dependent **crossover** Interface) internal wiring, while all other network nodes used an MDI interface (Media Dependent Interface).*

**Auto MDI-X** ports detect if the connection requires a crossover cable, and automatically chooses the MDI or MDI-X configuration to match the other end of the link.

Notes: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## 2.1.1 Front panel Components



Figure 2-1: APT IP Silver front panel components

### 2.1.1.1 Monitoring

(1) The 6.3mm jack socket is provided for audio monitoring with a headset or active monitor speaker. Depending on the type of Silver unit it is either the audio input (Encoder) or the audio output (Decoder). This monitor output has a fixed signal level and is not adjustable.

### 2.1.1.2 Power- Connection - and Alarm Status

(2) The blue Power LED indicates that power is applied to the unit

The red Alarm indicator LED indicates that an alarm condition exists. There are a number of alarm conditions which can be enabled on the Silver range.

The "Link" LED shows the presence of a connection. The following table shows the different states of the LED.

Link LED Color:	Off / Grey	Yellow	Red
No Stream enabled	<b>X</b>		
Receiving or Transmitting ok		<b>X</b>	
Connection Error			<b>X</b>

### 2.1.1.3 Reset Switch – Default IP Addresses

(2) Between the "Connected" and the "Power" LED there is a small hole in the front panel. Behind this hole sits the IP Address Reset Switch. To change the IP Address of the IP Silver units to the default address; insert a small tool and press the switch. Hold it in place until the Alarm and the Link LEDs start flashing (about 5 seconds) – then remove it.

The unit will then have changed the IP address; you do not need to reboot. It will take a short while (~10sec) until the Web GUI will be accessible again on the default addresses.

① *The default IP address of the ETH is: **192.168.100.110***

## 2.2 Wiring Information

### IP Silver Encoder /XLR

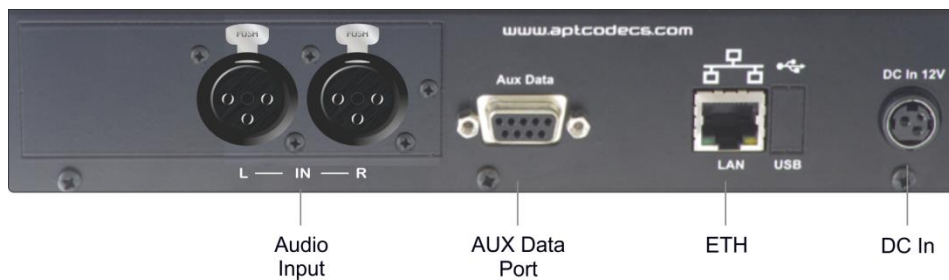


Figure 2-2: APT IP Silver Encoder rear panel components (XLR)

### IP Silver Decoder/XLR

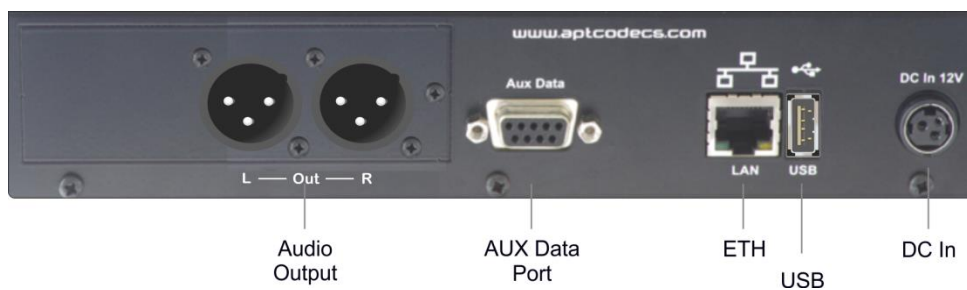


Figure 2-3: APT IP Silver Decoder rear panel components (XLR)

#### 2.2.1 Power Adaptor – DC In

The Silver units are supplied with an external Mains power adaptor suitable to work between 100 VAC and 240 VAC. This power adaptor applies 12 VDC to the unit and has a self-locking connector.

**ⓘ** Do not use another type of AC adaptor than supplied with the unit

#### 2.2.2 Ethernet Interface

This is a 10/100BaseT Ethernet connection with Auto MDI/MDI-X capability on a RJ45 connector.

### 2.2.3 Audio Inputs and Outputs on XLR version

The audio inputs on the XLR version accept up to +24 dBu (clip level)

The audio outputs on the XLR version deliver up to +24 dBu (clip level)

#### Analog Audio Input (Encoder)



Standard XLR-3 female socket

Pin	Description
1	screen
2	hot (+ve)
3	cold (-ve)

The analog input level can be adjusted via the Web GUI in increments of 0.1 dBu. The input impedance is selectable between 600  $\Omega$  and >10 k $\Omega$  on the Web GUI.

#### Analog Audio Output (Decoder)



Standard XLR-3 male socket

Pin	Description
1	Screen
2	hot (+ve)
3	cold (-ve)

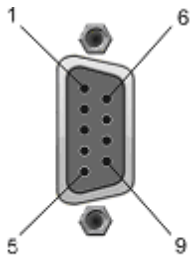
The analog output level can be adjusted via the Web GUI in increments of 0.1 dBu. The output impedance is selectable between 600  $\Omega$  and 50  $\Omega$  on the Web GUI.

### 2.2.4 Audio Inputs and Outputs on RCA version

The audio inputs on the RCA version accept line level up to +10 dBu (clip level). The input clip level (internally referenced to digital full scale) can be adjusted in increments of 0.1 dBu from 0 dBu to +10 dBu.

The audio outputs on the RCA version deliver line level up to +10 dBu (clip level). The output clip level (internally referenced to digital full scale) can be adjusted in increments of 0.1 dBu from 0 dBu to +10 dBu.

## 2.2.5 Auxiliary Data Interface



9 pin female connector contact view

This is a SELV connection and must only be connected to other SELV ports.

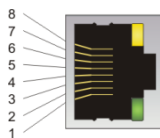
### RS-232 (DTE) Serial Inputs

Pin	Signal	Description
1	N-C	Not connected
2	Rx	RS-232 Receive
3	Tx	RS-232 Transmit
4	DTR	Not connected
5	GND	Ground
6	N-C	Not connected
7	N-C	Not connected
8	N-C	Not connected
9	N-C	Not connected

The RS232 auxiliary data channel of the Silver units offer continuous data transfer rates from 1.200 to 115.200 Baud (non-embedded on AUX IP-Streams).

**i** An AUX DATA connection on the Silver units can be configured for duplex operation (even that the audio is always simplex).

## 2.2.6 Ethernet Interface



10BaseT socket wiring scheme

### Ethernet Interface

Pin	Signal	Description
1	Tx +	Transmit data +ve
2	Tx -	Transmit data -ve
3	Rx -	Receive data -ve
4	N-C	Not connected
5	N-C	Not connected
6	Rx +	Receive data +ve

This Ethernet interface is available for both connecting to a PC running the WorldCast NMS (or WEB browser) and for sending and receiving audio data.

This ETH port is auto MDI/X enabled. An **Auto-MDI/X** port detects if the connection would require a crossover link, and automatically chooses the MDI or MDIX configuration to match the other end of the link properly.

## 3.0 WorldCast/IP Silver WEB-Browser GUI

The WorldCast/IP Silver Web GUI is the control and monitoring tool which communicates with the IP Silver units. All the next generation units, including the Silver range, run their own Webserver which can connect to standard Web Browsers or to the APT NMS. It is used to configure the unit, create audio streams and to get status and alarm information. It is also possible to make and to drop calls by using predefined profiles.


This section outlines this application and provides a detailed description of all aspects of the IP Silver configuration options.

### 3.1 The WorldCast WEB GUI - Overview

The Web GUI allows you to view and control a single instance of the IP Silver Streamer. The application has an intuitive look and feel that is easy to understand by both the experienced technician and the casual user. All configuration instructions described in this section relate to the WEB GUI. This section provides detailed step-by-step instructions on how to set up the APT IP Silver.


#### 3.1.1 Web Browser

In most cases, the device is controlled and managed using a standard web browser. By default, the web browser access for management is possible on Ethernet port; no service filter is enabled with the factory default configuration.

 For security reasons you should close all services on the Ethernet port where these services are not used before you connect the unit to the network.

You can connect the WorldCast Web GUI to a standard web browser such as:

Mozilla Firefox, Google Chrome, Safari, Internet Explorer v9 and higher as well as MS Edge

 *Recommended screen/window size: min. 1280px by 1024px*

The GUI is a web application utilizing standard browser technologies: JavaScript, cookies and CSS (2.0/3.0). The application does not require installing any additional browser add-ons and does not utilize the Java runtime environment. The cookies are session cookies used as temporary storage for configuration changes until they are uploaded to the hardware. A session cookie expires after the actual session is closed.

The Secure Socket Layer connection (https) to the IP Silver requires installing the WorldCast Systems SSL Certificate. You can download the certificate from the unit (refer to section 3.5.11.1)

#### 3.1.1.1 Browser Cache

The browser cache is used to hold mainly static parts of the web pages in the PC memory. However, there are situations where the browser cache cannot be updated correctly and a manual page refresh will be necessary (reload, ignoring cache).

After the following actions, we recommend reloading the web page manually:

1. After firmware update
2. If any kind of page error appears (corrupted appearance)
3. If an IP address is re-used, that was previously assigned to another device.





## 3.2 WEB GUI – Getting Started

Open your preferred web browser and type in the IP address of the Codec you like to configure, and you will be prompted with the LogIn screen.

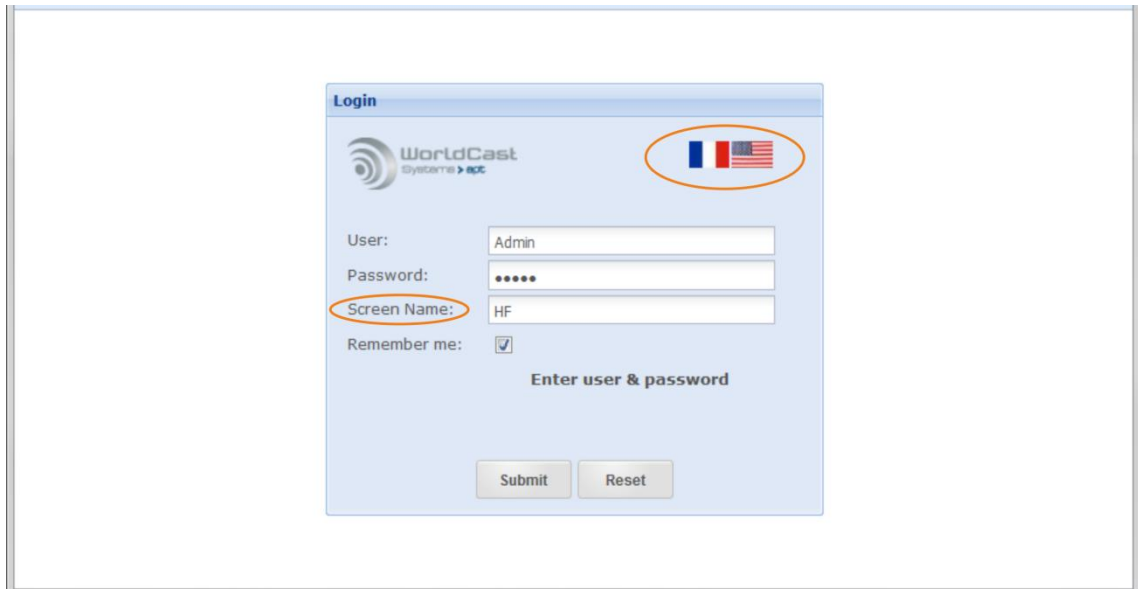


Figure 3-1: The WEB GUI LogIn screen

The multi-lingual GUI currently provides two languages, French and English. Clicking on the flags reloads the screen with the selected language.

The Screen Name can be anything but blank. If two or more users are connected at once, they can chat through the Web GUI, and this Screen Name will be used to identify the participants.

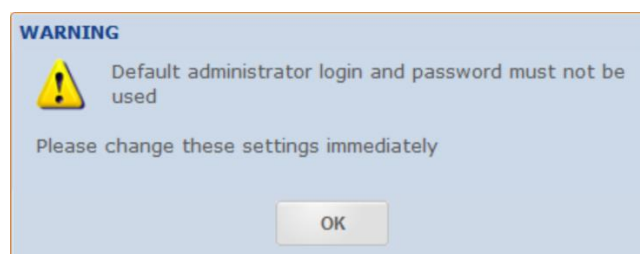
Activating the tick box "Remember me" allows the browser to remember your last LogIn for a new session.

### 3.2.1 Default LogIn

By default, the Administrator account is selected. The user management allows modifying this account, and it also allows setup a read-only account.

**i** *Default LogIn, User: Admin - Password: admin*

A security alert will pop up if the default login has not been changed. This alert can be remedied only by changing the login.



**⚠** Never use the default login for regular operation in an unprotected network!

### 3.2.2 Loading and Locking

After you have submitted correctly the web browser starts loading the web application.

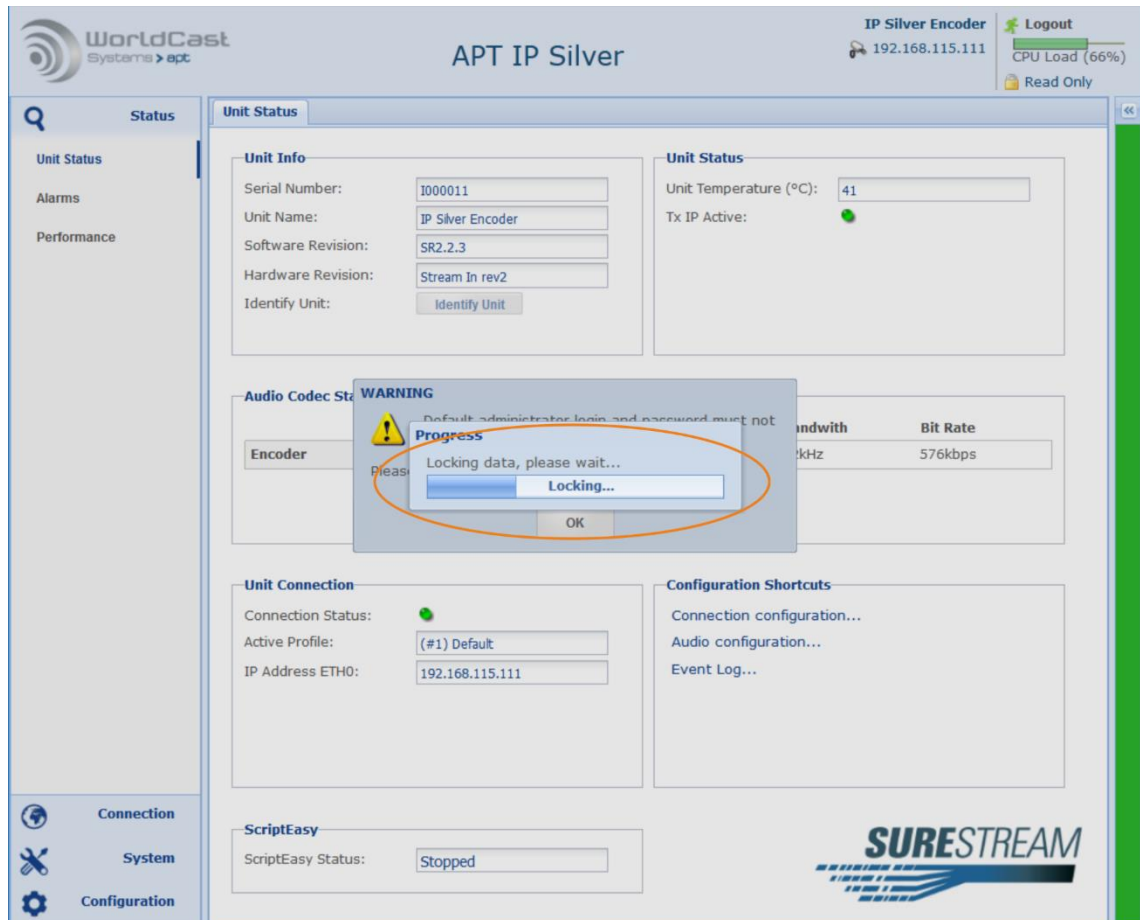


Figure 3-2: After loading the status page the GUI tries to lock the current session for read/write access

For a full read/write access, the GUI must lock the current session. Read/write is a privileged status and is applied to the first user who logs in using the administrator account.

Any other user who tries to log in to the administrator account after will be set to a read-only status. If the first user with administrator privileges logs out, the next user gets administrator rights. The current user status is shown in the top right corner of the window

### 3.2.3 Activated Applications and Options

Depending on applications enabled and licenses applied, the unit may give additional information while loading the control interface.

The image below shows that the IP Silver Decoder has a ScriptEasy Script loaded. If a script is loaded, it will be activated during start-up. The alert window indicates this status and asks the user to acknowledge.

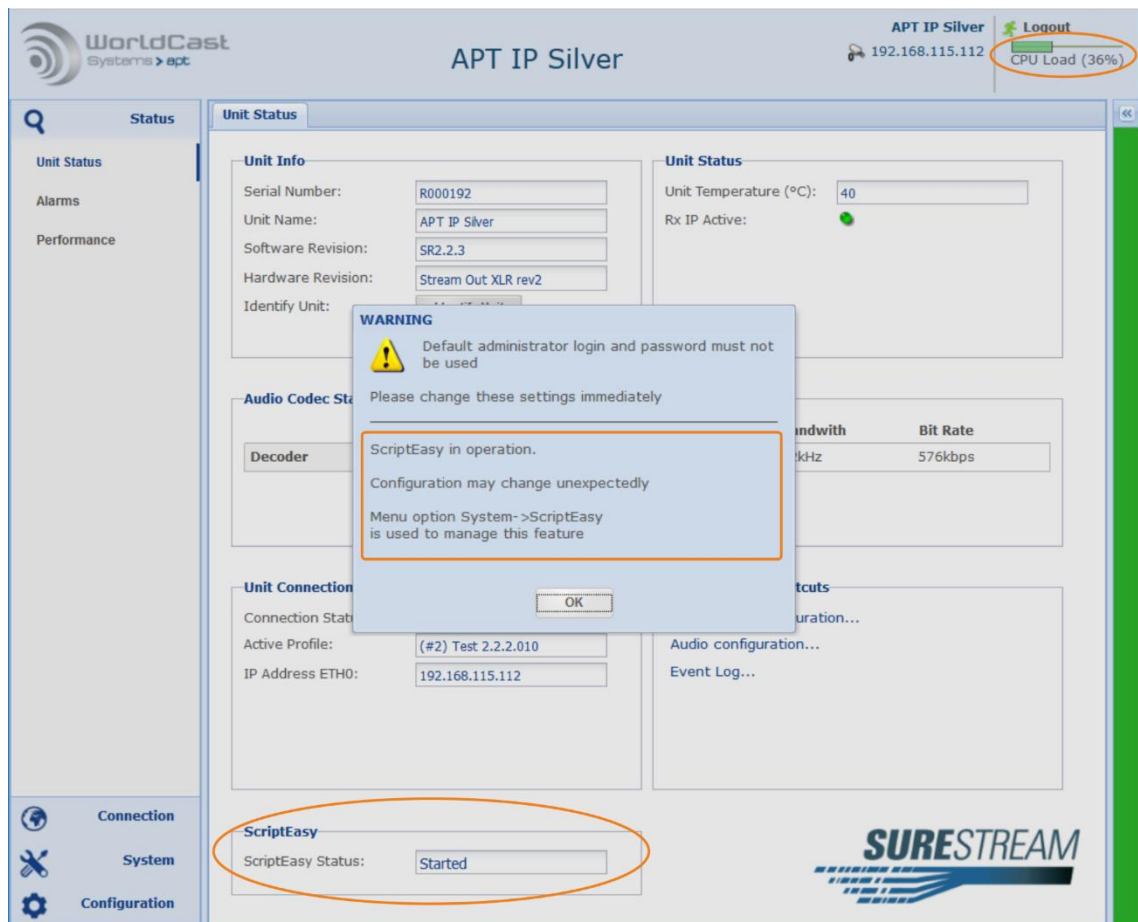


Figure 3-3: Shows the ScriptEasy alert window during start-up

- ① ScriptEasy "started" indicates that a script is applied and activated – "stopped" indicates that no script is loaded, or a script has been stopped. More information about the use of ScriptEasy is provided in section **Fehler! Verweisquelle konnte nicht gefunden werden..**

#### 3.2.3.1 CPU Utilization

A CPU meter is added in the top right corner of the Main Page. This meter provides information about the CPU utilization in real-time. Depending on the number of IP streams, the packet size and the selected audio algorithm, the CPU load can vary significantly.

- ⚠ It is important not to overload the CPU!

### 3.2.4 Status Page

Once the Web GUI has downloaded the application data from the IP Silver, it shows the “Status Page” of the WEB application. This “Status Page” consists of three sections: The main menu (1) on the left-hand side, the main pages (2) in the middle and the “Current Status” frame (3) on the right-hand side which can be hidden and its status is indicated by a colored bar: green, orange, or red depending on current alerts.

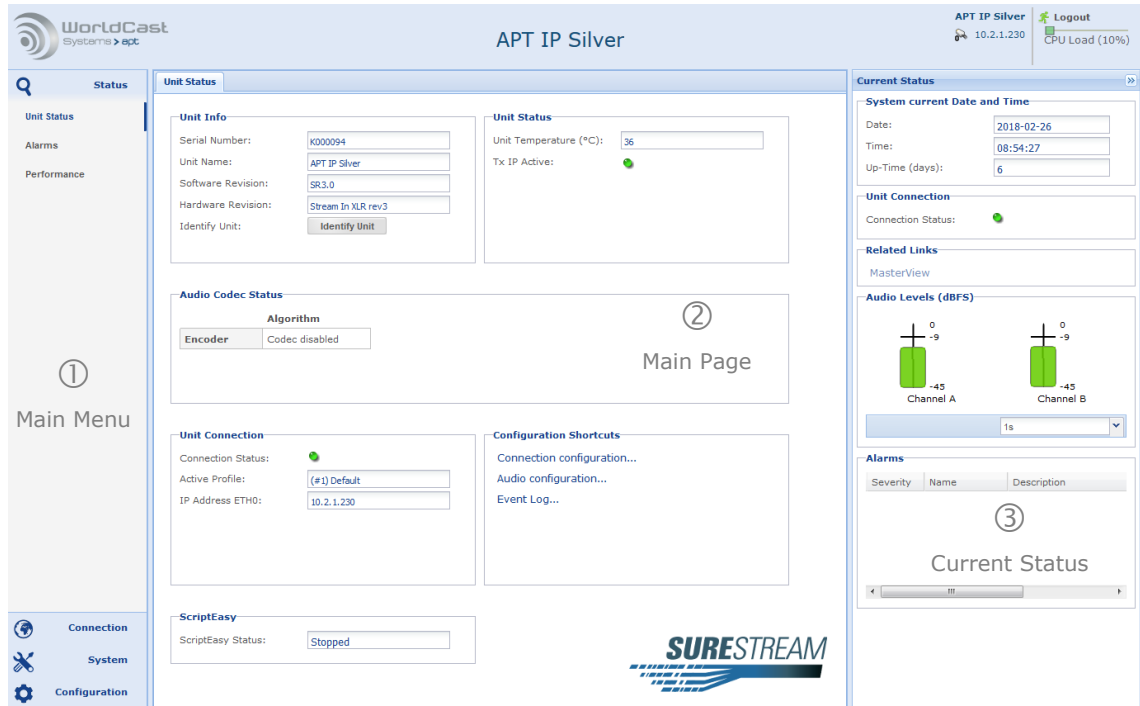


Figure 3-4: Shows the Unit Status page of a IP Silver Encoder with popped up "Current Status" frame

The default Main Page (2) is always the Unit Status page summarizing the status of the hardware unit, the current Audio Codec settings and the Connection Status. The color of the stylized LEDs indicates the current status condition (gray, green or red).

### 3.2.5 Session Close/Session Time Out

The Web GUI of the IP Silver allows multiple users to connect simultaneously. However, while all can see the data, only one user has the full Admin privileges to make changes in the configuration (read/write access). Usually, this will be the first Admin user to have connected for the session; subsequent logins will be given "Read Only" status.

For a different user to obtain full read-write control, the prior connectee must log out. The GUI will automatically close a session after 70 minutes of inactivity so that access to a unit cannot be blocked accidentally.

The session owner can manually close a session by using the “Logout” button, closing the browser or the browser tab or by forcing a reloading of the application data by pressing the F5 key.

**①** Only the session owner can close his own session whether logged in with admin rights or in guest mode.

### 3.2.6 Main Menu

The main menu (1) is always present on the left-hand side of the browser window. Depending on the selected menu item, it will expand and show related submenu items.

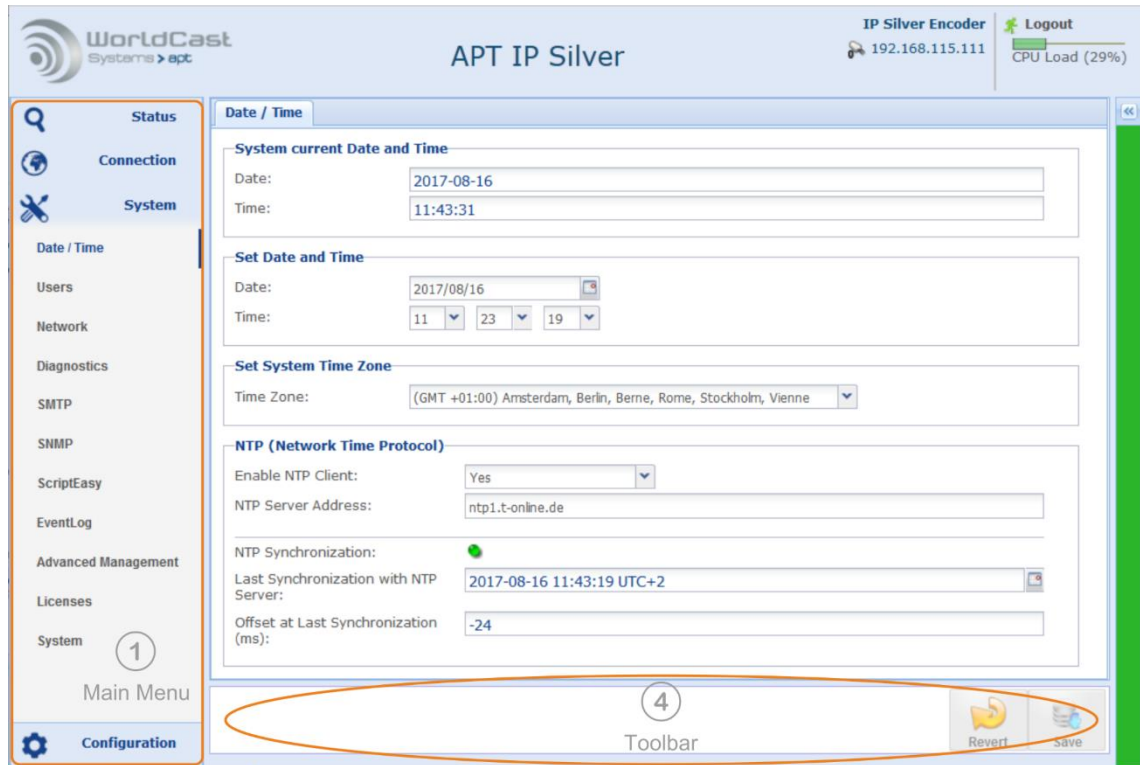


Figure 3-5: The Main Menu expands depending on the selected menu item. The "Current Status" frame is hidden and actually indicated by the green bar on the right-hand side ("good" condition).

The screen shot above shows the Main Menu (1) with related sub-menu entries of the System menu. This figure also displays the hidden "Current Status" frame on the right. This frame is indicated by the currently green color ("good" condition). Clicking on this colored bar pops up this frame.

A selected menu entry opens the corresponding page and the toolbar (4) on the bottom of the browser window that provides related items.

- ❗ The "Current Status" bar changes its color depending on the current conditions. Possible colors are GREEN (no error), YELLOW (minor error), RED (major error) and light BLUE (no active configuration).

Notes: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

### 3.3 Main Menu - Status

Starting the WEB application always opens the Main Menu “Unit Status” item with the Unit Status page and the corresponding sub menu items loaded. The Unit Status page is organized in various sections.

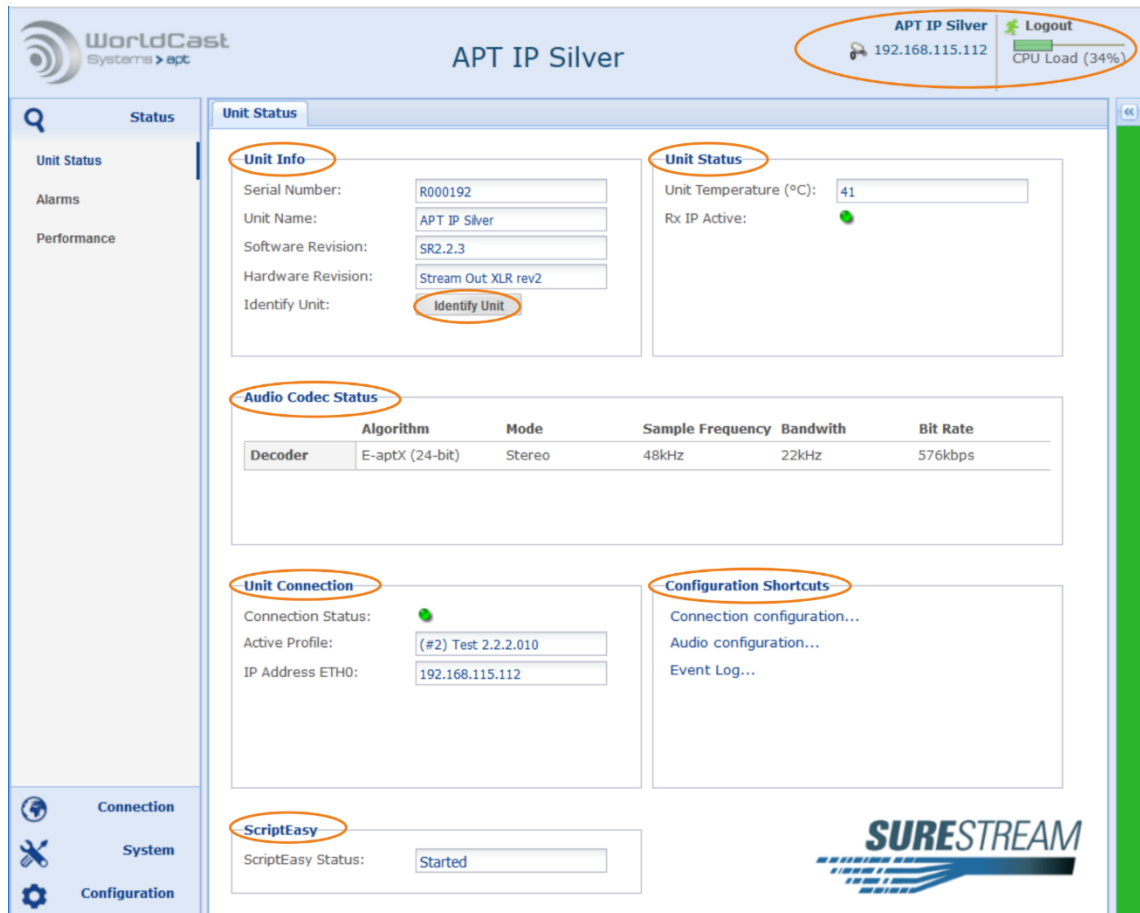


Figure 3-6: Main Menu Status - Unit Status page

#### 📶 Main Frame

In the upper right corner of the main browser frame, you can find the ETH IP address, the name assigned to the unit, the CPU meter, and the logout button. This is also where the "Read Only" indication will appear if another user has already logged in with read-write privileges.

#### 📶 Unit Info

This section displays the hardware and software release version:

- ➔ Serial Number of the unit
- ➔ Unit Name (individual Name as applied)
- ➔ Software Revision
- ➔ Hardware Revision
- ➔ “Identify Unit” button

## Unit Status (*continued*)

### **“Identify Unit” - button**

This button is the only control on this page; all other information is “read only”. Clicking on this button turns on the alarm LED of the particular (physical) unit. This is an easy way to identify a physical unit in case many units are in use.

### **Unit Status Section**

#### Unit Temperature

This shows the current Engine temperature of the unit and is not the environmental temperature. This value can exceed 40°C without causing a critical situation. There are no fans fitted as default for two reasons; the emitted noise, and fans are wear and tear items which need to be replaced periodically.

#### IP Transport Error

This status indication is related to IP audio streams (RTP/RTCP). If an RTP stream is enabled on the streams table, any IP Rx or Tx error will trigger a change in this status indicator, using RTCP (Real Time Control Protocol). These alarms have a latency of about 10-15 seconds due to the RTCP timeout.

### **Audio Codec Status**




This section provides information about the currently active Codec settings for the IP Silver Encoder or the Decoder.

### **Unit Connection**



This section shows the currently active connection, i.e. the status, the name of the loaded profile and the unit’s IP address. The stylized LED indicates a physical “Loss of Connection” on the IP interfaces if a stream is assigned to the interface (this is a copy of the “Current Status” frame item).

### **Configuration Shortcut**

This section provides direct links to:

-  Connection Configuration page (advanced configuration)
-  Audio Configuration Page
-  Event Logs

### **ScriptEasy activity status**

-  “Started” – Script loaded and active (running)
-  “Stopped” – Script loaded but temporarily stopped or no script loaded



### 3.3.1 Current Status Frame

This "Current Status" frame allows a quick inspection of the current condition of a running configuration. Clicking on the little arrows on top of the bar opens it as browser frame. In this mode, it is re-sizable and parameters can be changed (e.g. refreshment cycles). Clicking on the colored bar opens this window as popup window with a fixed size and in read-only mode.

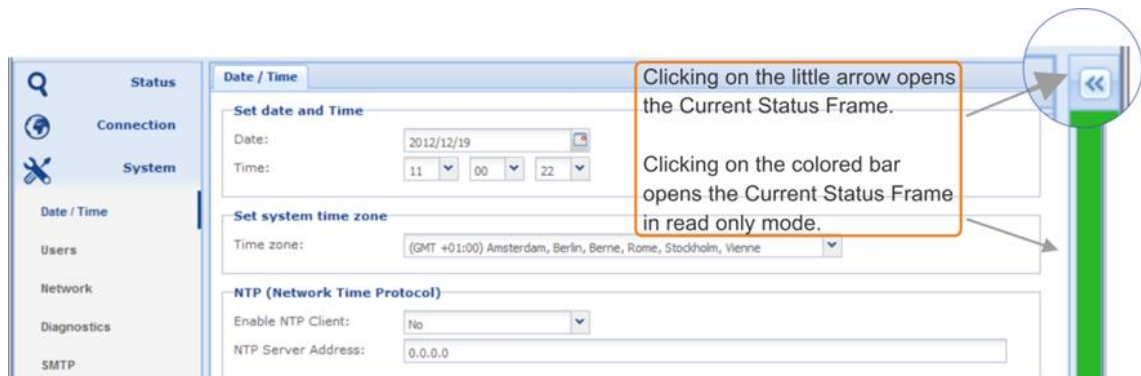


Figure 3-7: Two methods to open the "Current Status" frame; as a re-sizable (read-only) pop-up or with a fixed size and editable.

- ① The "Current Status" bar changes its color depending on the current conditions. Possible colors are: GREEN (no error), ORANGE (minor error), RED (major error) and BLUE (no active configuration)

#### Date and Time (5)

Indicates the current system date and time. The date and time settings can be found in the "System" menu. - The up-time counter is only reset by a system restart.

#### Unit Connection (6)

If an RTP stream is enabled on the streams table, it broadcasts IP Rx and Tx errors to this status indicator utilizing the RTCP protocol (Real Time Control Protocol).

#### Related Links (7)

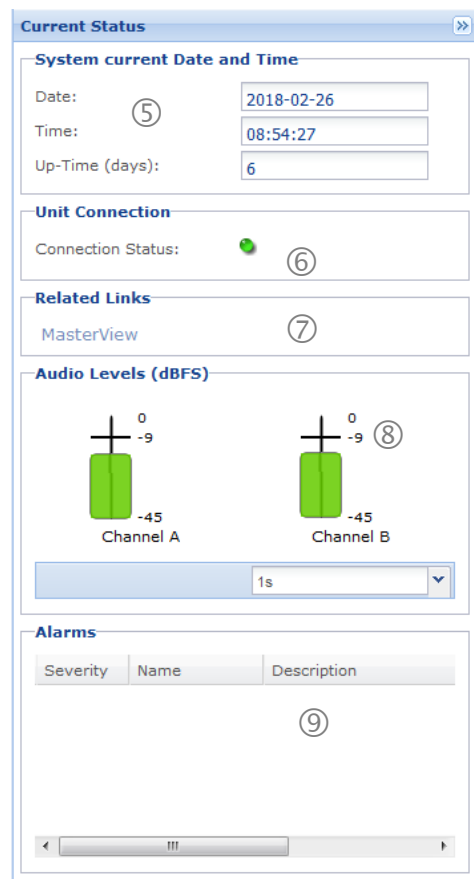
If a ScriptEasy script is loaded, this link to MasterView becomes active. It opens MasterView in a new browser tab

#### Audio Levels (8)

These level bars are always representing the digital signal domain reading as dBFS. The refresh period can be set from 500 milliseconds to 10 seconds.

#### Alarms (9)

This window shows current system or connection alarms in real time. It indicated the level of severity by LED colors (red and orange), the alarm name and the alarm description.



### 3.3.2 Alarms Status

The following screen shows the alarm status page. Note that a stylized red or yellow LED means the alarm is active. Green means everything is working normally, and gray means this alarm is not enabled or not applicable.

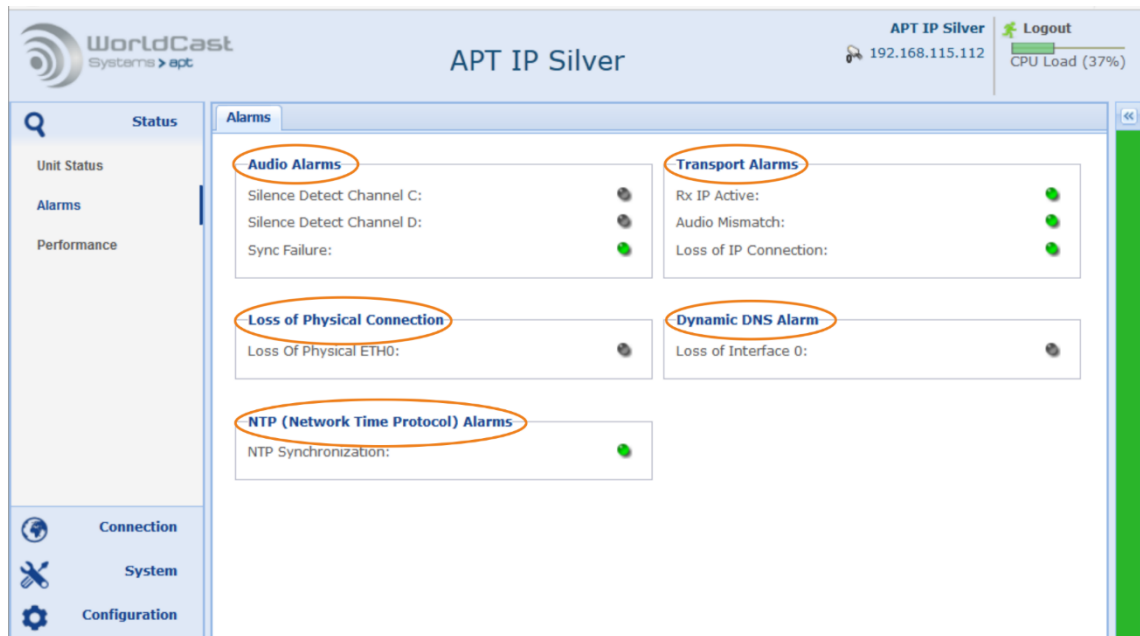


Figure 3-8: Main Menu Status – Alarms page from a IP Silver Decoder

#### 3.3.2.1 Audio Alarms Section

This section shows the status of the audio alarms. The alarms listed here are Silence Detection for channels C&D (A&B on the Encoder) and Sync alarm.

##### **🔊 Audio Alarms (Silence Detection)**

The Audio signal has decreased below the threshold level and the timeout specified in the audio configuration menu. This alarm will be flagged if silence is caused by a network fault, or the call was dropped, or just because the audio source has stopped.

##### **🔊 Sync Failure (AutoSync Alarm)**

This Alarm indicates a general sync failure in a situation where an excessive amount of packets were dropped or out-of-sequence resulting in a gap in the audio stream significant enough to generate the Sync alarm. The different audio algorithms or linear PCM have their particular sync-failure sensitivity.

For aptX® Enhanced, this alarm corresponds to the AutoSync Alarm. AutoSync is a bit pattern sent embedded in the aptX® audio stream that allows a very rapid resumption of decoding after a gap in the bit stream. This alarm will be flagged if the following conditions occur (for network faults, usually along with other network alarms):

- Mismatch of audio algorithms on Transmit and Receive units
- Connection or transport errors
- A call being dropped by the Transmit unit

## Alarms Page (*continued*)

### 3.3.2.2 Transport Alarms

This section shows IP alarms only such as IP Rx and Tx errors and audio mismatch and Loss of IP Connection.

#### **IP Transmit (Tx) Error (Encoder)**

The packets from the Tx unit have not been confirmed as hitting the Rx unit – either the Rx unit is stating in its RTCP stream that there have been no packets, the RTCP port has been blocked, or there is another form of network fault resulting in no line of sight to the Rx codec.

#### **IP Receive (Rx) Error (Decoder)**

Packets are not arriving at the Decoder, and it is expecting to see traffic. This can be caused by stream being dropped on the Encoder, a network fault or mismatch in audio algorithm settings.

#### **Audio Mismatch**

This is likely to be raised if the algorithm and packet size do not match on both sides of the link.

#### **Loss of IP Connection**

If the de-Jitter buffer runs empty, a "Loss of IP Connection" is detected and activates this alarm condition (Gray=no Rx stream active, Green=no alarm detected, Red=LOC detected).

### 3.3.2.3 Loss of Physical Connection

Physical loss of connection to the network on the Ethernet port (cable pulled).

### 3.3.2.4 Dynamic DNS Alarms

This alarm indicates the loss of connection to the Dynamic DNS service. The Dynamic DNS service configuration is located on the Network/DynDNS configuration page (system menu).

### 3.3.2.5 NTP Alarm

This alarm indicates the "Loss of NTP Server connection" condition.

### 3.3.3 Stream Performance Monitor

The Performance Monitor is for all active transmit or receive streams. Clicking on an individual stream in the Stream Performance Table will display the performance details below the table. The time interval for the data update is set to 1 second as default. However it is user selectable down to 500 ms and up to 10 seconds. The Buffer Level Display is the graphical equivalence of the current receive buffer condition (shown on receive routes only).

Clicking on the “Reset” button resets the IP statistics. A shortcut allows the direct navigation to the stream configuration page “Connection Configuration”.

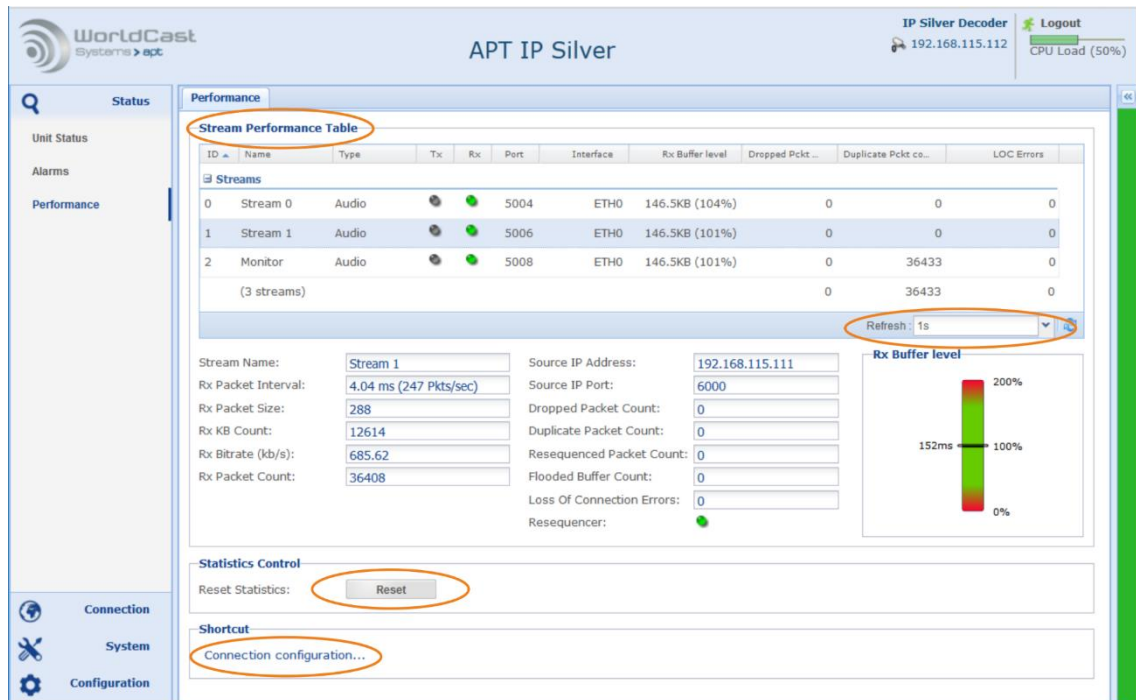
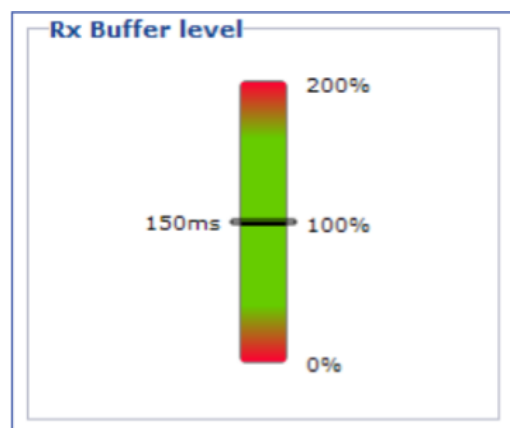


Figure 3-9: Status Menu - Performance Monitor page on the Decoder

#### 3.3.3.1 IP Statistics – Receive Buffer Level

This Buffer Level display is the graphical equivalence of the current receive buffer condition. This example shows a buffer which is set to 150 ms nominal. Depending on the delay jitter behavior of the network the actual level marker will swing around the nominal value. If the marker stays in the green area, the buffer management can cope with this amount of deflection.

A high value of deflection indicates that the nominal buffer level is set too low. Increasing the value keeps the marker closer to the mid-point.



### 3.3.3.2 IP Statistics - Details

This section shows the IP statistics of Figure 3-9 of a selected stream. The table below provides the description of each of the statistics (Tx for Encoder and RX for Decoder).

Statistic	Description
Stream Name	Shows the name of the analyzed stream
Rx or Tx Packet Interval	Shows the packet time (p-time in msec.) and the packet rate per second
Rx or Tx Packet Size	Size of received or transmitted packet in Bytes
Rx or Tx kB Count	Kilo Bytes received or transmitted
Rx or Tx Bit Rate	Bit rate of receive or transmit stream (data & IP overhead)
Rx or Tx Packet Count	Number of packets received or transmitted
Rx Source IP Address	IP Address of the transmitting Codec
Rx Source IP Port	IP Port on which the transmitting Codec is sending the stream
Rx Dropped Packets Count	Number of dropped packets
Duplicated Packets Count	The number of duplicated packets arrived on the Rx stream.
Re-Sequenced Packets Count	Number of packets that reached the de-jitter buffer out of sequence (also indicates the level of re-sequencer activities)
Flooded Buffer Count	The Buffer has detected above 200%. Buffer level has been normalized to mid-point by the engine
Loss of Connection	Loss of connection is detected if the buffer level has dropped to 0%.
Rx Resequencer	The green LED indicates the Resequencer status: On There are currently no options for the re-sequencer (always on)

**i** *Statistic records can be reset by clicking on the "Reset" button (refer to Figure 3-9)*

### 3.3.3.3 Packet Re-Sequencer

The Decoder utilizes a Packet Re-Sequencer to keep arriving packets in the right order even if they arrive in the wrong sequence because of the network delay jitter behavior. The Re-Sequencer performs at best with a minimum number of six (6) packets in the buffer. In consequence, the buffer size should be chosen in accordance with the packet size for six packets. The validation engine prompts you to modify this setting whenever a mismatch of packet size and buffer size is identified; the Resequencer is always enabled. Even with a validation warning, the Resequencer stays active.

### 3.3.3.4 About Stream Tables (general)

In general, a Stream Table is a list of IP-Stream configurations organized in a table. Depending on where a stream table is accessed it will appear in read-only mode, like on the performance monitor page, or the table can be directly accessed by changing values and entries on the connection pages.

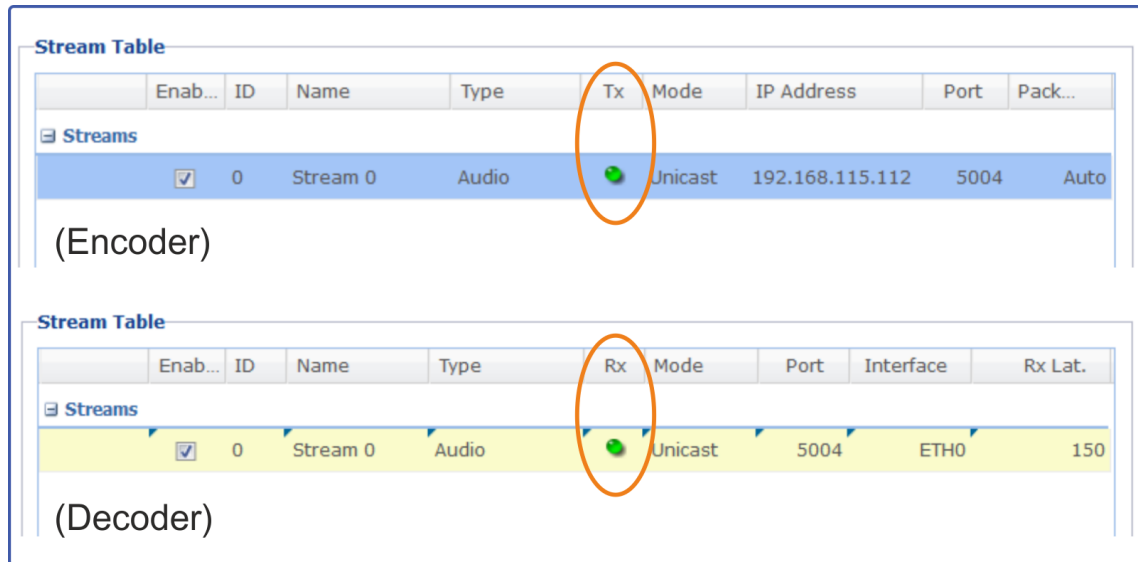


Figure 3-10: Shows Stream Tables from the Encoder and the Decoder

### Streams Table Exposure Options

The exposure of the Streams Table is flexible and can be widely controlled by the user. Clicking on the little arrow on each of the columns opens a context menu and allows sorting the table ascending or descending. Another submenu provides tick boxes for controlling the columns visibility. In general, the stream table exposure also depends on the size of the current browser window. The width of the columns can be adjusted by clicking between the columns and drag the border as appropriated.

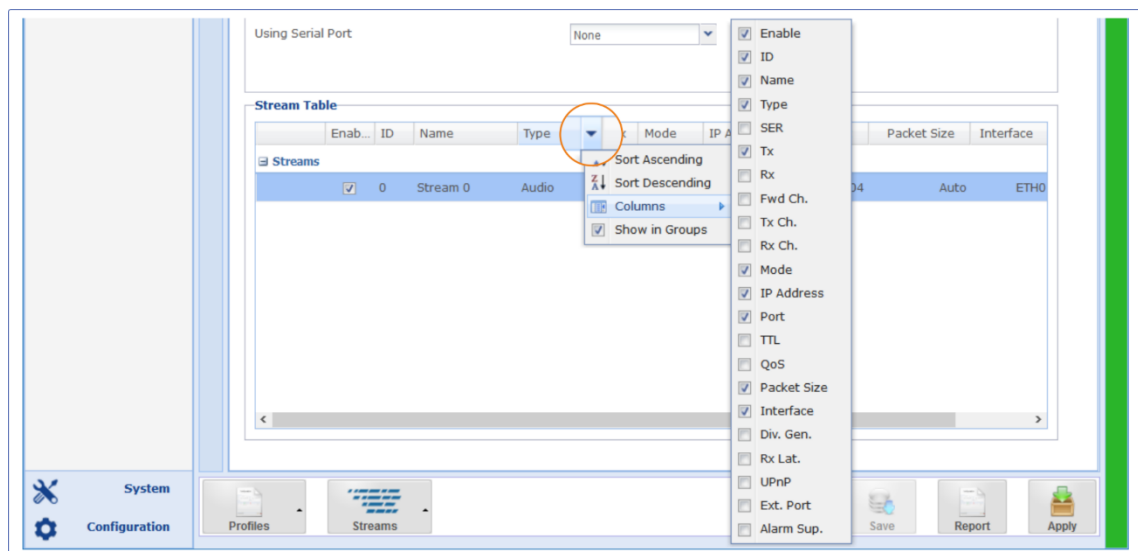


Figure 3-11: Exposure options on the Streams Table (connection page)

### 3.4 Main Menu – Connection

The connection page is the page where Connection Profiles can be created and IP streams can be enabled or disabled. This page also provides a Profile Wizard for a step-by-step procedure. A connection profile is a set of configuration parameters related to IP connections. A profile stores audio Codec settings and IP stream configurations

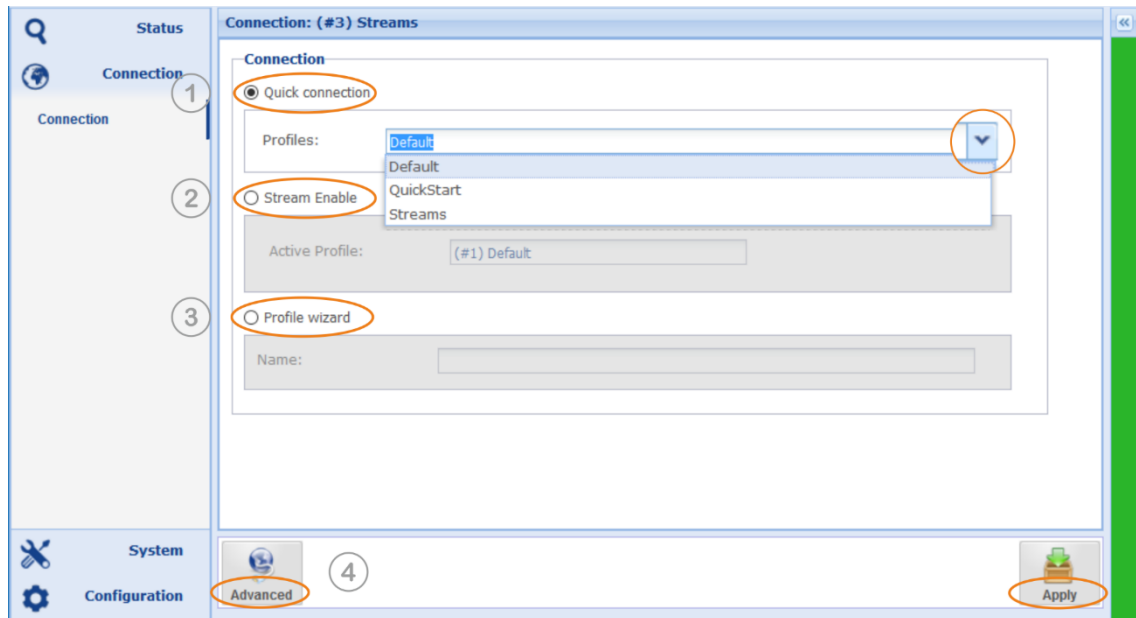


Figure 3-12: Shows the Connection Page of the IP Silver Encoder

The WEB GUI offers four options to create, manage and to apply a Configuration Profile:

- ➔ Quick Connection - loads an existing profile (1)
- ➔ Stream Enable – allows enabling and disabling of streams of the current profile (2)
- ➔ Profile Wizard – provides a step-by-step procedure (3)
- ➔ Advanced Configuration - manual stream configuration procedure (4)

#### 3.4.1 Quick Connection (1)

A “Quick Connection” is a pre-configured and previously stored profile. This profile was created and merged from an audio mode configuration and an IP stream setup. Before a Quick Connection can be used, a profile must have been created first.

Clicking on the little arrow opens a list with available profiles. Once the required profile was selected you must apply it to the Codec by clicking the “Apply” button on the bottom right corner.

## Connection Page (continued)

### 3.4.2 Stream Enable (2)

This section allows you to enable or disable each single stream of a loaded profile. The profile on the screen shot below has two streams. The stream labelled as Stream 1 is disabled. Clicking on the “Push to Enable” button will enable this stream immediately. It is not necessary to confirm this change. The “Apply” button disappears for this function.

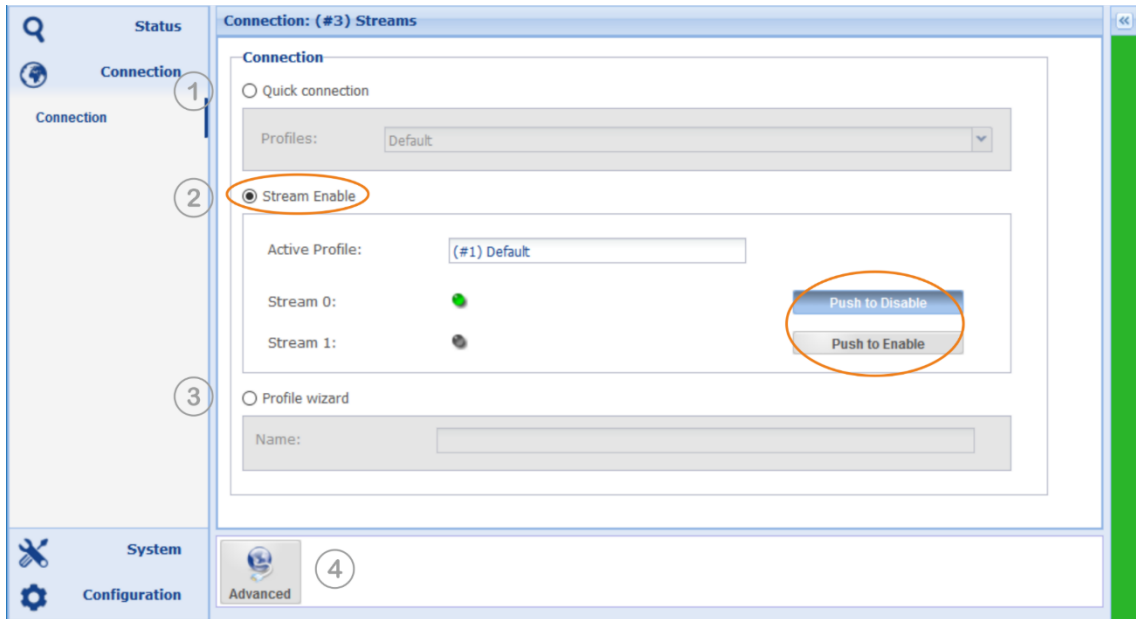


Figure 3-13: Shows the Connection Page – Stream Enable

### 3.4.3 Advanced Configuration (4)

The “Advanced” configuration procedure provides all configuration and management options on a single page. Other than the Configuration Wizard the “Advanced” configuration allows modifications on the currently applied profile and configuration. It also provides options and tools to edit already created profiles.

#### Notes:

---



---



---



---



---



---



---



### 3.4.4 Profile Wizard (3)

The “Profile Wizard” guides to a step-by-step procedure creating a profile. It prompts for audio settings and for IP settings. Finally, it creates a profile by merging both components. Once a profile was created it appears on the Quick Connection drop down list.

#### Profile Wizard – Profile Name

Selecting the radio box “Profile Wizard” on the connection page starts the Wizard. Firstly, a profile name must be entered in the Name field. Once a name is entered the “Next” button becomes active. Clicking on this button opens the next page prompting the audio Codec settings.

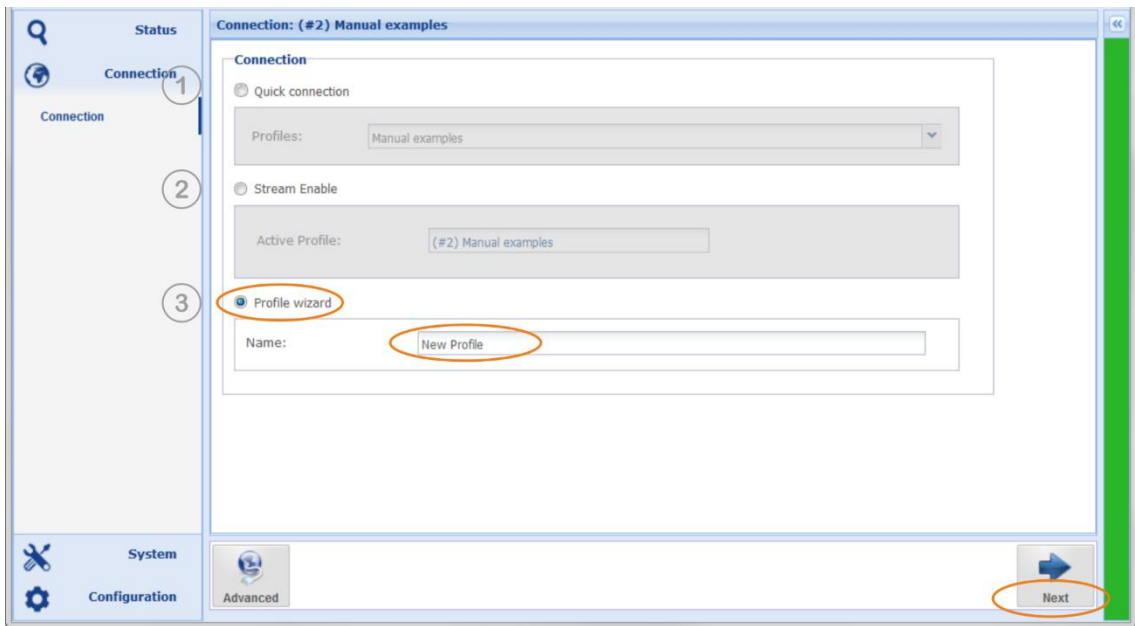


Figure 3-14: Shows the Connection Wizard's first page

#### Notes:

---

---

---

---

---

---

---

---

---

---

---

---

### 3.4.5 Profile Wizard - Encoder

The next page guides you to the Audio mode settings. The IP Silver units provide similar pages for the Encoder and the Decoder depending on the type of unit.

The following description is made using the example of an encoder. The decoder settings differ only slightly from this.

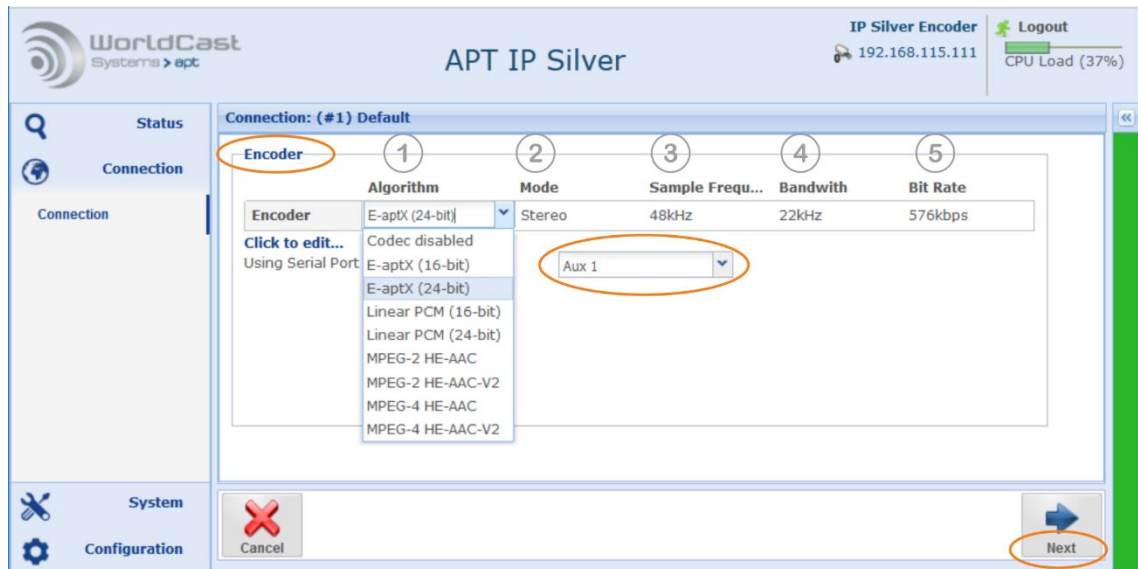


Figure 3-15: Shows the Encoder configuration page

#### 📡 (1) Algorithm

Clicking on the "Algorithm" field opens the drop-down list offering the available audio codec formats. Select the desired format. Depending on the format selected, the next fields display the available options.

#### 📡 (2, 3, 4, 5) Mode, Sample Frequency, Bandwidth and Bit Rate

These columns present the available options for the selected audio format.

#### 3.4.5.1 Embedded AUX Data (Using Serial Port)

For most audio algorithms (except Liner PCM) auxiliary data can be embedded into the audio stream. Once a suitable audio algorithm is selected and configured, the Serial Port drop down list becomes active. The embedded data channel accepts RS232 data up to 9.600Baud. Audio algorithms have baud rate constraints in dependence of the selected audio bit rate

### 3.4.6 Profile Wizard – Decoder

#### 3.4.6.1 Auto Detection of Incoming Streams

In addition to the manual selection of audio algorithms, the Decoder supports the “Auto” mode. This mode reads the algorithm parameters provided by the IP stream and automatically configures the decoding path of the receiver.

If an incoming stream can also contain AUX data which is to be decoded in auto-mode, the option "Aux Data" must be activated.

**ⓘ** Note, the "Auto Detection of incoming Streams" works for receive streams only. It is not available for bi-directional streams.

The decoder also supports the popular MP3 format (MPEG 1/2 L III).

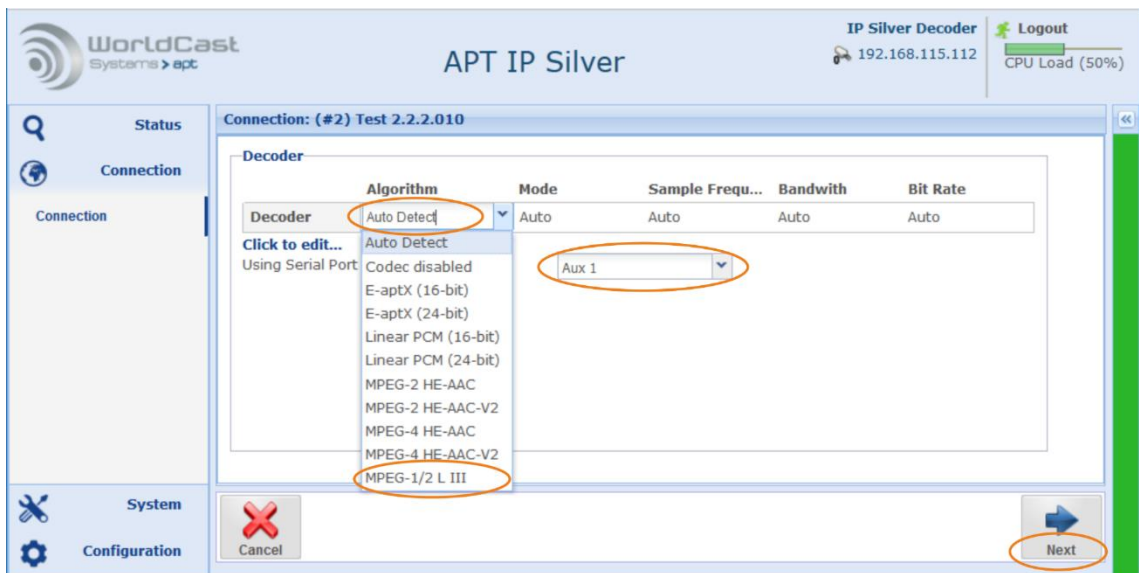


Figure 3-16: Shows the additional options of the Decoder

After completing the Encoder or Decoder settings, click on the “Next” button to enter the IP Stream configuration page.

Notes:

---



---



---



---

### 3.4.7 Profile Wizard – IP Streams Configuration

This window is the very heart of the Connection Wizard providing all options to setup the IP streams.

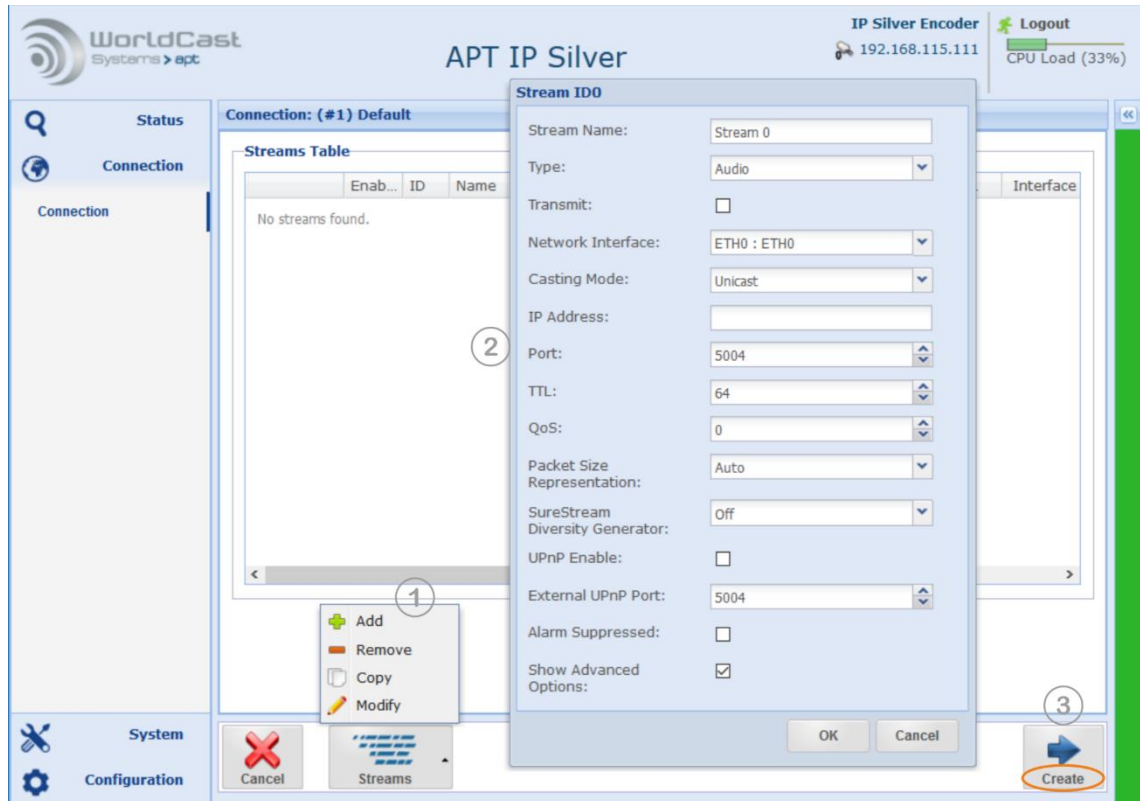


Figure 3-17: Shows the IP Stream configuration page on the Encoder with the stream setup window

#### Adding an IP Stream

Clicking on the “Streams” button (1) displays all options for creating and editing IP streams.

Clicking on “Add” opens the Stream Configuration window (2). This Window provides all setting options for the desired IP connection. Once the first stream is completed, a second or more streams can be added by clicking on the “Add” button again. Each stream gets a unique ID assigned by the system. This ID cannot be modified by users.

As long as the profile is not yet created a stream can be edited by double clicking on it or can be deleted by using the “Remove” function. The “Copy” function allows copying a selected stream.

**i** Clicking on the “Cancel” button, deletes all configurations including the audio settings and the profile name.

### 3.4.8 Profile Wizard – Saving a Profile

After all streams were created they are now appearing on the Streams Table. The little blue marker on the table fields indicate that the stream was not yet saved in a profile and can be modified.

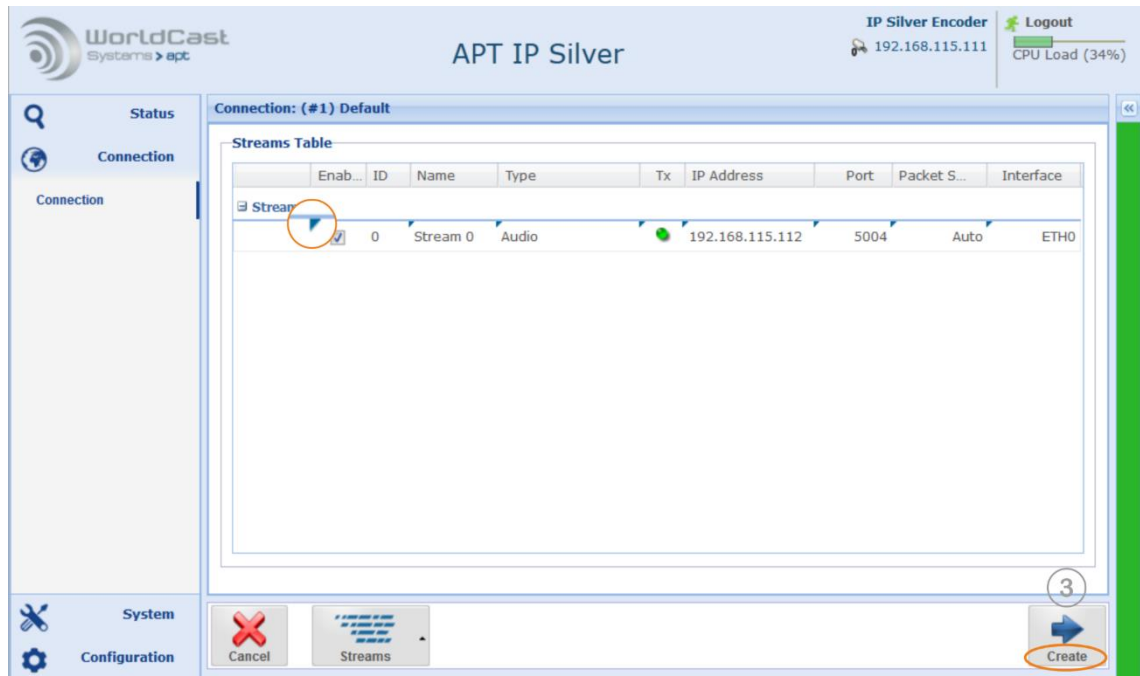


Figure 3-18: Shows a Tx stream ready for being merged into a profile

Clicking on the “Create” button (3) now merges the audio settings with the IP stream configuration into the “New Profile”.

This step completes the Connection Wizard and opens the “Advanced” configuration window.

#### Notes:

---



---



---



---



---



---



---

### Saving a Profile (continued)

The new profile "New Profile" appears in the list of profiles on the left side. To enable it, click the profile name so that the stream becomes visible in the table. By clicking on the "Apply" button (1), the profile is loaded and becomes the "Current" profile.

The Tool Bar provides several ways to edit profiles (2).

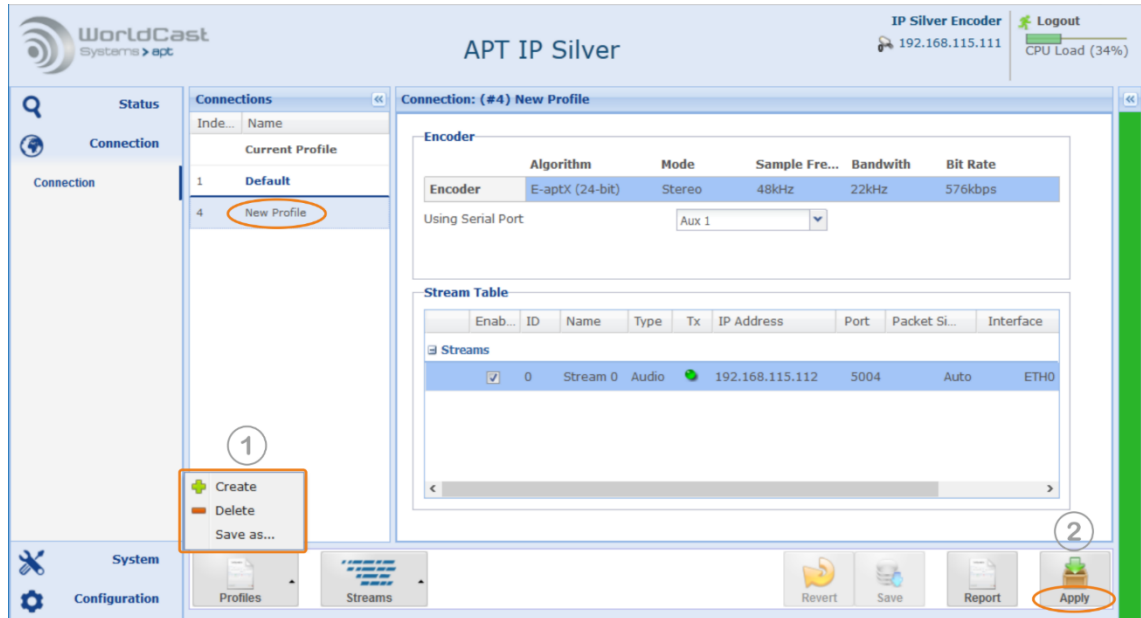


Figure 3-19: Shows the new created profile ready to be applied

**i** The "Advanced" configuration page (section 3.4.14) provides all options on a single page. A shortcut link on the status page opens the advanced configuration page directly.

### Notes:

---



---



---



---



---



---

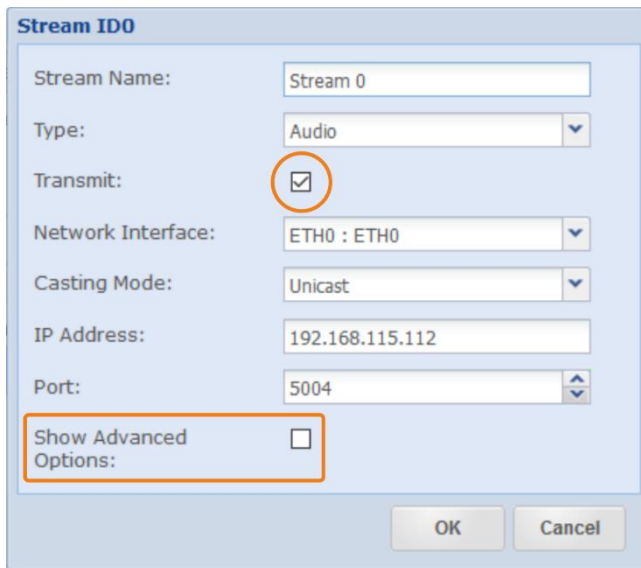


---

### 3.4.9 IP Stream Configuration – general

The stream configuration window provides options for different stream types and operational modes. Adding a new stream opens the configuration window with basic options. Enabling “Show Advanced Options” expands the configuration window presenting all stream options

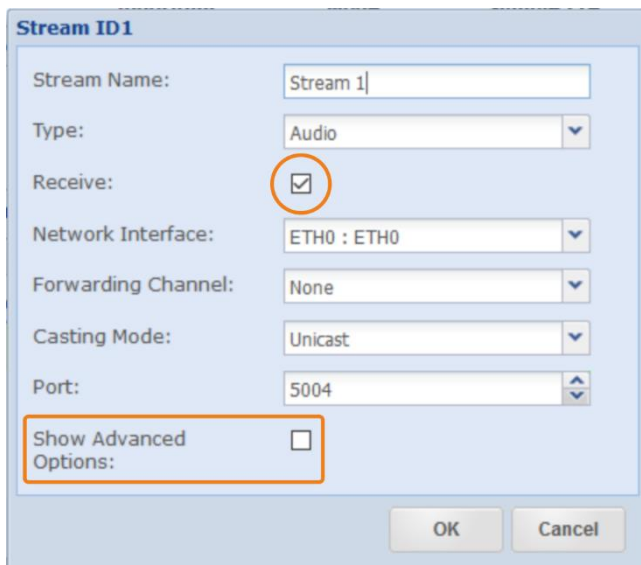
The basic parameters are sufficient to create a single media stream. In most cases, the default values of the advanced options are correct and applicable



The screenshot shows the 'Stream ID0' configuration window. It contains the following fields and controls:

- Stream Name: Stream 0
- Type: Audio
- Transmit:  (circled in orange)
- Network Interface: ETH0 : ETH0
- Casting Mode: Unicast
- IP Address: 192.168.115.112
- Port: 5004
- Show Advanced Options:  (boxed in orange)
- Buttons: OK, Cancel

Figure 3-20: Shows the basic configuration options for Audio Tx



The screenshot shows the 'Stream ID1' configuration window. It contains the following fields and controls:

- Stream Name: Stream 1
- Type: Audio
- Receive:  (circled in orange)
- Network Interface: ETH0 : ETH0
- Forwarding Channel: None
- Casting Mode: Unicast
- Port: 5004
- Show Advanced Options:  (boxed in orange)
- Buttons: OK, Cancel

Figure 3-21: Shows the basic configuration options for Audio Rx

Enabling the “Show Advanced Options” tick box expands the window offering all configuration options. The following sections discuss the complete configuration.

### 3.4.9.1 About Stream Types

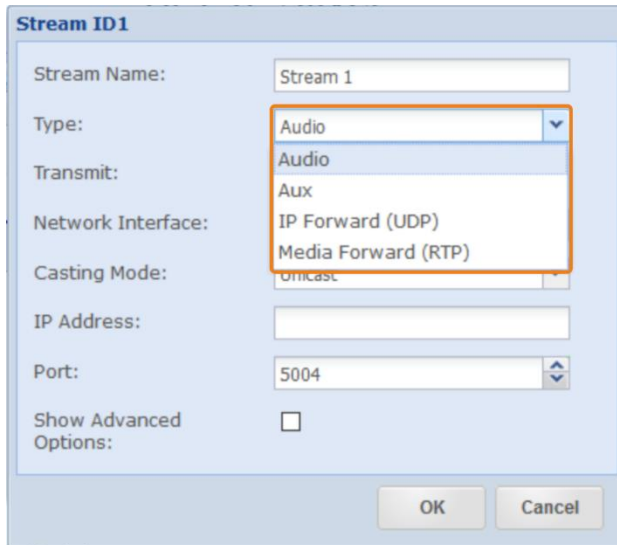


Figure 3-22: Shows the stream type selection menu

#### **Audio Stream**

An Audio stream is send via RTP/UPD. The possible streaming mode is:

- ➔ Simplex only, Transmit on Encoder and Receive on Decoder

#### **AUX Data Stream**

An AUX data stream is send via UDP datagrams only. This is different from the RTP/UDP mode and is not treated by the RTP engine at all. In consequence an AUX stream does not pass the de-jitter buffer on the receiving side. As a result, an AUX data stream is not synchronized with the audio content – it is always faster than the audio by the amount of the de-jitter buffer size.

- ➔ Transmit or Receive on both Streamer types

#### **Packet Forwarding**

The IP packet forwarding mode is data agnostic and can consist of UDP or RTP/UDP payload

The possible streaming modes are:

- ➔ Transmit or Receive on Encoder and Decoder
- ➔ IP Forwarding (UDP)
- ➔ Media Forwarding (RTP)



### 3.4.10 About Stream Forwarding

The APT Codec range supports IP Stream Forwarding as standard. This unique feature allows receiving and forwarding audio or non-audio data streams, like RDS, PAD or even EDI data (DAB/DAB+ bouquets), sent via UDP or RTP.

For an RTP/UDP audio stream, this feature supports the decoding and simultaneous forwarding of the same stream.

In the case of a non-audio data stream, like RDS over UDP from a server, the Encoder receives the UDP stream and allows forwarding the same. It is a user choice to forward the stream in the original format (UDP) or to re-encapsulate it into RTP/UDP.

The RTP protocol assigns sequence numbers to the packets; it supports time stamping and redundant streaming with SureStream. This data stream is then processed in the Decoder by the RTP de-encapsulation engine including resequencing and passing the de-jitter buffer. Thus, this forwarded non-audio data stream is protected and aligned by the SureStream technology in the same way as an audio stream over RTP/UDP.

The forwarding mode is to select separately for receiving and transmitting. The splitting in Receive and Transmit enables the use of both modes on the same stream, and thus the re-encapsulation of UDP to RTP/UDP (refer to Figure 3-29).

#### 3.4.10.1 IP Forwarding - UDP Forwarding

We use the term “**IP Forward**” for forwarding of UDP content regardless of the payload data type or protocol encapsulated in the UDP packet.

- ➔ IP Forward Receive (stream received at the IP Silver)
- ➔ IP Forward Transmit (stream sent from the IP Silver)

❗ *Both forwarding modes, IP Forwarding Receive and Transmit are possible with the IP Silver Encoder and the Decoder.*

#### 📶 IP Forwarding Receive

Preferably, this mode should be used for non-audio data streams between the data source (server, etc.) and the Encoder, but can be utilized for media streams as well. IP Forwarding “Receive” extracts the payload from the UDP packet and makes the data available in a forwarding channel. The UDP content can be of any type; audio or other non-audio data like RDS, PAD or EDI, and any protocol.

#### IP Forwarding - Receive

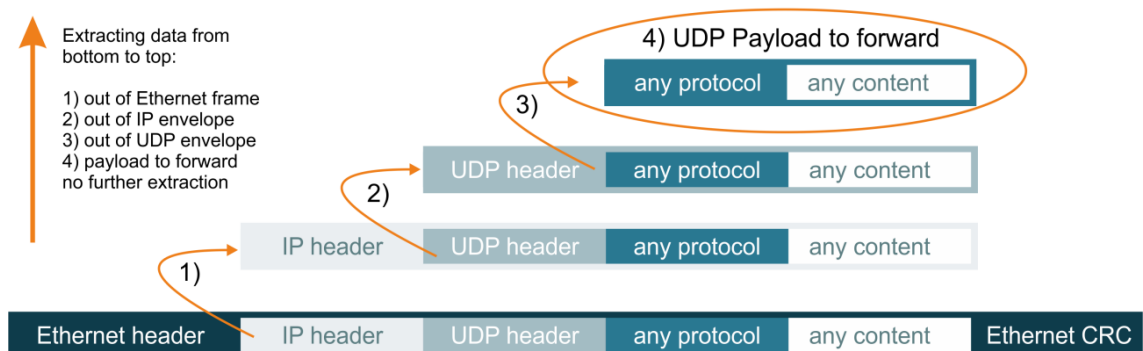


Figure 3-23: Shows how “IP Forward receive” extracts the payload of a receiving stream from the bottom to the top of the image - this mode is payload agnostic.

### IP Forwarding Transmit

This mode is the complementary of IP Forward Receive and describes the opposite flow direction. It must be used on the Decoder to forward receive data to the destination.

The encapsulation process flows from the top to the bottom.

#### IP Forwarding - Transmit

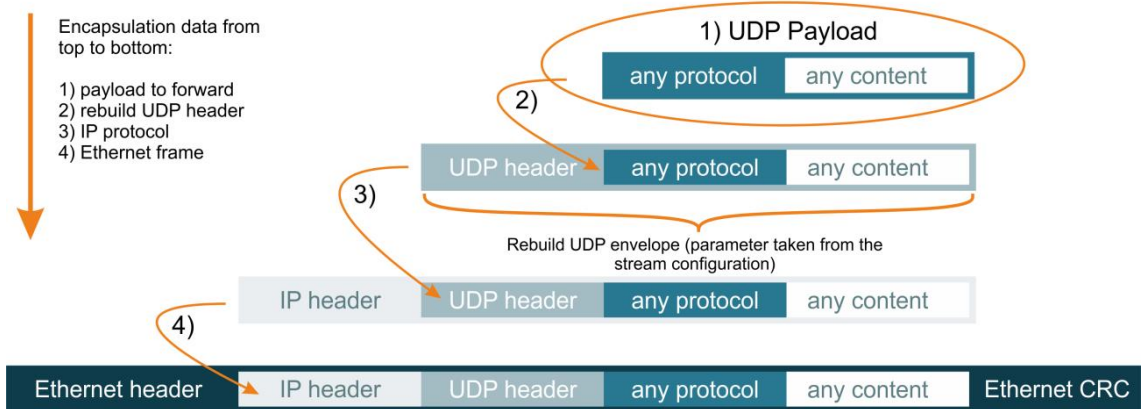


Figure 3-24: Shows how IP Forward "Transmit" encapsulates the payload on a transmit stream from the top to the bottom of the image.

**i** IP Forward is payload agnostic – any data can be forwarded (audio and non-audio)

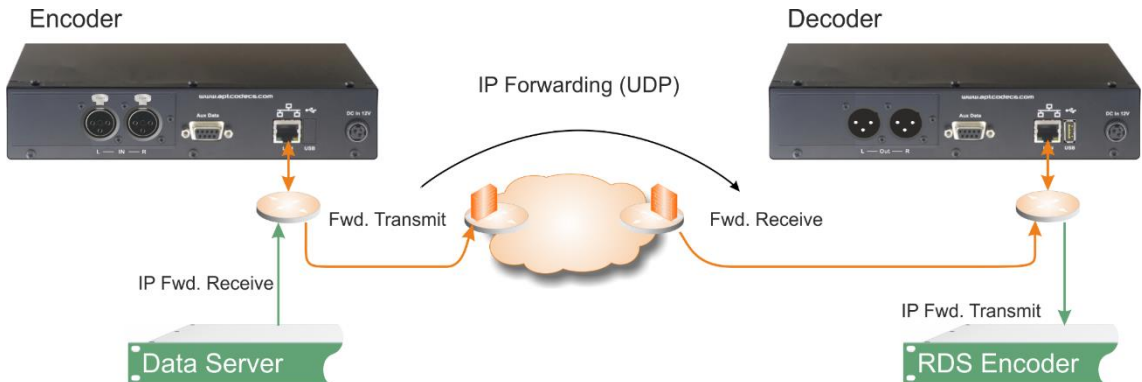


Figure 3-25: Shows an example of IP Forwarding for RDS data over UDP.

**⚠** The Forward "Receive" and the Forward "Transmit" method must be the same on both ends of the link.

### 3.4.10.2 Media Forwarding - RTP Forwarding

We use the term “**Media Forward**” for forwarding of content carried by the RTP protocol. The typical payload is audio or media content for real-time transmissions.

**i** *Both forwarding modes, IP Forwarding Receive and Transmit are possible with the IP Silver Encoder and the Decoder.*

- ➔ Media Forward Receive (stream received at the IP Silver)
- ➔ Media Forward Transmit (stream sent from the IP Silver)

#### **Media Forwarding Receive**

This mode receives the IP packet from a data source and extracts the media payload of the RTP protocol. The packets must contain the RTP protocol, or the stream will be rejected.

This forwarding mode is typically used for audio data. However, the payload can be any type, even non-media data as discussed in section 3.4.10.

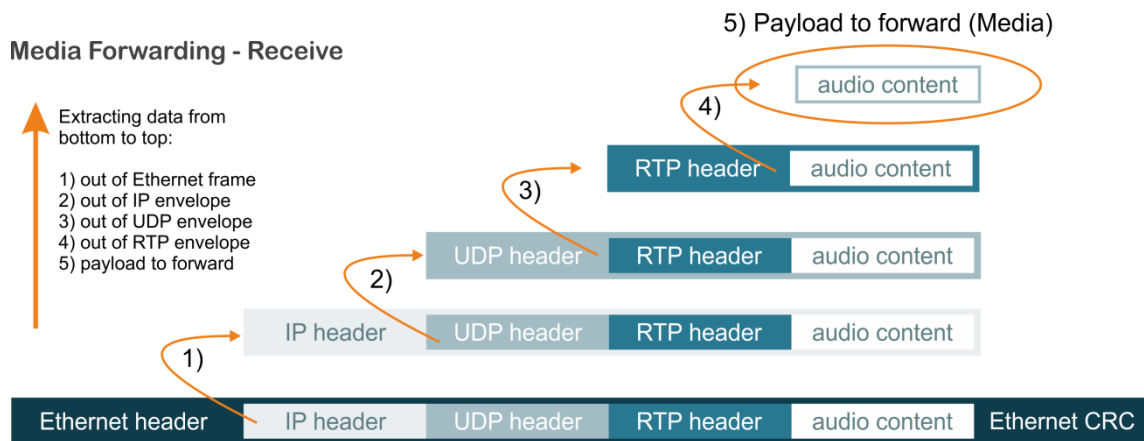


Figure 3-26 shows how Media Forward “Receive” extracts the payload on a receiving stream from the bottom to the top of the image - this mode is payload agnostic.

**i** *Media Forward Receive only expects the RTP protocol. Any UDP stream not containing the RTP protocol will be rejected.*

**⚠** The modes for “Forward Receive” and “Forward Transmit” must be the same on both ends of the link.

### Media Forwarding Transmit

This mode is the complementary of Media Forward "Receive" and describes the opposite flow direction. Media Forwarding Transmit encapsulates the media content in packets with new RTP header and new SSRC (Synchronization Source).

**i** Packet sequence numbers are copied from the originator.

This forwarding mode is typically used for audio/media data. However, the payload can be any type, even non-media data as discussed in section 3.4.10.

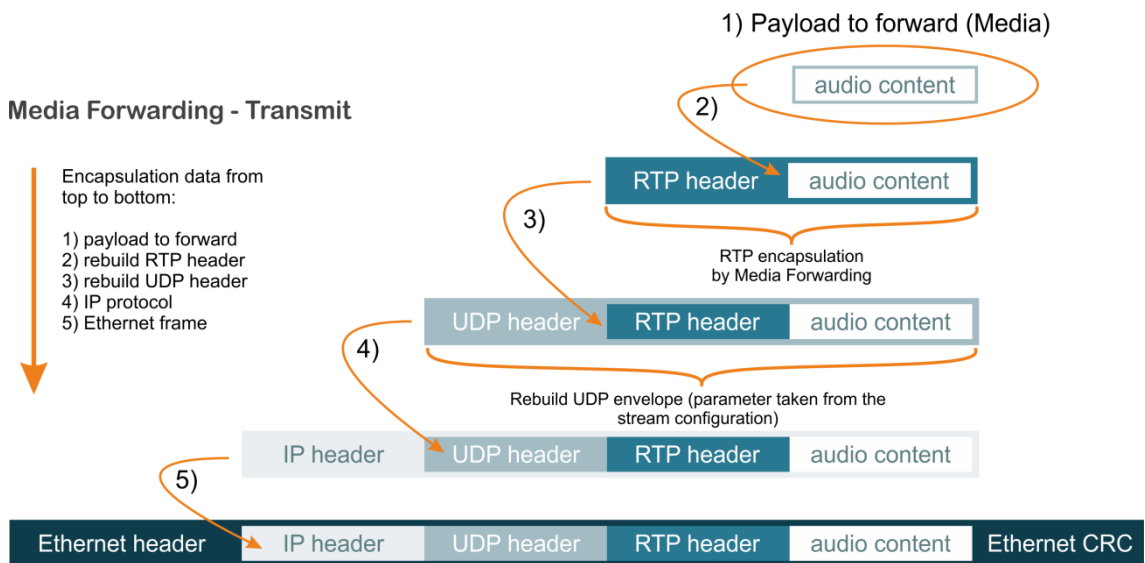


Figure 3-27: Shows how Media Forward "Transmit" encapsulates the media payload on a transmit stream from the top to the bottom of the image - this mode is payload agnostic.

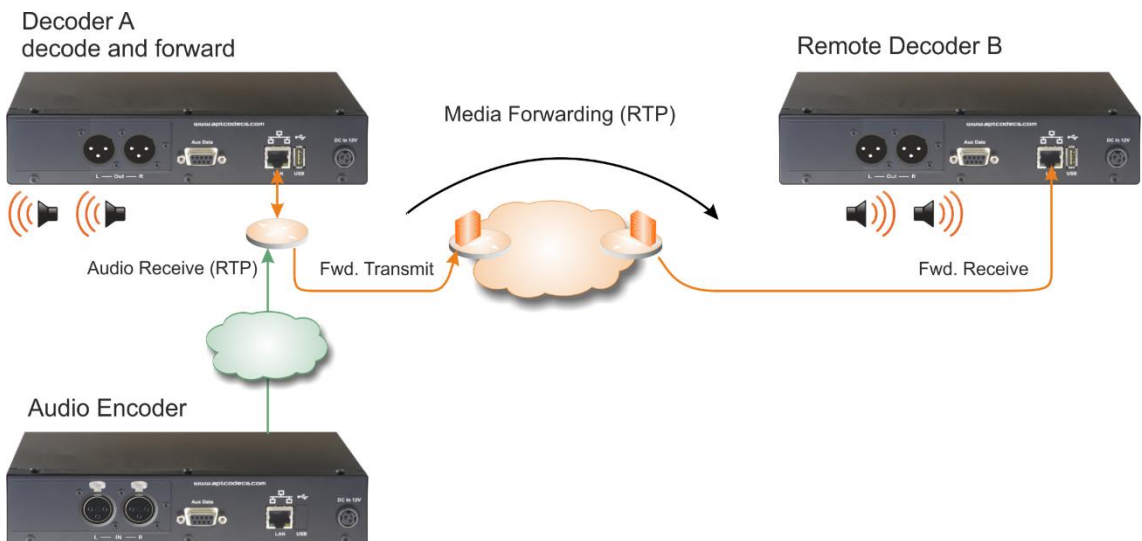


Figure 3-28: A typical Media Forward Transmit application with one Encoder and two Decoder



### 3.4.11 Audio Stream Configuration

#### 3.4.11.1 Transmit (Tx) Encoder

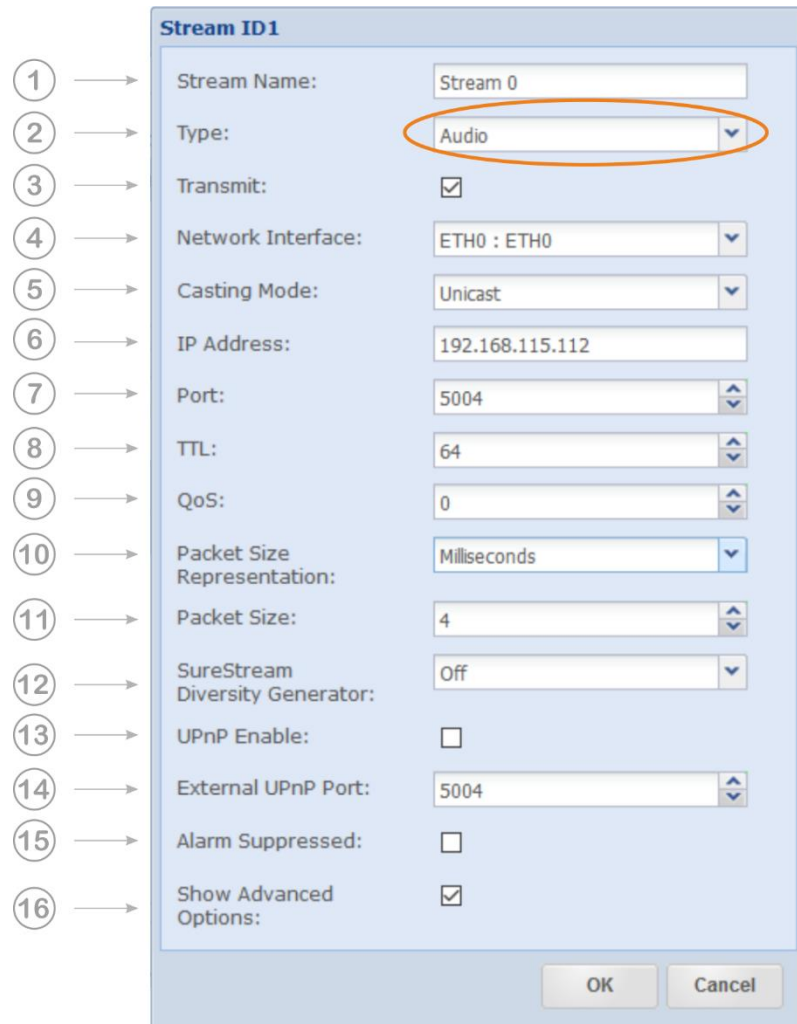


Figure 3-30: The IP Stream configuration window showing the available transmit options (Audio)

**ⓘ** Depending on the selected stream type: Audio, AUX or Forwarding and the streaming mode: Transmit or Receive, the available options will change.

**Notes:**

---



---



---



---



---



---

## Audio Streams Configuration (*continued*)

1. **Stream Name:**  
Enter the name for this stream
2. **Type:**  
Selected Stream Type is: **Audio**
3. **Transmit:**  
Enable "Transmit" on the Encoder (no other option).
4. **Network Interface:**  
Select the physical network interface (ETH0 : ETH0) or any pre-configured virtual interface for this stream. The physical and all virtual interfaces can be used.
5. **Casting Mode:**  
Unicast is a point-to-point connection. A stream can be sent to one decoder only. However, you can create several unicast streams to different destinations (multiple unicast). Multicast allows point-to-multi point streaming and uses the IGMP protocol for managing multicast joins and leaves (IGMP v2/v3)
6. **IP-Address:**  
Enter the destination IP address or the hostname of the remote unit.  
For unicast, this is either the unique IP address of the remote receiver or the network gateway or a hostname. Using a Hostname requires an active Dynamic DNS service (refer to section 3.5.3). For multicast: Enter the multicast group address.
7. **Port:**  
This is the IP port number of the remote Codec (destination IP port). The number selected here means that the stream must be received on this port number at the remote site. Each stream must use a separate port. Port numbers for audio streams are defined as even numbers in the 5000 range (5004/5006/5008 and so on); the odd numbers are reserved for the RTCP protocol and should not be used.
8. **TTL:**  
Time to live describes the number of network hops the packet can pass. Each passed hop reduces the TTL number by 1. If the TTL value becomes 0 and has not reached the destination, it will be deleted. This avoids flooding the network with "blind" packets.
9. **QoS (Quality of Service):**  
If the network supports QoS mechanisms the here entered value (DiffServ) can be evaluated by the QoS-enabled routers. QoS defines a mechanism for prioritizing UDP packets against other IP traffic in the network. - QoS is a network feature; the Codec allows the QoS tagging of the packets only. The range of the DSCP value is 0 (off) to 63 (highest priority). It is important to know about the QoS implementation of the network, before entering a value – not all values will be accepted by the network router.
10. **Packet Size Representation:**  
A packet size can be described in Bytes/Packet or in (audio) Time/Packet (packet time, p-time). The option "Full Frame" is required for all framed algorithms. Framed algorithms are all MPEG formats; MPEG defines the packet size in accordance with the algorithm settings. The "Auto" mode configures 4ms packet size for unframed algorithms and selects "Full Frame" in case an MPEG algorithm is selected.

 *If "Auto" is selected the Packet Size field is not visible.*

## Audio Stream Configuration (*continued*)

### 11. **Packet Size:**

Packet size describes the size of the payload in the UDP packet. It can be selected in bytes per packet or time per packet for all non-MPEG algorithms. For MPEG algorithms, use "Full Frame". If p-time is the representation mode, the value in milliseconds describes the amount of audio in a packet. The recommendation is 4ms or higher – also less than 4ms is possible. Refer to the description below.

### 12. **SureStream Diversity Generator:**

This allows setting the diversity generator level for SureStream component streams in Encoder Mode (Tx). Streaming through a single ETH interface (physical or virtual), it is recommended to enable the Diversity Generator on all component streams except the first one. This setting ensures that the stream diversity between the component streams is maintained on the single ETH port (refer to section: 4.2.1).

### 13. **UPnP Enable:**

This check box enables the UPnP IGD "Internet Gateway Device" feature for this individual stream (refer to section 3.5.3.3).

### 14. **External UPnP Port:**

If UPnP is enabled, on default the internal port equals the external port. This is a 1:1 port mapping performed in the router. In some cases, it might be necessary reconfiguring this. This setting allows an individual port mapping. It is recommended not to change the 1:1 assignment without a good reason.

### 15. **Alarms Suppressed:**

Enabling this check box suppresses all alarms generated by this stream. Sometimes it is useful suppressing alarms on a stream which are not applicable in the given situation. This can be set for each stream individually.

### 16. **Show Advanced Options:**

Allows changing from "Basic Options" to "Advanced Options". This tick box expands the configuration window.



### 3.4.11.2 About Packet Sizes

A small packet size allows a lower latency transmission but adds significant packet overhead into the network.

A large packet size needs more time to get “loaded” with payload and adds latency to the link. The packet overhead is significantly lower. It depends on the network which packet size can be used. A lower performing network may require a larger packet size while a high-performance network can cope with smaller sizes. The Codec engine can create several unicast streams. Streams with a small packet size require more engine power as larger packet sizes. The CPU utilization bar on the top frame of the GUI gives an indication of the CPU performance.

### 3.4.11.3 Packet Sizes of Framed Algorithms

Framed algorithms like the MPEG formats require packet sizes containing a full algorithm frame. For each algorithm, the frame size is different and presented in milliseconds of audio.

The packet size is set automatically for these algorithms and cannot be changed manually.

#### Coding Algorithms – Packet Sizes

MPEG2 HE AAC	min.42,6	variable
MPEG4 HE AAC	min.42,6	variable

#### Notes:

---

---

---

---

---

---

### 3.4.11.4 Receive (Rx) Decoder

The image below shows the additional receiver options on the Decoder.

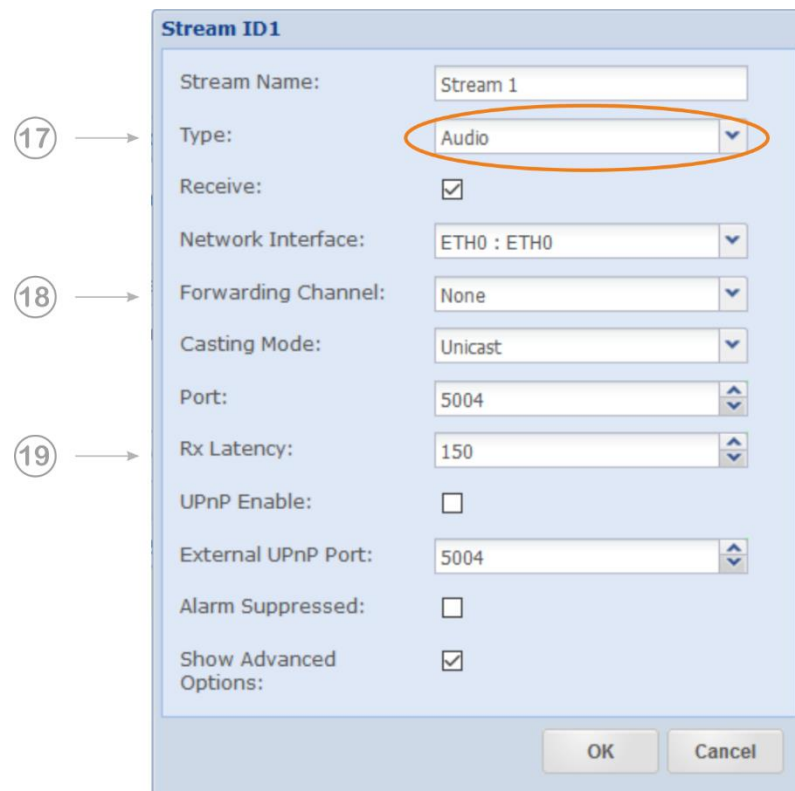


Figure 3-31: The IP Stream configuration window showing the available receive options (Audio)

**17. Type:**

Selected Stream Type is: **Audio**

**18. Forwarding Channel:**

For an incoming audio stream (Rx), if a channel number is selected, the stream is also made available in this channel for forwarding to another destination. For IP or Media Forwarding, the selected channel number becomes the payload source for the Tx stream. (stream type: IP Forward on pos. 17).

**19. RX Latency:**

This is the setting of the de-jitter buffer in Decoder Mode (Rx only). It describes the buffer size in time. The required buffer size depends on the network performance and the packet size. The goal is to have an appropriate timing window able to cope with the delay jitter in the network and to maintain the minimum number of packets required for reliable operation. The recommended number of packets in the buffer is six packets allowing the re-sequencer to work properly. If the amount of network jitter is low, a smaller number of packets is also possible. If the packet size is represented as p-time, the calculation is obvious.

### 3.4.12 AUX Data Stream Configuration (RX and Tx)

Creating an AUX follows the same principal as described for the audio stream. An Aux data stream is an UDP stream for transmit or receive the RS232 data.

- ① *The AUX data stream directions are Transmit or Receive on both Streamer units! So, AUX data can be configured as a bidirectional link between Encoder and Decoder.*

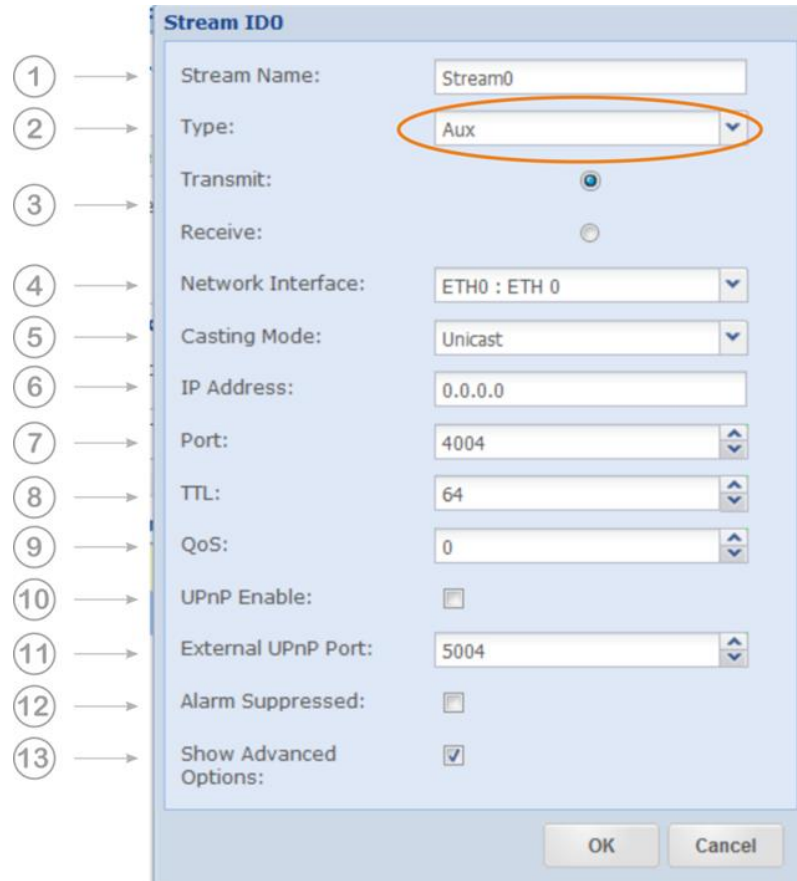


Figure 3-32: Shows the configuration options for AUX data streams

#### Notes

---



---



---



---



---



---



---

## AUX data Stream Configuration (Tx) (*continued*)

1. **Stream Name:**  
Enter the name of this stream
2. **Type:**  
Select Stream Type is **AUX**
3. **Mode:**  
**Transmit or Receive** (no Encoder and Decoder)
4. **Network Interface:**  
Select the network interface (ETH0) or any pre-configured virtual interface for this stream. Both physical and all virtual interfaces can be used.
5. **Casting Mode:**  
Unicast is a point-to-point connection. A stream can be sent to one decoder only. However, you can create several unicast streams to different destinations (multiple unicast). Multicast allows point-to-multi point streaming and uses the IGMP protocol for managing multicast joins and leaves (IGMP v2/v3).
6. **IP Address:**  
Enter the destination IP address or the hostname of the remote unit.  
For unicast, this is either the unique IP address of the remote receiver or the network gateway or a hostname. Using a Hostname requires an active Dynamic DNS service (refer to section 3.5.3). For multicast: Enter the multicast group address.
7. **Port:**  
This is the IP port number of the remote Codec (destination IP port). The number selected here means that the stream must be received on this port number at the remote site. Each stream must use a separate port number. Port numbers for AUX data streams are defined as even numbers in the 4000 range (4004/4006/4008 and so on).
8. **TTL:**  
Time to live describes the number of network hops the packet can pass. Each passed hop reduces the TTL number by 1. If the TTL value becomes 0 and the packet has not reached the destination, it will be deleted. This avoids flooding the network with "blind" packets.
9. **QoS (Quality of Service):**  
If the network supports QoS mechanisms the here entered values (DiffServ) can be evaluated by the QoS-enabled routers. QoS defines a mechanism for prioritizing UDP packets against other IP traffic in the network. - QoS is a network feature; the Codec allows the QoS tagging of the packets only. The range of the DSCP value is 0 (off) to 63 (highest priority). It is important to know about the QoS implementation of the network, before entering a value – not all values will be accepted by the network router.

## AUX Data Stream Configuration (*continued*)

### 10. **UPnP Enable:**

This check box enables the UPnP IGD “Internet Gateway Device” feature for this individual stream.

### 11. **External UPnP Port:**

If UPnP is enabled, on default the internal port equals the external port. This is a 1:1 port mapping performed in the NAT router. In some cases, it might be necessary to change the default configuration. This setting allows a different port mapping. It is recommended not to change the 1:1 assignment without a good reason.

### 12. **Alarms Suppressed:**

Enabling this check box suppresses all alarms generated by this stream. Sometimes it is good suppressing alarms on a stream which are not applicable to the given situation. This can be enabled for each stream individually.

### 13. **Show Advanced Options:**

Allows changing from “Basic Options” to “Advanced Options”. This tick box expands the configuration window.

### 3.4.12.1 About Packet Size of AUX Data streams

The packet size for AUX data streams is set automatically by the unit – this is not a configurable value. It is read from each serial port to a maximum block size of 1400 bytes (UDP MTU) and is sent in UDP packets with a maximum interval of approximately 16 milliseconds.

For example, a constant 9600 baud serial stream will send approximately 16 bytes per packet on an aux data stream over UDP.

For higher bitrates, this average number of bytes per packet increases.

### Notes:

---

---

---

---

---

---

---

---

---

---

### 3.4.13 Stream Forwarding

The principles of Stream Forwarding are described and discussed in section 3.4.10.

#### 3.4.13.1 Audio Stream Receive, decode and prepare Forwarding

With this configuration, an audio stream is received at the Decoder and decoded locally and simultaneously made available in the Forwarding Channel Number #1. for Media Forwarding (RTP). Audio streams consist of RTP/UDP packets; therefore, "Media Forward (RTP) must be chosen to forward the payload correctly in RTP packets.

- ❗ Only the IP Silver Decoder allows forwarding (transmit) of an incoming Audio stream; the Encoder only allows forwarding (transmit) of UDP and UDP/RTP streams!

#### Decoder Audio Receive

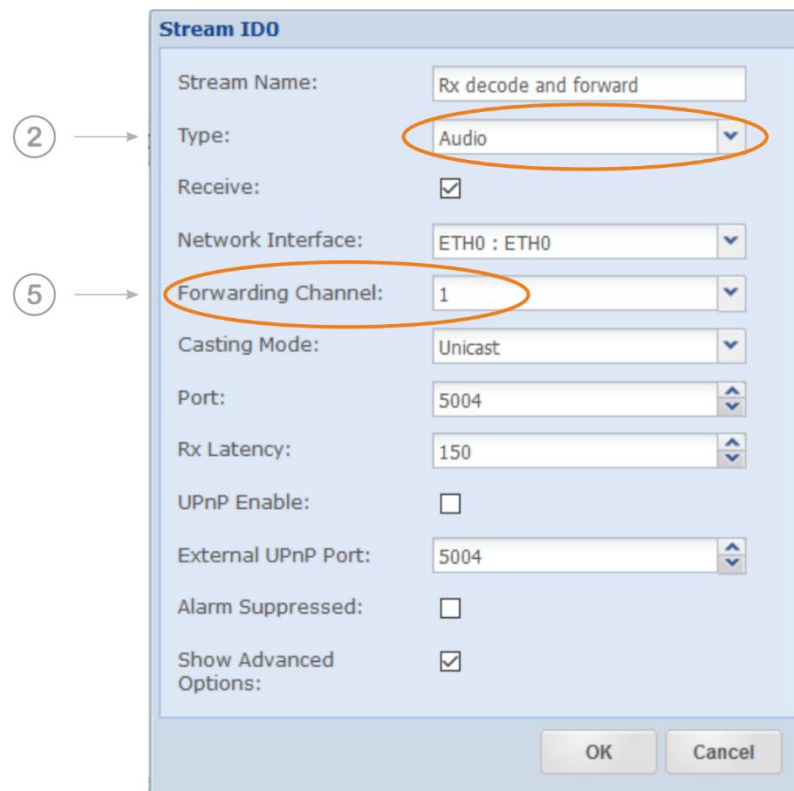


Figure 3-33: Shows the configuration options for Decode and Forward

This configuration is the same as for receiving and decoding an audio stream except for the selected Forwarding channel number.

- ➔ (2) Select the Stream Type: "Audio" for receiving the desired audio stream. All other values must be set for receiving an audio stream (refer to section 3.4.11.1 & 3.4.11.4).
- ➔ (5) There are six Forwarding channels available; select one channel for this stream.

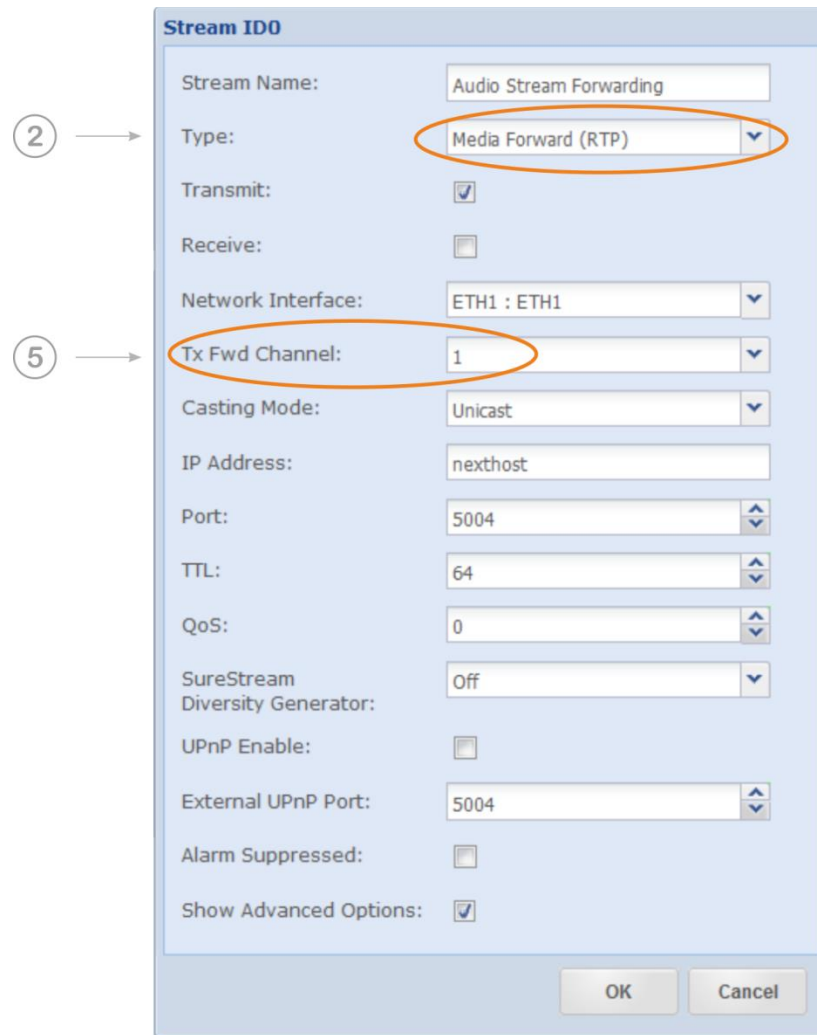
- ❗ By choosing a forwarding channel number, you make the stream available in this channel for the transmitting path.

### 3.4.13.2 Forwarding an Audio Stream (Tx)

To forward an audio stream (RTP) implies that it has been received and made available in a forwarding channel first (refer to section 3.4.13.1). Audio streams consist of RTP/UDP packets; therefore, Media Forward (RTP) must be chosen to forward the audio in RTP packets.

#### Encoder and Decoder Media Forward

This configuration is the same as for transmitting an audio stream except for the selected Forwarding channel number and the Stream Type.



The screenshot shows the 'Stream ID0' configuration window. The 'Stream Name' is 'Audio Stream Forwarding'. The 'Type' is 'Media Forward (RTP)'. 'Transmit' is checked, 'Receive' is unchecked. 'Network Interface' is 'ETH1 : ETH1'. 'Tx Fwd Channel' is '1'. 'Casting Mode' is 'Unicast'. 'IP Address' is 'nexthost'. 'Port' is '5004'. 'TTL' is '64'. 'QoS' is '0'. 'SureStream Diversity Generator' is 'Off'. 'UPnP Enable' is unchecked. 'External UPnP Port' is '5004'. 'Alarm Suppressed' is unchecked. 'Show Advanced Options' is checked. 'OK' and 'Cancel' buttons are at the bottom.

Figure 3-34 shows the configuration options for Media Forwarding (RTP)

- ➔ (2) Select the Stream Type: Media Forward (RTP) for transmitting the audio stream. All other values must be set for audio transmission (refer to section 3.4.11).
  - ➔ (5) There are six Forwarding channels available; select one channel for this stream.
- ⓘ For Stream Forwarding (UDP and RTP), the data source is the "Channel Number"! The example above reads from channel 1 and forward the IP stream (RTP).
- ⚠ This forwarding option allows the configuration of bidirectional streams - this feature is not recommended and will be removed in a later firmware.

### Forwarding an Audio Stream (Tx) *(continued)*

In the image below, Decoder A is configured as shown in Figure 3-33 (Rx) and Figure 3-34 (Tx). Decoder A receives an audio stream from the network, decodes the stream and forwards the payload to Decoder B in the same or different network.

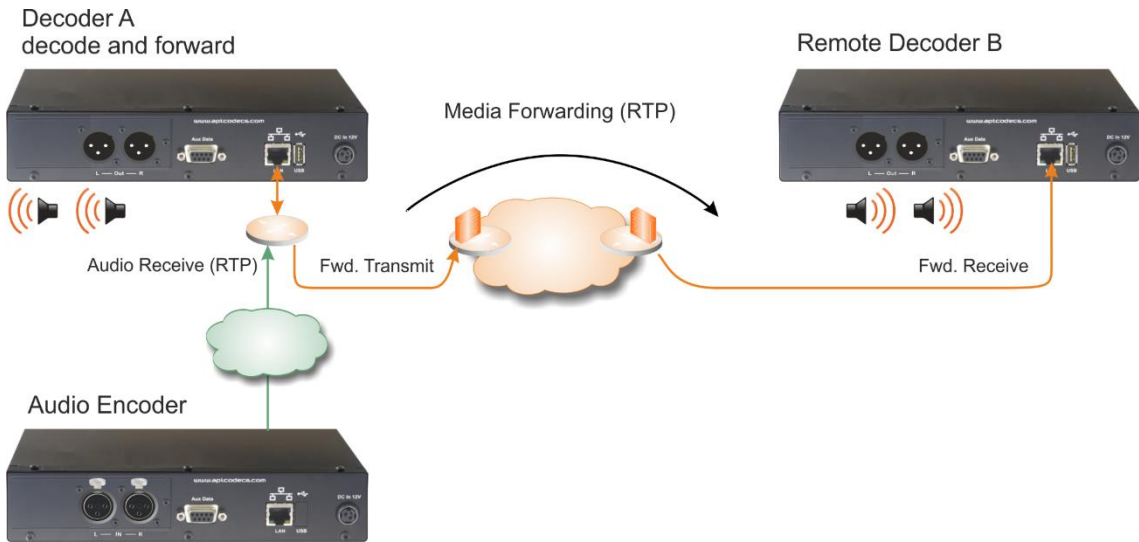


Figure 3-35: Shows an application of Media Forwarding (RTP)

### 3.4.13.3 IP Stream Forwarding (UDP)

The principles of Stream Forwarding are described and discussed in section 3.4.10.

If you want to forward a UDP stream regardless of the encapsulated protocol or no protocol, **IP Forwarding (UDP)** must be selected in the stream type selection. This method forwards the entire UDP content; it may be audio data or non-audio data.

Typical application is to forward RDS or PAD data through the same network as the audio stream. The audio stream is separately configured. This application runs two IP streams.

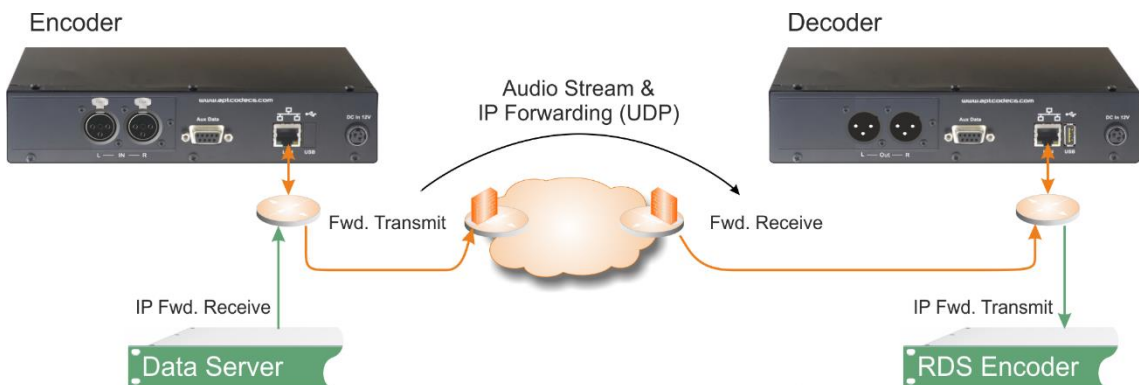


Figure 3-36: Shows a typical application for non-audio data forwarding



### 3.4.13.4 Combination of UDP/RTP Forwarding

The principle of UDP/RTP re-encapsulation is described in section 3.4.10.3.

A typical application for re-encapsulation of UDP content into RTP packets is the protection of content against network errors by utilizing redundant streaming (SureStream).

The application below shows how a Digital Radio signal contribution through a set of IP Silver Encoder/Decoder can look like (it is the same principle for DAB or HD Radio).

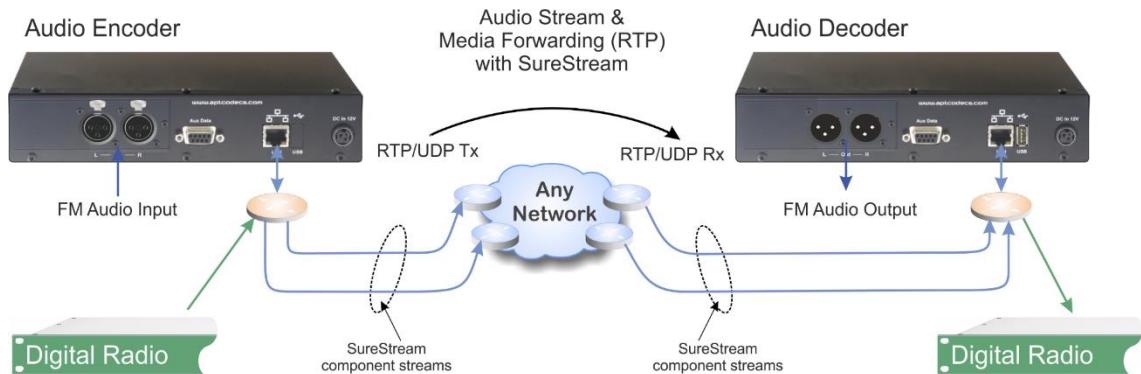


Figure 3-37: This example shows the FM Audio Input and the Digital Radio data streams protected by SureStream

#### Stream Type settings:

- ➔ Enc. - IP Forwarding Rx (receives the UDP stream from the digital exporter or EDI mux.)
- ➔ Enc. - Media Forwarding Tx (encapsulates the payload into an RTP/UDP packet)
- ➔ Dec. - Media Forwarding Rx (receives the RTP/UDP packets)
- ➔ Dec. - IP Forwarding Tx (forwards the data as UDP stream to the Digital Radio modulator).

**i** *Redundant streaming is only possible if the content is encapsulated in RTP packets. A UDP stream does not support sequence numbers or any flow control. The combination of IP Forwarding (UDP) and Media Forwarding (RTP) is the solution for many network applications.*

### 3.4.14 Advanced Stream Configuration

You can reach the “Advanced” configuration page directly from the Connection Page, from a shortcut on the Status Page - bypassing the profile wizard - or after the Configuration Wizard procedure has been completed. This page presents all configuration parameter of the IP streams.



Figure 3-38: Shows the Advanced configuration window


The Connection Wizard as described earlier has created the “New Profile” from the audio settings and the IP stream configurations. The “New Profile” now appears in the list of profiles on the left-hand side (Connections). This list of profiles is also accessible with the “Quick Connection” tool. A click on the little arrow opens or closes the profile list.

The Advanced configuration page offers all options for creating new profiles or modifying an existing one or deleting profiles from the list. It also allows changing the currently applied (and active) configuration on the fly.

### **Current Profile**

“Current Profile” shows the currently active profile name. On the example of Figure 3-38, the current profile is “Default”.

Clicking on “Default” in the profile section allows modifying the profile. If you have edited this (current) profile, it **MUST** be applied to the unit to save it; saving the “Current” profile without applying it to the hardware is not possible. It can be copied with another name by using the “Save as...” function (1); also, you cannot delete the “Current” profile.

 Re-applying a modified “Current” profile interrupts the active transmission.

### **Editing Profile**

Clicking on any other than “Current” profile in the list loads the profile configuration into the main Connection Page. At this stage, the profile can be modified (2) and saved by a click on the “Save” button (3) on the toolbar (“Save” appears if any profile was edited but not the “Current Profile”). This action does not affect the running configuration. The modified profile is now stored and can be applied to the hardware by clicking on the “Apply” button (4).

### **Creating and Deleting a new Profile**

Clicking on the “Profile Create” button (1) creates a new and empty profile. A new configuration can now be merged and saved as a new profile. Clicking the “Profile Delete” button deletes a selected profile from the list. Creating and/or deleting any profile while a “Current Profile” is loaded and running does not affect the audio streaming. The current profile is protected against accidental changes.

### **Copying a Profile**


After a profile was selected from the list and loaded into the Connection Page it can be copied by using the “Profile Save as...” function (1). A new name must be applied to this profile.

### **Applying a Profile to the Codec**

Clicking on a profile in the profile list loads the configuration into the Connection Page. Clicking the “Apply” button (4) loads the profile to the Codec hardware and appears as “Current Profile” in the list. This action always interrupts the IP transport.

### **Access the Performance Page**

You can access the performance page by clicking on the button in the tool bar at any time.

 *After a profile was applied to the hardware a popup alert (4) appears providing a shortcut link to the Performance Page. This popup alert stays for several seconds and will disappear after a timeout.*

### 3.4.14.1 Configuration Validation

The Validation (Valex) Engine protects the user against incorrect inputs and obvious configuration mistakes. It validates IP stream configurations made on the local unit in terms of consistency and correctness.

The Valex Engine cannot judge e.g. wrong destination IP addresses, or inconsistent configurations on a local encoder compared with a remote decoder.

The image below shows an example about how the Valex Engine intervenes and how it presents information about mistakes on the GUI.

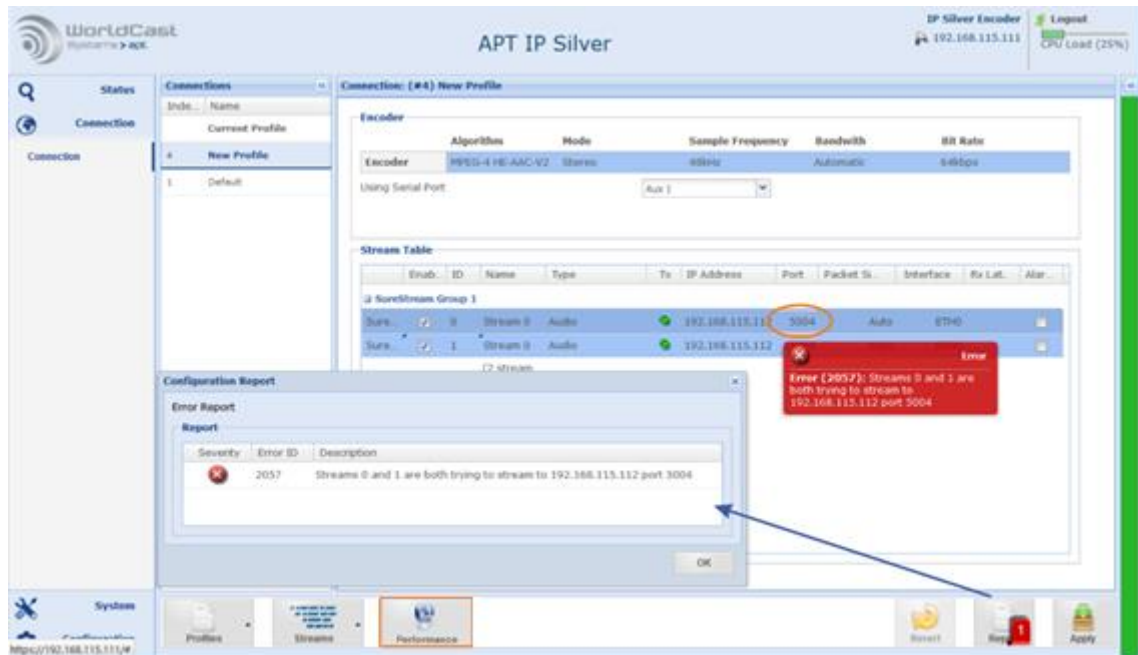


Figure 3-39: Shows how the Validation Engine presents error conditions and warnings

The invalid configuration in this example is the assignment of two transmit streams to IP port 5004. The Validation Engine highlights this misconfiguration as an error on the affected instances; i.e., on the port configuration of one Tx stream. A mouse-over event pops up with a clear error description.

Whenever a mistake is detected, the Validation report appears automatically and lists all instances where the mistake takes effect.

#### Notes:

---



---



---



---



---



---



---

## Validation Engine (continued)

The image below shows another example about how the validation engine warns on precarious configurations.

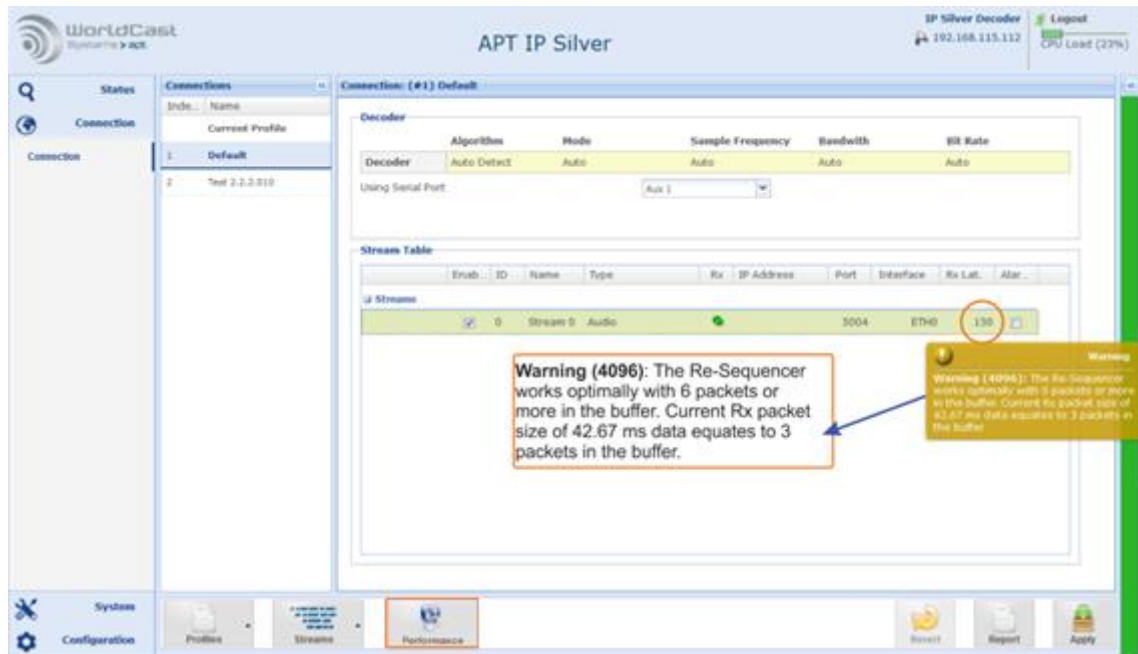


Figure 3-40 shows a yellow warning from the Validation Engine

The Validation Engine has identified a problem within this profile. In this example, the de-jitter buffer is set to 150 milliseconds. The Valex Engine has calculated 42.67 ms of packet time and indicates that the buffer must take at least six packets to get the full performance from the resequencer. Either the buffer size must be set to 256 ms (6x 42,67 ms = 256,02 ms) or the re-sequencer cannot unfold the full performance (which is an accepted condition).

This is a “Yellow” warning and not a critical alarm. The validation report does not pop up automatically, but with a mouse over on the highlighted fields, the warning will be presented.

**i** Due to the nature of the Validation Engine, it cannot foresee a misconfiguration especially on a Rx stream before the configuration was applied and becomes active. On the example above the Valex Engine must firstly receive packets before the required buffer size can be calculated.

### Notes:

---



---



---



---



---

## 3.5 Main Menu - System

### 3.5.1 Date and Time

The IP Siler runs an internal timing reference. This reference is always UTC. This UTC reference can be set either manually or via the NTP Client. The **System Time** of the unit, which all timing related actions are referring to, is derived from this UTC timing reference considering the Time Zone shift.

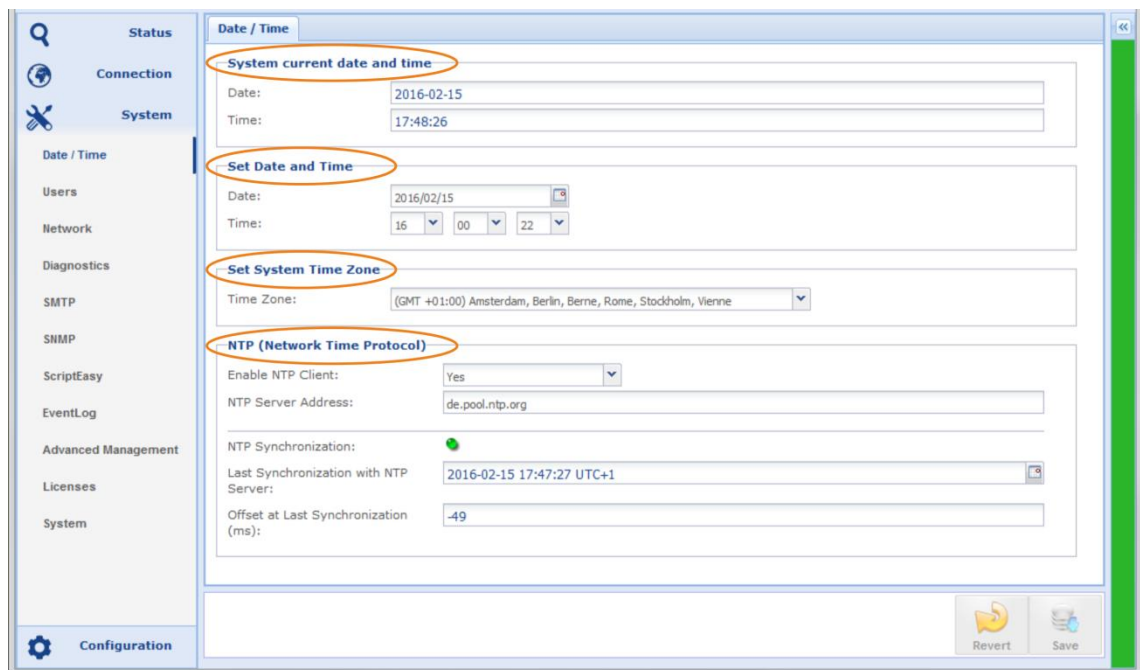


Figure 3-41: Shows the system page for date and time configurations

#### System current Date and Time


This section is read only and shows the current system date and time of the unit calculated from the selected timing references below. The GUI updates the system time display every 10 seconds.

#### Set Date and Time

It is best first to select your Time Zone, as those setting affect the System Time.

On boot-up the unit reads the time from your PC. Change date and time here to change the unit System Time manually. You must change a value and then click on "Save" in the toolbar to take the new values.

The manually entered time (UTC+TZ ) = System Time (displayed on the GUI).

 *Make sure that the NTP client is disabled if you want to set the system time manually!*

#### Set Local Time Zone

The Time Zone setting influences the System Time. The System Time is calculated from the UTC and the Time Zone. Select your local Time Zone to get the correct offset between UTC (Universal Time Coordinated) and the System Time.


### 3.5.1.1 NTP Client Settings

This entry allows enabling/disabling the NTP client (Network Time Protocol) as well as entering the NTP server IP address or Server hostname.

If the NTP Client is enabled ("Yes"), the internal timing reference is synchronized to the NTP time reference (always UTC). The NTP Client starts the synchronization process after a randomly configured delay.

Once the NTP reference is applied to the internal timing reference, the NTP service runs in a continuous mode where the external server is polled periodically. The poll interval is randomly adjusted and will increase after a time to a maximum of 1024 seconds.

It adjusts the system clock to stay in sync with the NTP reference. In case the timing is entirely out of sync from the NTP reference (offline etc.); you must force a re-synchronization by disabling and re-enabling the NTP Client.

 If the NTP time is selected and enabled as your time base do not manually change the system time! The NTP protocol is not made to resynchronize a significant time difference between the NTP reference and the manually set System Time. To resynchronize you must disable the NTP client (save) and re-enable it again (save).

### 3.5.1.2 NTP Synchronization Alarm



Should a server become unreachable for some time determined from the current poll interval, the NTP alarm is activated.

The last synchronization with the NTP server is displayed as well as the corrected time offset in milliseconds.




The NTP Synchronization LED is GREEN for correct NTP synchronization, Orange if the connection was lost or the synchronization has failed. The LED is gray if the NTP client is disabled.


#### NTP Routing

The NTP client connects to the network via ETH0 as standard, if a gateway is entered there. If no gateway address is entered, NTP attempts to connect via a VLAN or a virtual interface, if any, configured.

-  *Please note that an invalid IP address cannot be recognized as such. If the NTP client is to be connected to a different ETH port than the ETH0, the gateway address at ETH0 must be "0.0.0.0".*
-  *It is important to set the Time Zone correctly; otherwise, the NTP Client (when enabled) may unintendedly change the System time.*

### 3.5.1.3 NTP Server general Considerations

-  The NTP Server should always be referenced to an external source (GPS or another IP).
-  The stratum number of the clock should be as low as possible for greater accuracy (stratum numbers from 1 to 9 are preferred)
-  Servers running without a reference should be run in orphan mode for correct operation, e.g., a server using *ntpd* should add "tos orphan 6" to the *ntp.conf*. configuration file.

 *Any setting on this page must be saved before it becomes active on the hardware.*



## 3.5.2 User Management

### 3.5.2.1 User Accounts

The user management offers a two-level hierarchy. The Administrator account allows full access to the entire system while the Read-Only Account (Guest) may be used for monitoring purposes only. There is one Admin Account and one Guest Account.

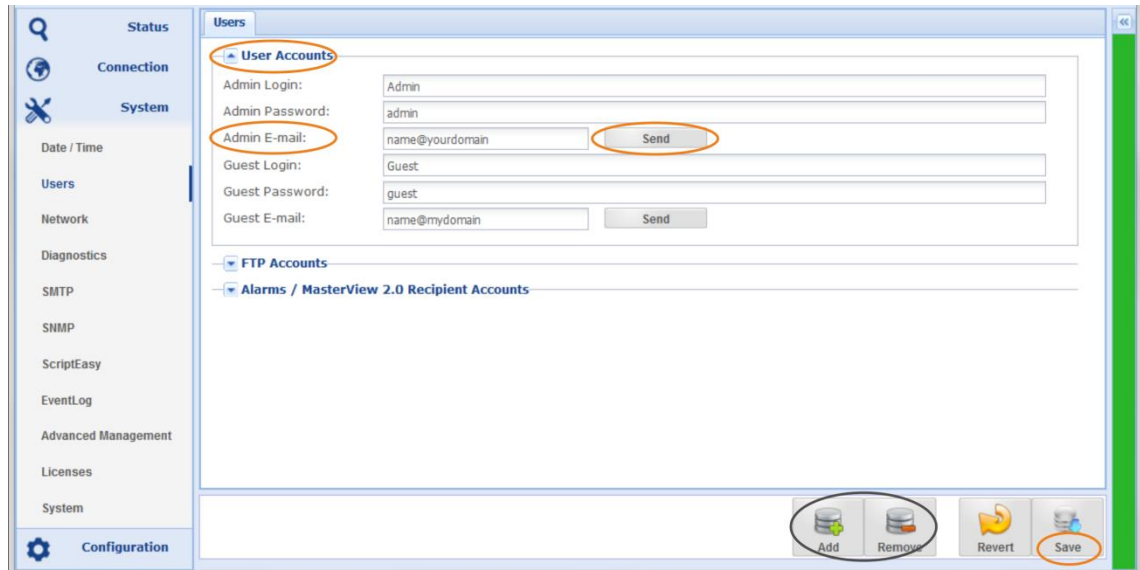


Figure 3-42: Shows the user page with account managers

The user management assigns administration privileges only to one Admin user at once. If another Admin user tries to connect from another seat while the first Admin user is logged in, this second LogIn attempt is treated like a Guest user (read-only). After logging out from the first Admin user, the administrator privileges are automatically assigned to the next admin user in the LogIn queue.

**i** The "Add" and "Remove" account buttons located on the toolbar do not take effect on the Administrator and Guest accounts.

#### **📡 User Account E-Mail Address**

The user accounts allow the entry of an email address for each of the users. This email address is used by the alarms system to send notification emails as configured in the alarm configurations. This page also provides an option for sending a test mail by clicking on the "Send" button. Sending emails requires a valid configuration of the SMTP details (refer to section 3.5.5).

**i** All changes on this page must be saved before they become active. Changing email address entries requires a re-connect to the unit.

**⚠** Do not forget to modify the default passwords for the user accounts before connecting to an unprotected network!



### 3.5.2.2 FTP Accounts

These FTP accounts will be used for the communication with external applications (future option).

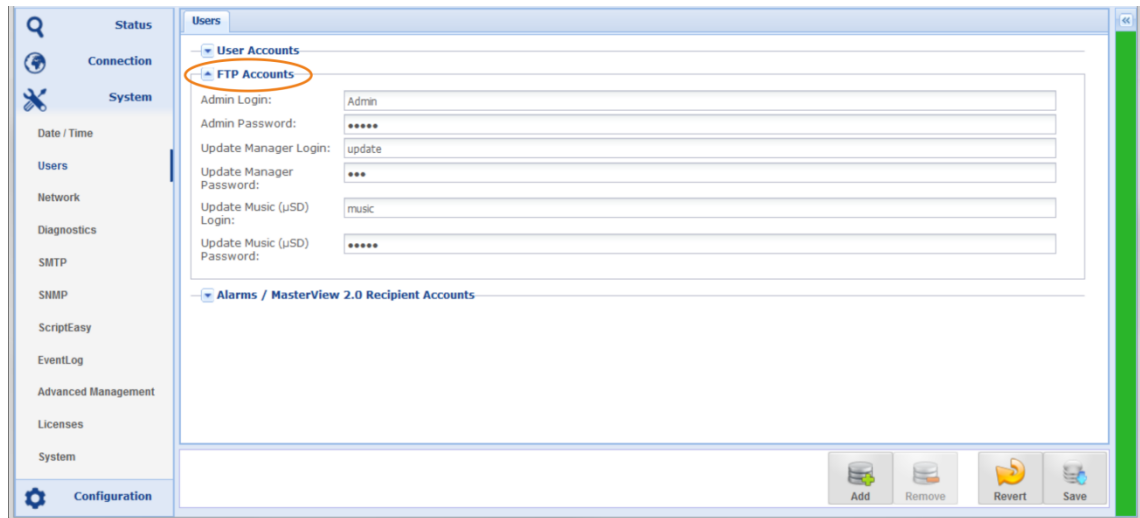


Figure 3-43 shows the user page with the FTP account manager

#### **ScriptEasy Applications**

ScriptEasy requires access via FTP for uploading a new script initially. However, ScriptEasy uses a dedicated and hidden FTP account which is invisible for the user (no management access).

#### **FTP Administrator**

Currently, there is no specific application accessing the unit by this account. You should change the default LogIn by a stronger password if you cannot filter the FTP service completely on the firewall page.

#### **FTP Update Manager**

*Currently not in use*

#### **FTP Update Music (μSD Card)**

Not used on the IP Silver units

### 3.5.2.3 Alarms / MasterView 2.0 Recipients Accounts

In this section, create accounts for MasterView users and/or users who should receive mail alerts. For each account enter the name and the email address.

Three access levels are available:

#### **Administrator:**

Access to all parameters and pages without restriction.

#### **Guest:**

Access to configuration and MasterView pages in read-only mode.

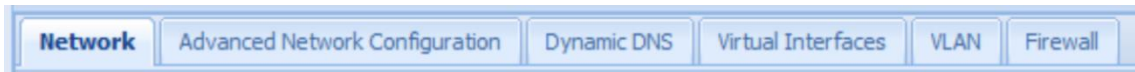
#### **Operator:**

Access to MasterView pages only, with the ability to trigger script actions with control buttons.

For email alarms, specify the minimum severity level the alarm must have before it is sent to that user: critical, major, minor, warning, all or none.

### 3.5.3 Network Configurations

This section consists of six pages organized by six tabs on the top of the window.



#### 3.5.3.1 Network - Network

This page is the first page of the network configuration showing the Current Status and the manually entered network settings. It is organized into five broad categories.

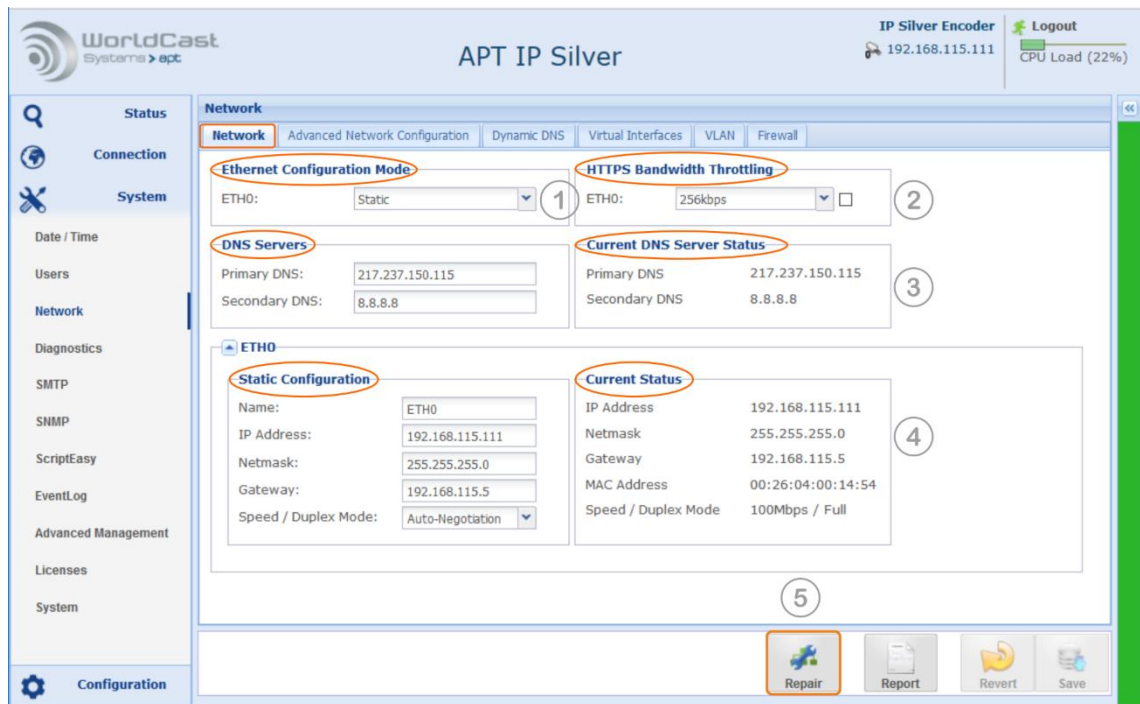


Figure 3-44 shows the options on the Network configuration page

#### 📶 (1) Ethernet Configuration Modes

- ➔ Static Mode for manual IP address assignment
- ➔ DHCP Mode that takes the IP configuration from a DHCP server
- ➔ "Bridged Modem" supports connected modems in Bridge Mode, i.e., DHCP=enabled, Firewall=enabled on all ports except port 443.

⚠️ When you change the configuration mode back to either Static or DHCP, you must manually disable the firewall filters if desired.

#### 📶 (2) HTTPS Bandwidth Throttling

Bandwidth Throttling allows you to limit HTTPs traffic over the network and can be set from 16 kbps to 1000 kbps. With this setting enabled, a disproportionate use of the network capacity by the GUI can be avoided, especially on the first start. In the case of low network capacity, the possible impairment of the audio stream is prevented.

- i** Note that a low value (<512kbps) results in longer load times when the WEB GUI is started for the first time.

### (3) DNS Server and Status

Values on the right-hand side display the currently applied DNS server configuration. This Current Status could be from the DHCP server if this mode was enabled or from manual settings.

- ➔ Primary DNS from static or DHCP mode
- ➔ Secondary DNS from static or DHCP mode

Usually, the DNS address is the Network Gateway address (the address of your router). DNS server addresses can be managed manually or by the DHCP server. The DHCP server configures both DNS entries from the same network.

- i** On static IP address settings, the DNS address must be entered manually. In DHCP mode, the DNS addresses are applied by the DHCP server in the network.

### (4) Current Status and Static Configuration for ETH0

Section 4 shows the “Current Status” of the interface on the right-hand side. The entry fields for the “Static Configuration” are located on the left-hand side. Depending on the configuration mode the “Current Status” can be either the manually edited configuration or the settings applied by a DHCP server.

The “Static Configuration” asks for:

- ➔ Name of the Interface (eight characters allowed)
- ➔ Static IP Address of the interface
- ➔ Netmask of the interface
- ➔ Gateway address – necessary for the WAN connection
- ➔ Port speed and duplex modes (must be selected manually in any case)

### (5) Repair Network

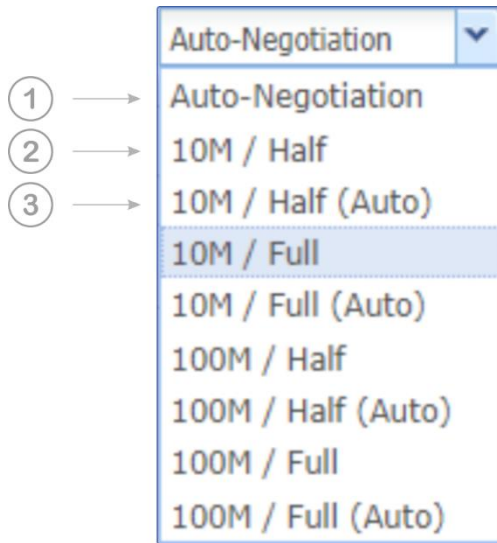
Clicking on this button re-applies the network settings to the unit. It brings the ports down and up again. Bringing the ports down and back up also has the effect of resetting equipment that is external to the system (routers or others).

### Ethernet Port Speed

In addition to the full auto negotiation mode for Port Speeds, it is possible to control the setting using the Restricted Auto Negotiation method or the hard-coded port speed setting.

Restricted Auto Negotiation means, the ETH port advertises only the manually selected speed and mode (half/full duplex) to the corresponding ETH interface on the switch. To get the speed and mode correctly negotiated, you must set the connected switch to Auto Negotiation or to the same restricted negotiation mode.

The hard-coded inputs are not negotiated. To establish a trouble-free connection, the remote station (the switch) must be set in the same way.



- 1) Full Auto-Negotiation: The interface advertises all speeds and modes (full).
- 2) Hard-Coded: The value set here (speed and mode) is not negotiated and must be congruent with the remote station.
- 3) Restricted-Negotiation (Auto): The setting is negotiated, but only this one value is advertised by the Interface.

**i** Note, the **Restricted Auto Negotiation** method is different to hard coded port speed setting. The corresponding ETH port must set to either the same method if supported or to Full Auto Negotiation!

**⚠** By definition of the negotiation algorithm, if the negotiation process fails, the setting falls back to the smallest (default) value: 10M / half.

Notes:

---

---

---

---

---

---

---

---

### 3.5.3.2 Advanced Network Configuration



Advanced Configuration provides UPnP settings for the management ports.

### 3.5.3.3 UPnP - NAT Traversal Mode

The NAT traversal mode enables the IP Silver to request port mappings from an Internet Gateway device using a sub-section of the UPnP protocol (Universal Plug and Play) called the Internet Gateway Device Protocol (IGD Protocol).

When UPnP is enabled on a router, the IP Silver can request port mappings to be added and removed automatically without the need to edit the router configuration. Router configurations do not need to be backed up or transferred.

The IGD protocol, supported by UPnP, ensures that port mapping operations are “hidden” from the user and allows a seamless plug and play operation. No server assistance or specific network infrastructure is required.

**i** IGD is the only part of the UPnP protocol which is used in the Codec device.

For the management settings, the UPnP page provides the controls as shown in the screenshot below.

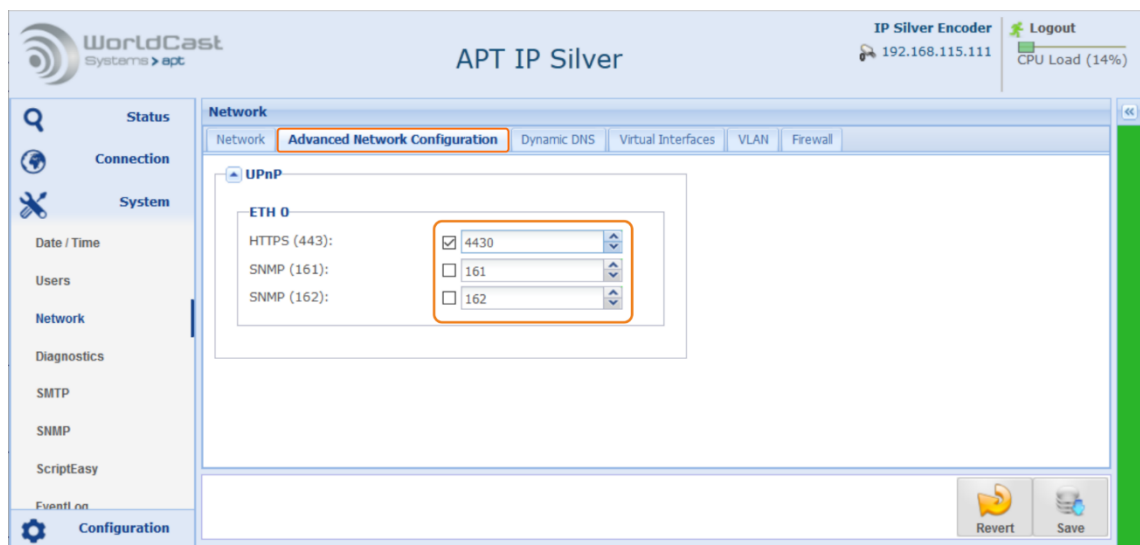


Figure 3-45: Shows the UPnP settings for management port 443

This page allows specific port mapping of common services, utilizing UPnP.

The example above shows a port mapping on port 443 for HTTPS. The check box enables the port forwarding in the router. With this setting, a connect request from a browser to the external IP address and port 4430 (HTTPS) is re-routed to port 443 on the Codec, identified by its MAC address (port forwarding rule in the router).

### 3.5.3.4 Dynamic DNS



Dynamic DNS is a method which automatically updates a name server in the Domain Name System (DNS) with the active DNS configuration of a configured hostname, address or other information.

The IP Silver provides an integrated Dynamic DNS client allowing communication with the most popular Dynamic DNS service providers. With this service enabled, the network interface of the IP Silver can be addressed, in a WAN environment, without using its allocated numeric IP address. Each interface should be configured with a unique hostname that can be utilized instead of a numeric destination IP address for WAN-based audio streaming.

Usually on xDSL lines, the DSL router receives an allocation of IP address by the Internet service provider. The assigned address may either be static or may change from time to time (dynamic).

The screen shot below shows the Dynamic DNS configuration page. Before this DDNS client can be used, a hostname must have been registered on one of the DDNS services provided on the drop-down list (1).

- ① *Once a hostname is registered and applied to an interface, this hostname can be used on the streams table as the destination address. Regardless of where the unit is (globally) connected, the stream finds this device automatically.*

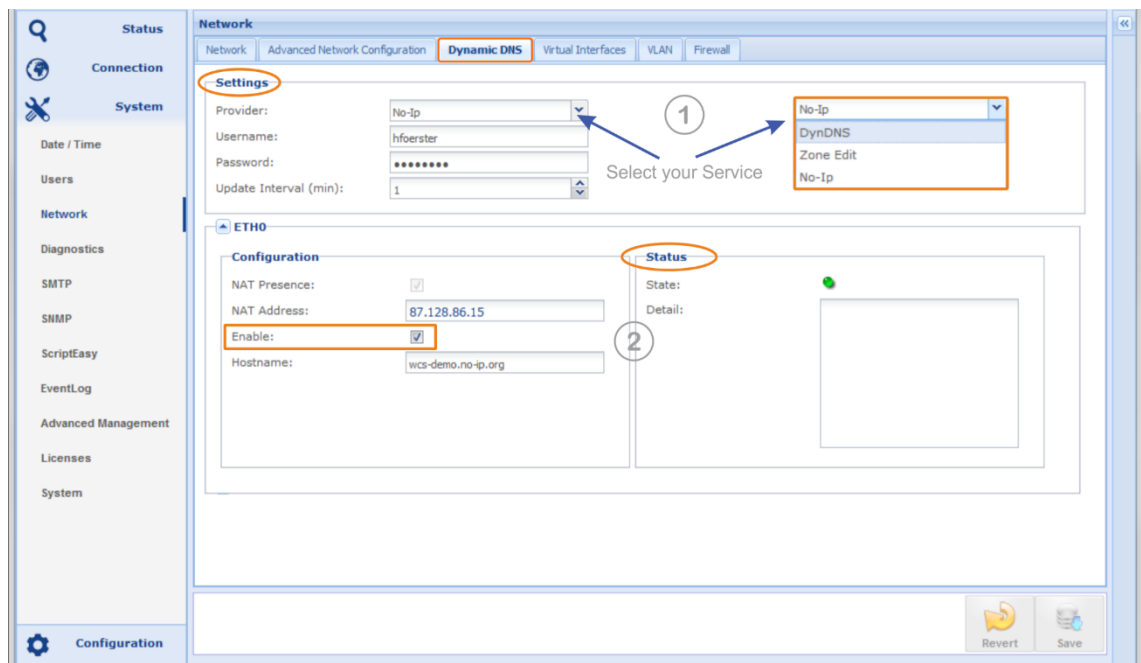


Figure 3-46: Shows the Dynamic DNS client settings and status information

### Dynamic DNS (*continued*)

The example above uses the No-IP service ([www.noip.com](http://www.noip.com)). With the username and the password, the client connects to this DDNS service provider if the “Enable” checkbox is ticked on the ETH port and the entries were saved by clicking on the “save” button.

The registered hostname for the Codec interface for this example is wcs-demo.

The full hostname entry for the No-IP account is wcs-demo.no-ip.org.

Once DDNS is enabled, the software client automatically enters the public IP address of the current link in the “NAT Address” field (2) – this is for information only (read-only field). Further, the status field presents messages from the DDNS provider if applicable. This can be error messages or other information.

The stylized LED on top of this field indicates the status of the DDNS service:

Green: active and ok

Red: active but not ok

Grey: inactive (not enabled)

Example of an error message from the status field:

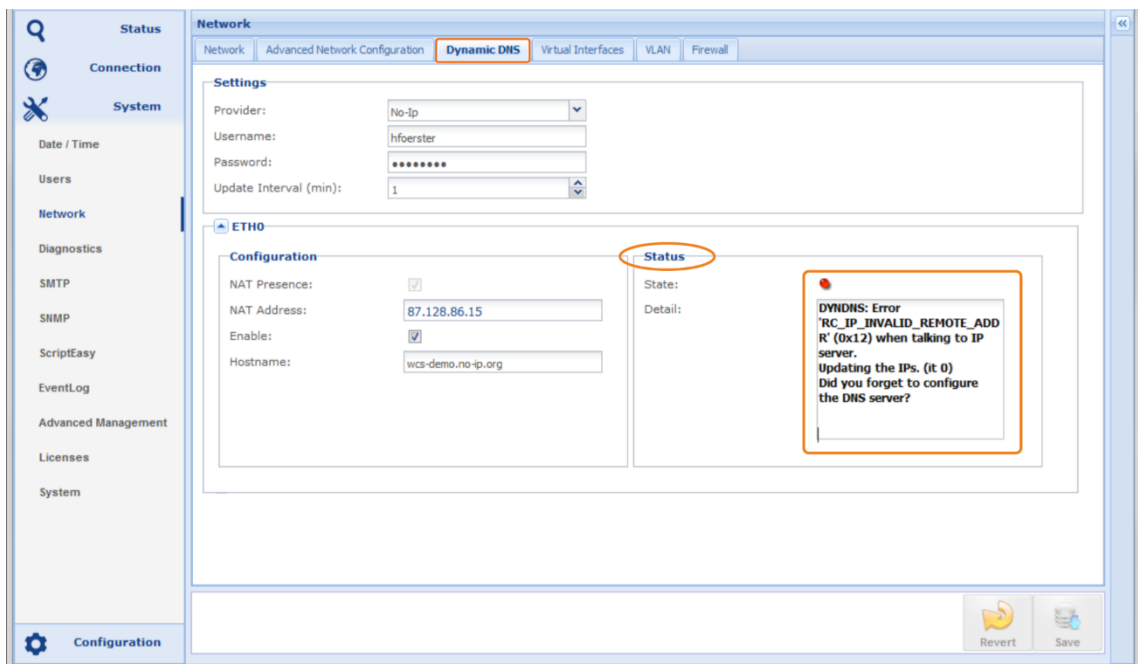


Figure 3-47: Shows an error message of the DDNS status

This error message was caused by having no DNS server information entered on the network configuration page. The messages are almost in clear text and guide to the current misconfiguration.

### 3.5.3.5 DNS Look Up - mDNS

DNS lookup allows the connection to the unit in a LAN without knowing the current IP address! Using mDNS (multicast DNS) requires Zeroconf installed on the PC. The easiest solution for this is to install Apple's implementation of Zeroconf for Windows (Bonjour Service). In the case that DHCP must be used to get a network access, the DNS lookup feature may help to identify the current IP address of the unit that was dynamically applied. With the DNS look up you can access your unit by using the mDNS name for the browser navigation.

**i** For using mDNS your management PC must be connected to the same sub-network as your unit.

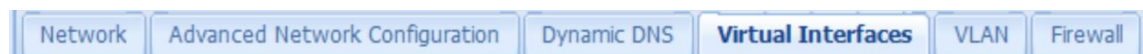
**📶 For the IP Silver the mDNS name is:**

wcs-SerialNumber.local – e.g. for a IP Silver Encoder with serial number I000011:

<http://wcs-I000011.local>

The serial number is available on all production units on a label at the rear of the units. The “.local” domain is the standard domain of your PC.

### 3.5.3.6 Virtual IP Interfaces



With virtual IP interfaces applied to the physical ETH port (ETH0), the single physical interface can have multiple static IP addresses and multiple gateways, but without virtual LAN tagging.

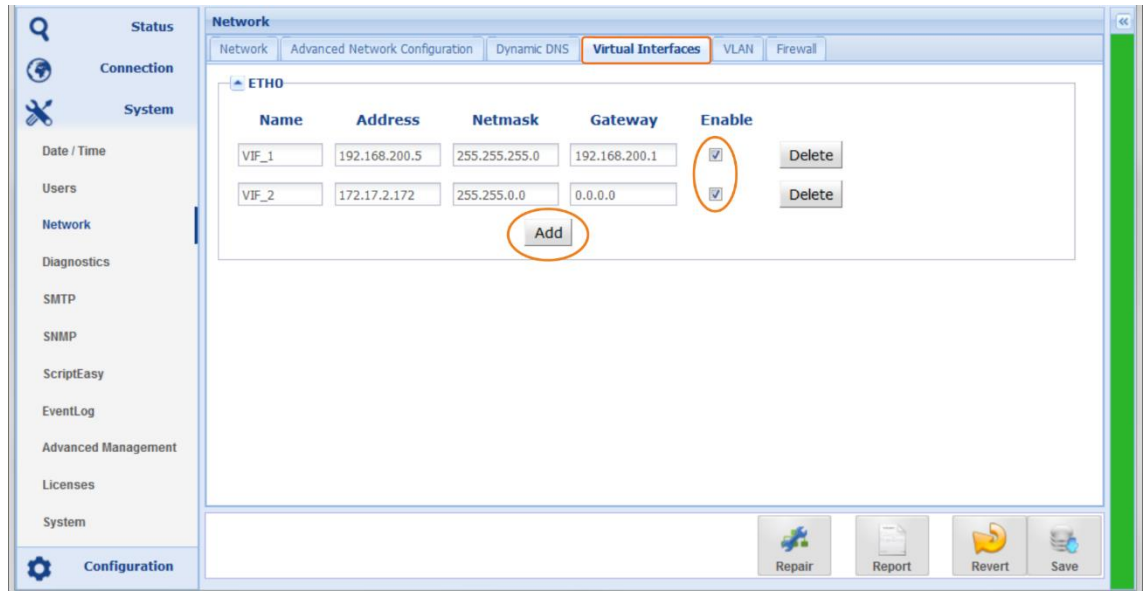
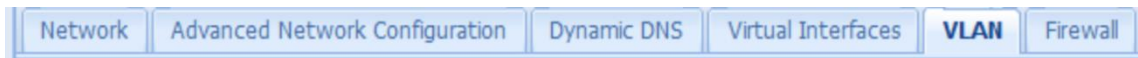


Figure 3-48: Shows the management page of virtual interfaces

Select the physical interface (ETH) and add a virtual interface. Enter a name (eight characters) and enter the IP address information. Enable the interface and save the configuration. In the stream configuration window (section 3.4.11.1), the new IP interface is available in the drop-down list (ETH0: VIFxxx)



### 3.5.3.7 VLAN Tagging – Virtual LAN



Applying VLAN IDs (VID) to the virtual interface allows integrating the IP Silver into a virtual LAN in accordance with IEEE 802.1q. A VLAN securely divides a network logically and keeps a broadcast domain within the limits of a VLAN (VID). With a VLAN topology in place, a single physical interface overcomes any constraints caused by the limited number of physical interfaces.

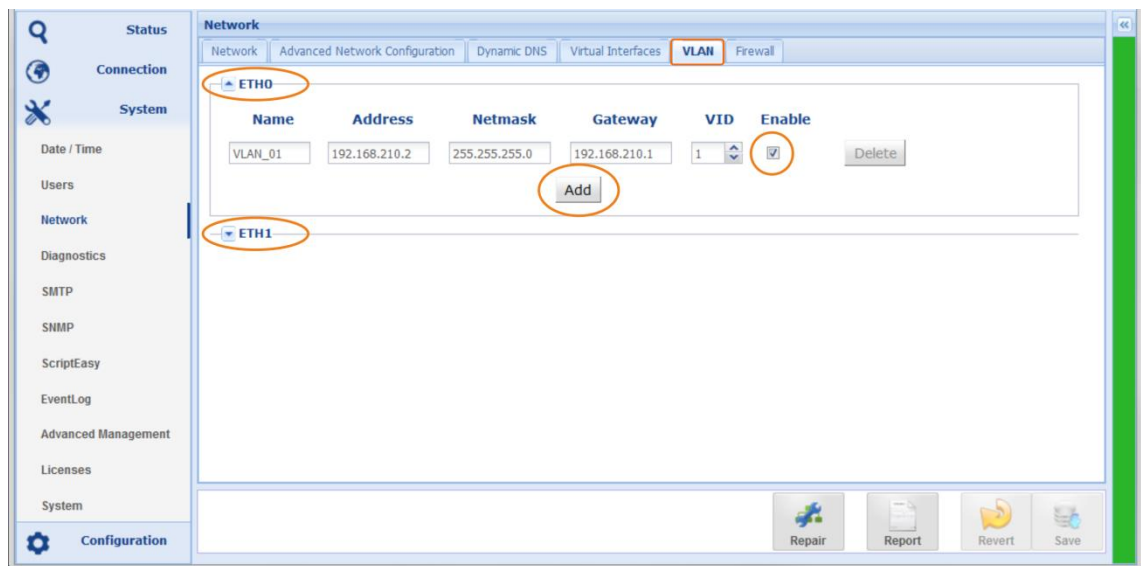


Figure 3-49: Shows the management page of virtual LANs (VLAN)

Select the physical interface (ETH) and add a VLAN. Enter a name (eight characters); enter the IP address information and the VID. Enable the VID and save the configuration. In the stream configuration window (section 3.4.11), the new VLAN interface is available in the drop down list (ETH0: VLANxx)

The IP interface of a VLAN is protected by the VLAN tag in the Ethernet frame (layer 2). Any stream to this MAC address without having the correct VLAN tag (VID) will be rejected from this interface. There are 4094 VLANs selectable.

**Notes:**

---

---

---

---

---

---

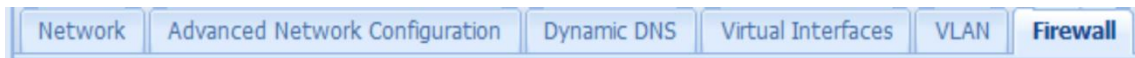
---

---

---

---

### 3.5.3.8 Firewall



As a network appliance, the IP Silver provides basic firewall features on the physical ETH port. The firewall configuration page offers a filter for various services and ports, selectable for each ETH interface.

**i** The checkbox activates the FILTER and blocks the port and the service of an interface.



Figure 3-50: Shows the filter options on the firewall page - HTTP service (port 80) is disabled on both interfaces

This service filter cannot replace a high-performance firewall in your WAN. The filter options simply allow shutting down unused services in the IP Silver.



Disabling port 80 and port 443 on the interfaces entirely inhibits access to the unit. You must not disable HTTP and HTTPS.

#### TCP/UDP Ports protected internally or externally

Port	Service	Protection
TCP 80	HTTP, WEB Services	Internal firewall
TCP 443	HTTPS, Web Services	Internal firewall
TCP/UDP 111	RPC	External
TCP 21	FTP	Internal firewall
UDP 161	SNMP	Internal firewall
UDP 162	SNMP TRAP	Internal firewall
UDP 5577	Internally used	External
UDP 7777	APT NMS communication	External
UDP 7778	APT NMS communication	External


### 3.5.4 Diagnostic Page

#### **Restart**

This forces a unit Reboot – the unit will reboot without configuration changes.

**Restart**

Reboot Unit:

 40 seconds loss of service


#### **Default Configuration**

Resets the System and sets all Configurations to factory defaults but keeps all network settings, including assigned port names, VIF and VLAN configuration.

**Default Configuration**

Reset system configuration to default:

 40 seconds loss of service

 The "Reset System to Default Configuration" action deletes all profiles, ScriptEasy Scripts (save first!) and all other user configurations BUT NOT the network settings!

#### **Ping Tool**

This ping tool works in the usual way and allows the sending of a ping directly from the selected interface. This diagnostic tool facilitates the identification of possible connection problems.

**Ping Tool**

Network Interface:

IP Address:

Ping:

Ping Tool Status:

Ping Result: **PING 192.168.115.201 (192.168.115.201) from 192.168.115.200: 56 data bytes**  
**64 bytes from 192.168.115.201: seq=0 ttl=64 time=11.291 ms**  
**64 bytes from 192.168.115.201: seq=1 ttl=64 time=0.946 ms**  
**64 bytes from 192.168.115.201: seq=2 ttl=64 time=0.946 ms**  
**64 bytes from 192.168.115.201: seq=3 ttl=64 time=1.038 ms**

--- 192.168.115.201 ping statistics ---  
**4 packets transmitted, 4 packets received, 0% packet loss**  
**round-trip min/avg/max = 0.946/3.555/11.291 ms**

### 3.5.5 SMTP Client (Email Setup)

All APT devices support email alerts on pre-configured operational conditions. E.g., any alarm condition can send an email message to a user account mail address (refer to section 3.5.2.1).

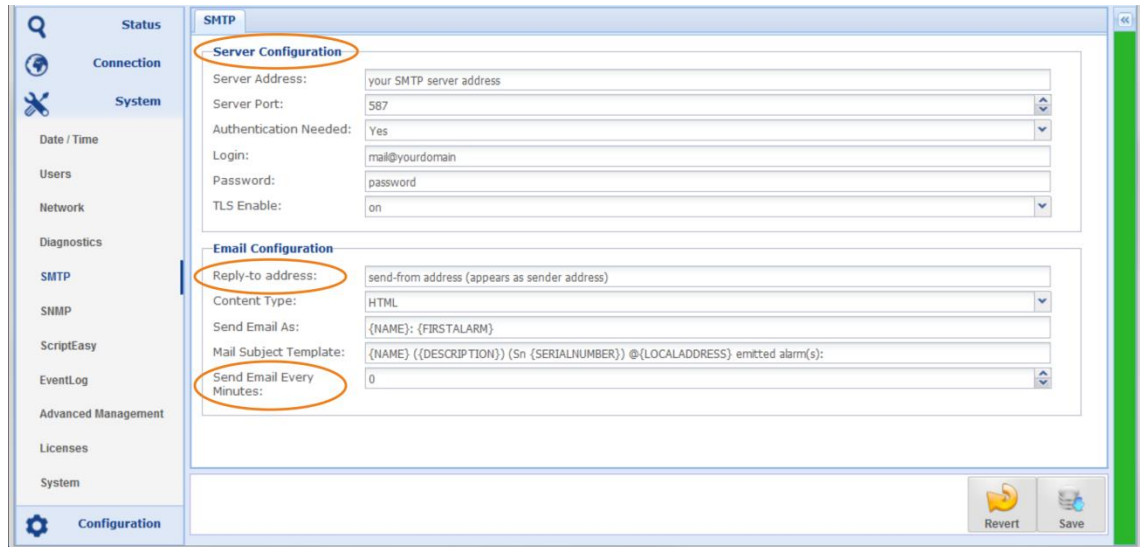


Figure 3-51: Shows the SMTP (email) configuration page

This setup page follows a standard procedure for setting up an email account.

#### 📶 Server Configuration

This section requires the configuration detail of your SMTP server as provided by your service provider or IT administrator.

#### 📶 Reply-to Address

This is the sender address and can be any valid address. This address appears in the "sent from" field of the receiving email client.

#### 📶 Send Email Every Minutes:

The number of minutes set here defines the interval to send an email. With the value "0" minutes the SMTP server sends the mail immediately when an alarm occurred.

Once this configuration is completed and tested, the mail alert feature can be used in the alarm settings. An option for sending a test mail is provided on the User Account page (section 3.5.2).

The content of an alert email consists of system variables that cannot be changed. A variable is inside a curly bracket. All other content can be modified or added if desired.

E.g.: {NAME} ({DESCRIPTION}) can also be: (My {NAME}) (unit type: {DESCRIPTION})

#### 📶 Standard System Variables:

- ➔ {NAME}: Unit name which was applied to the unit
- ➔ {FIRSTALARM}: Alarm Status (Alarm active / Alarm cleared)
- ➔ {DESCRIPTION}: Information about unit Type, i.e., IP Silver Encoder
- ➔ {SERIALNUMBER}: Serial number of alarming unit
- ➔ {LOCALADDRESS}: IP address of port ETH0 of alarming unit

### 3.5.6 SNMP

SNMP has been enabled as standard on all APT NextGen devices. The SNMP implementation supports both SNMPv1 and SNMPv2c.

#### 3.5.6.1 SNMP Agent

This page provides the configuration options of the inbuilt SNMP agent. These are the basic settings to setup the communication between the Codec device and the SNMP managers in the network (remote managers).

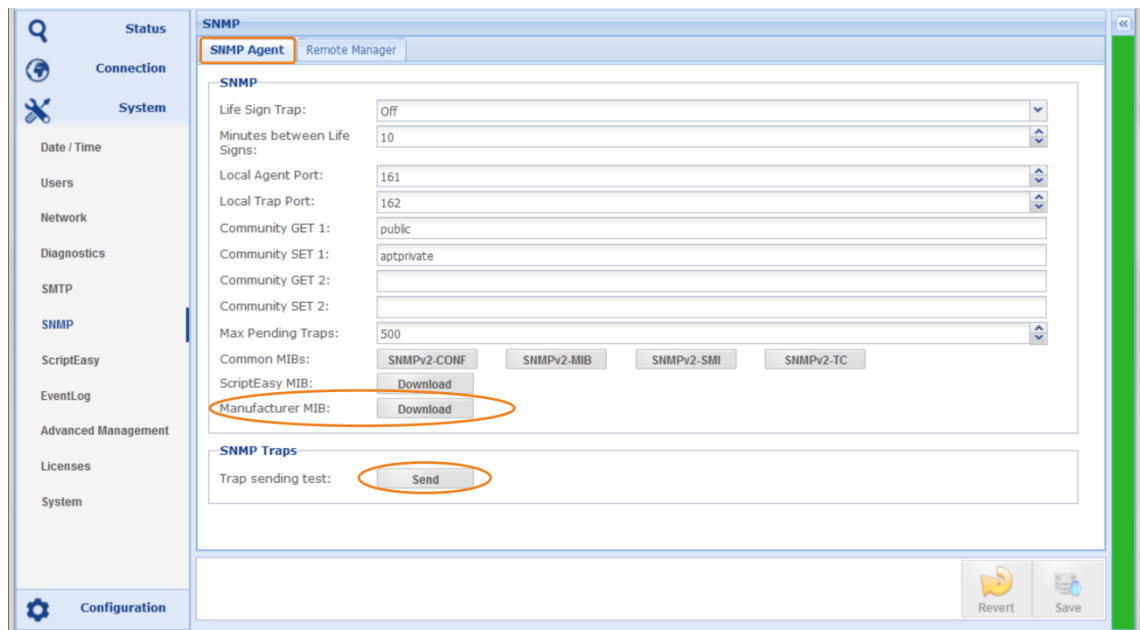


Figure 3-52: Shows the SNMP-Agent configuration page

#### SNMP options on this page

- ➔ Life Sign Trap: this is a heartbeat trap and can be enabled, disabled and managed here.
- ➔ The SNMP Agent UDP port (default port: 161)
- ➔ The SNMP Agent UDP port for sending Traps (default port: 162)
- ➔ Community Get 1/2: two public communities are supported; any name can be entered here (connect to port 161)
- ➔ Community SET 1/2: two private communities are supported; any name can be entered here (connect to port 161)
- ➔ Max Pending Traps defines the max number of traps in the memory (255 to 500).
- ➔ MIB: Allows downloading the device MIB from the device
- ➔ Trap sending test: Click the button for sending a Trap

#### 3.5.6.2 SNMP MIB Files

You can download the required MIB files from this page.

- ➔ The Manufacturer MIB is the MIB of your device – this MIB file is required!
- ➔ The ScriptEasy MIB is only required if you have OIDs created with ScriptEasy
- ➔ The SNMPv2 files are common SNMP files. If your SNMP Manager refers to these files, you can download the full set from this page. These are no device-specific files.

### 3.5.6.3 SNMP Remote Manager

The SNMP Manager configuration allows the setup of four SNMP remote manager instances. The general Trap management has been integrated into this page, allowing a different Trap management for each of the remote managers. A Remote Manager describes the SNMP Manager in the network.

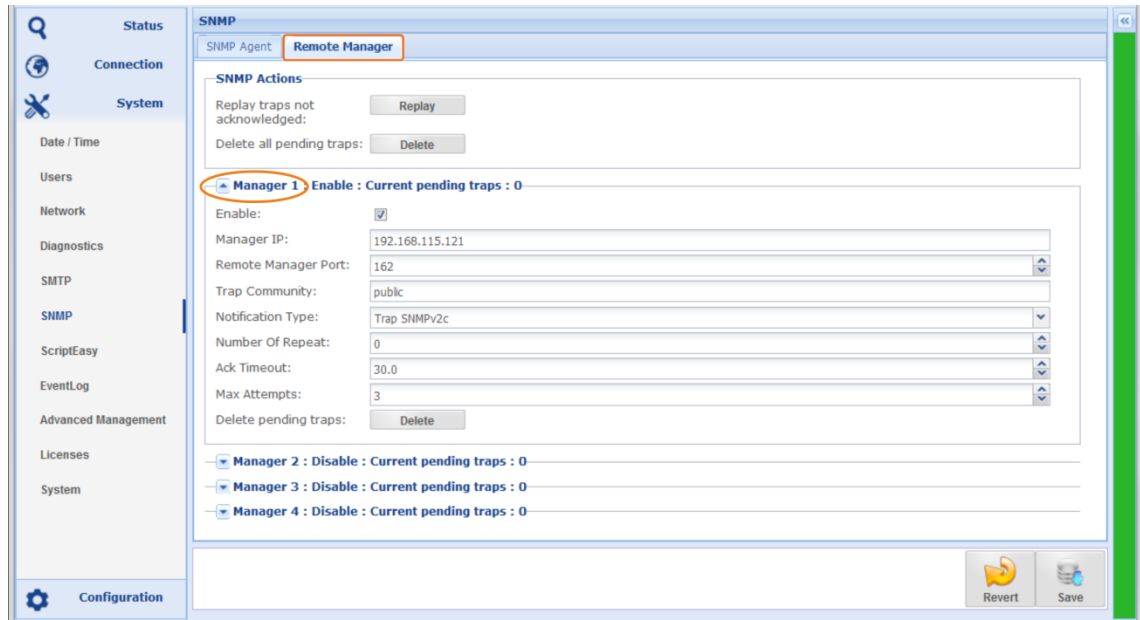


Figure 3-53: Shows the configuration page for the SNMP Remote Managers

#### SNMP Actions

This section allows control of the SNMP pending actions. A pending action is a non-acknowledged trap. This trap is stored in the unit; clicking on "Replay" re-sends the traps. Clicking on "Delete" deletes the pending traps from the memory.

#### Manager Configuration

This section provides configuration options for four different SNMP Managers in the network.

- ➔ Enable: This checkbox activates the configuration options of a Manager
- ➔ Remote Manager Port: This is the destination port for TRAPs on the Remote Manager
- ➔ Trap Community: Some SNMP manager offers a selection of trap communities
- ➔ Notification Type: this can be TRAPs SNMPv1, SNMPv2c or Inform notification SNMPv2c (sent on port 162)
- ➔ Number of Repeats: Defines the number of sending attempts if the acknowledgment is not received within the pre-configured time window (SNMPv2c)
- ➔ Ack. Timeout: Defines the time window during which an acknowledgment must arrive
- ➔ Delete: Clicking this button deletes the pending Traps of this Manager

### 3.5.7 ScriptEasy

A Script Application is a ScriptEasy script either supplied by WorldCast Systems or created by the customer, which adds extra functions to your APT Codec. The requirement to use an application is the activation of the ScriptEasy engine in your Codec. With the firmware release 2.x or higher, ScriptEasy is already enabled automatically. If you have installed an earlier firmware version, you need to upgrade to the current firmware.

Script applications are used for very different purposes. Most scripts are pure software applications that do not require additional hardware such as cables or adapters; some script applications, however, along with breakout cables or other utilities.

A separate user/developer manual can be found on the CD or downloaded from the [WorldCast System](http://WorldCastSystem.com) website (user account required).

#### 3.5.7.1 Application Builder

The ScriptEasy IDE (Integrated Development Environment) comes with as a separate PC application and consists of a graphical application designer (please contact your APT representative). The IDE allows creating the logic of an application, and MasterView is used to design individual dashboards. A dashboard can be utilized, but it is not mandatory. The following screen shot shows an example of how an application can be used on an IP Codec.

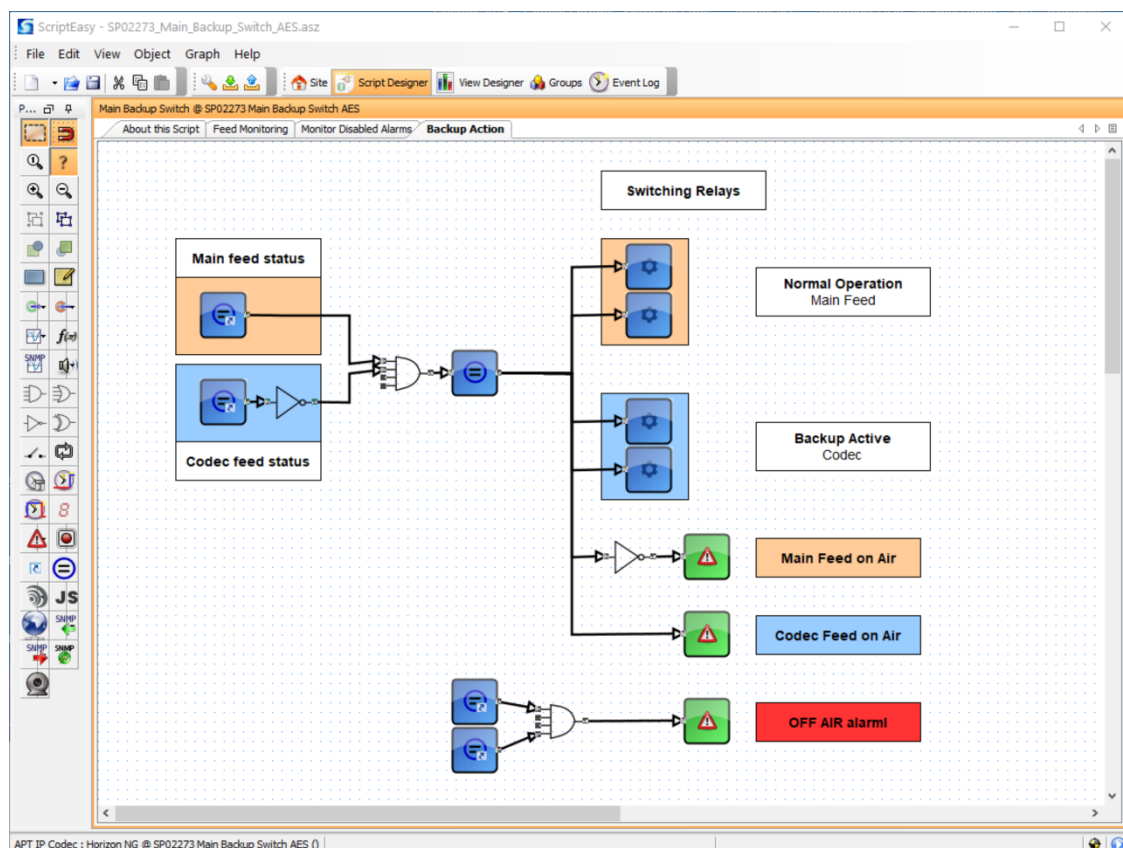


Figure 3-54: Shows the Script Application Designer IDE

The screenshot shows part of a multi-page script application (backup management).



### 3.5.7.2 Application

The application shown here by way of example monitors the main signal path and activates a backup link under certain conditions. The user has defined in the script the states that require switching of the signal paths. The following picture shows the application as a block diagram.

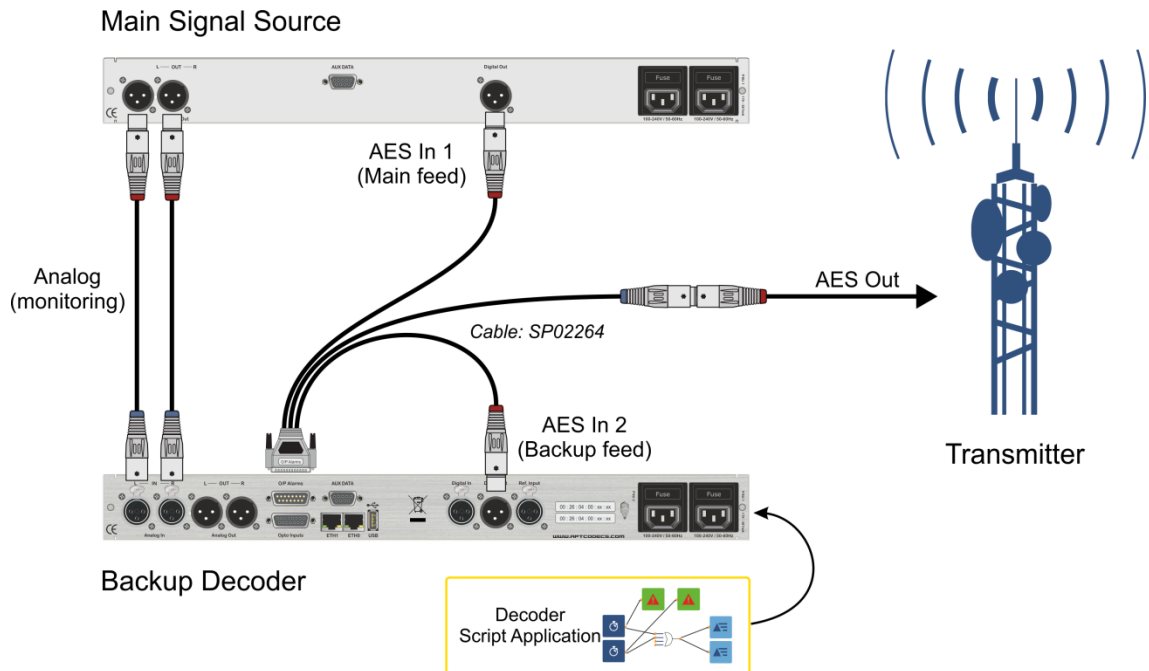


Figure 3-55: Shows the main-backup switching application controlled by the script application

This application monitors the main signal source, e.g. at a transmitter location, and switches the transmitter input to the backup source in the event of error. When the error condition is cleared, the script returns to the main signal.

The main signal is a local signal source such as a satellite receiver or an FM receiver or other. The backup signal is provided by the IP Codec via the network.

**i** This script and the required cable is available from WorldCast Systems (order code: SP02273).



### 3.5.7.3 MasterView

MasterView is the integrated web application for creating the dashboard and the graphical representation of the application, if so desired. An application also runs without a dashboard. MasterView is the browser-based version of the (legacy) MasterView application. You can start MasterView Web directly from the Codec GUI.

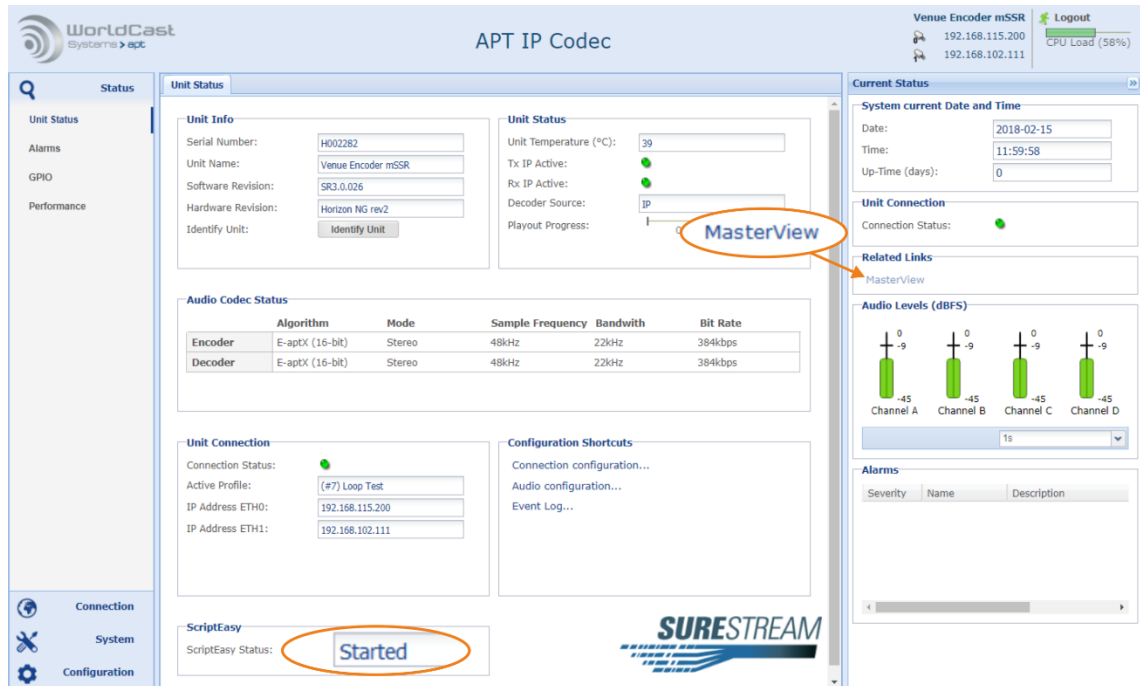


Figure 3-56: Status page showing the link to MasterView

With a script application running on the Codec device (script started), the link to the MasterView application becomes active on the sidebar. Clicking on this link opens a new browser window with MasterView. You must log in with your administrator account details.

### 3.5.7.4 MasterView Dashboard Designer

MasterView allows the design of individual dashboard views of the application created with ScriptEasy. The screenshot below shows the dashboard of the sample application in MasterView. Many more view variants (pages) are possible from the same application.

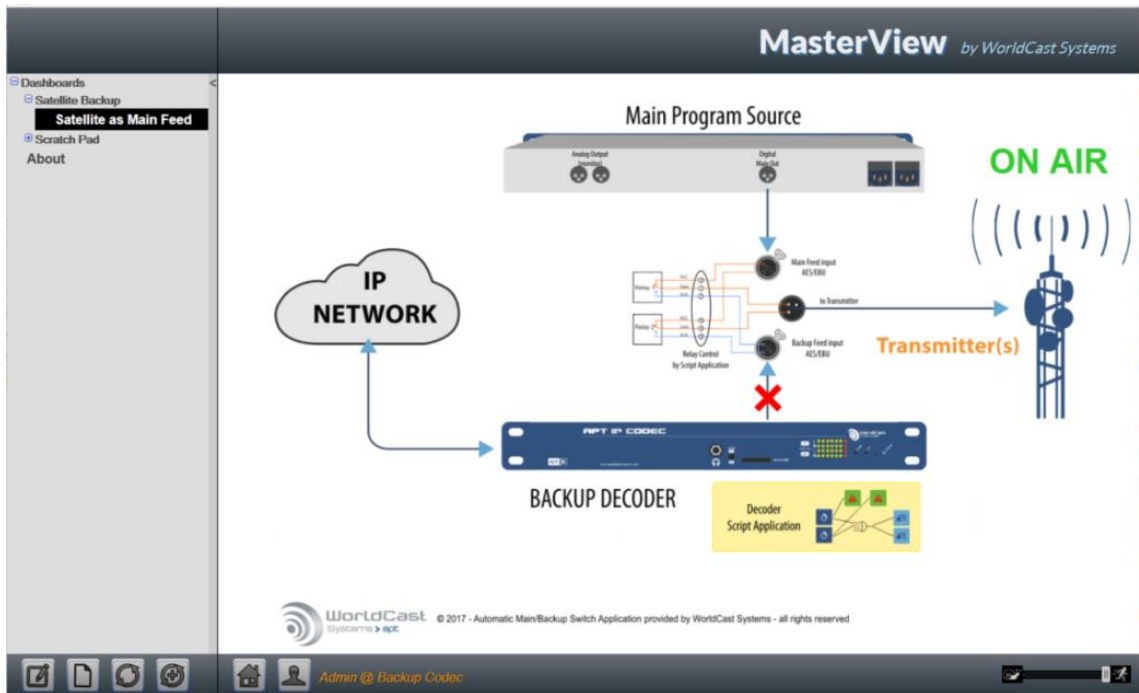


Figure 3-57: Shows the application status on the dashboard – On Air condition

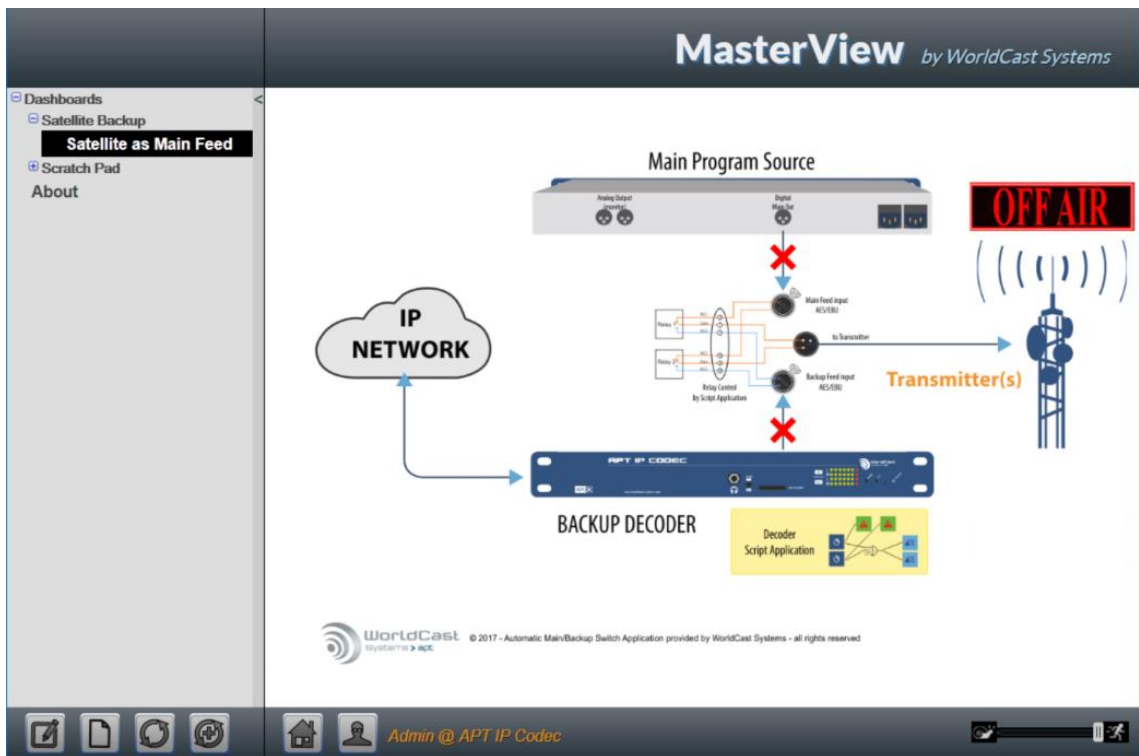


Figure 3-58: Shows the application status on the dashboard – Off Air condition

### 3.5.7.5 ScriptEasy Control

The ScriptEasy page is used to start and to stop an applied script. It shows the Current Status and allows entering a comment that describes the script.

Once uploaded to the hardware the script becomes “invisible” on the GUI. It starts whenever the unit is booted and can be stopped temporarily. When you have stopped the script on this page, it will restart after a reboot of the unit! If a script is loaded, the WEB GUI shows a warning when a user logs in the first time. Once you have acknowledged the script warning it will not appear again; this information is stored in a browser cookie.

- ❗ *A script may overwrite user actions on its own! If you want to deactivate a script permanently, you must follow the procedure described in section 3.5.7.6.*

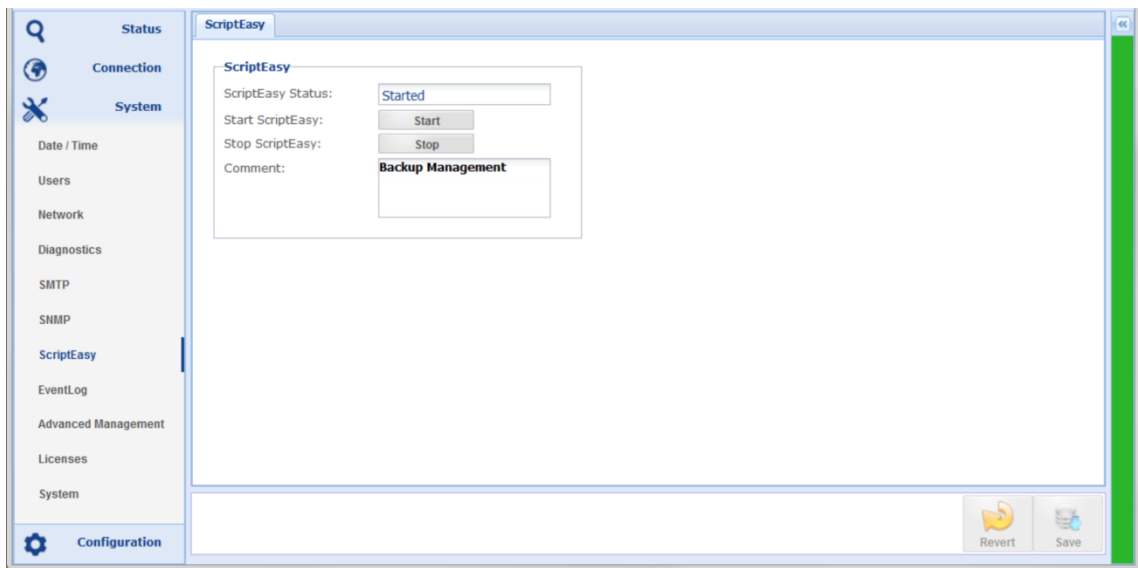


Figure 3-59: The ScriptEasy page in the system menu shows the script controls

- ❗ *A script becomes automatically active after system boot-up.*
- ❗ *Only one script can be loaded.*
- ❗ *A script can be stopped on the ScriptEasy page – but only temporarily. It becomes active again after re-boot!*
- ⚠ *ScriptEasy requires the FTP service for the initial script upload – make sure that FTP is not blocked by the Codecs firewall settings (refer to section 3.5.3.8).*

### 3.5.7.6 ScriptEasy Remove a Script

Once you have uploaded a script to the Codec device, it becomes active automatically. The GUI offers limited control of the script, but it cannot be deleted in a clear manner. To permanently deactivating (deleting) a script, it must be overwritten by an empty script (a script without content).

### 3.5.8 Event Logging

A basic event logging system is provided. It records all events in a single log file that can be inspected, exported and deleted. A history page allows searching for events in a defined time frame to limit the number of shown log entries.

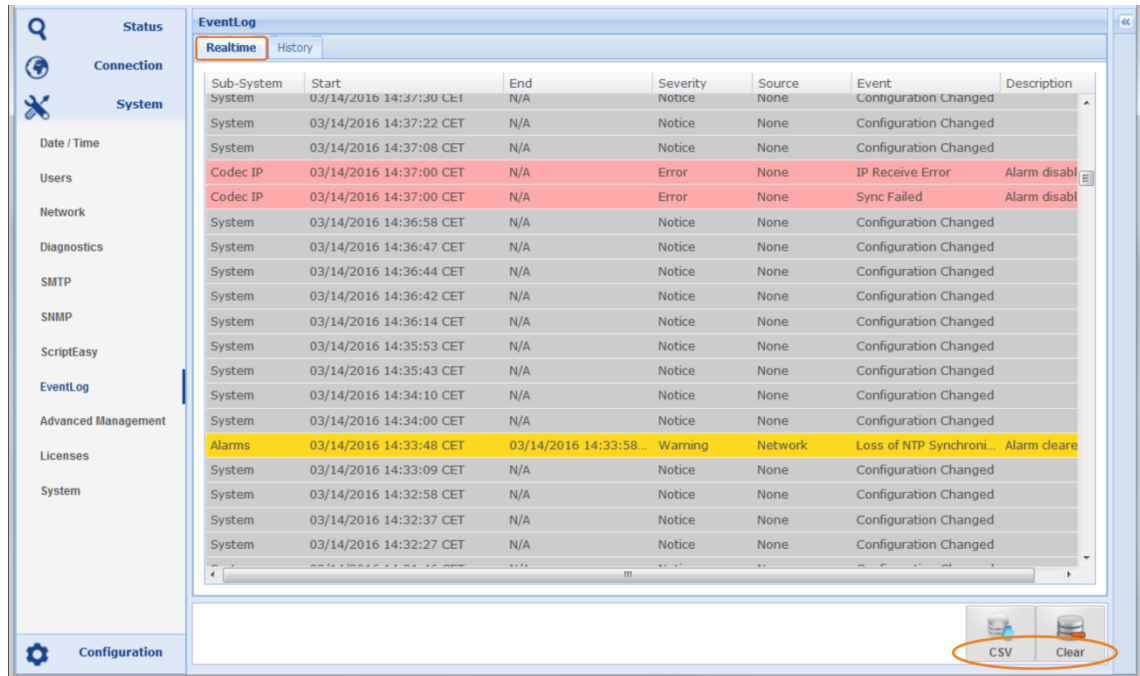


Figure 3-60: Shows Event Logs in the real time

#### 3.5.8.1 Event Log File Export

Clicking on the “Export to CSV” button opens a popup window from the browser. The file is formatted as a CSV file and can be imported to any spreadsheet application.

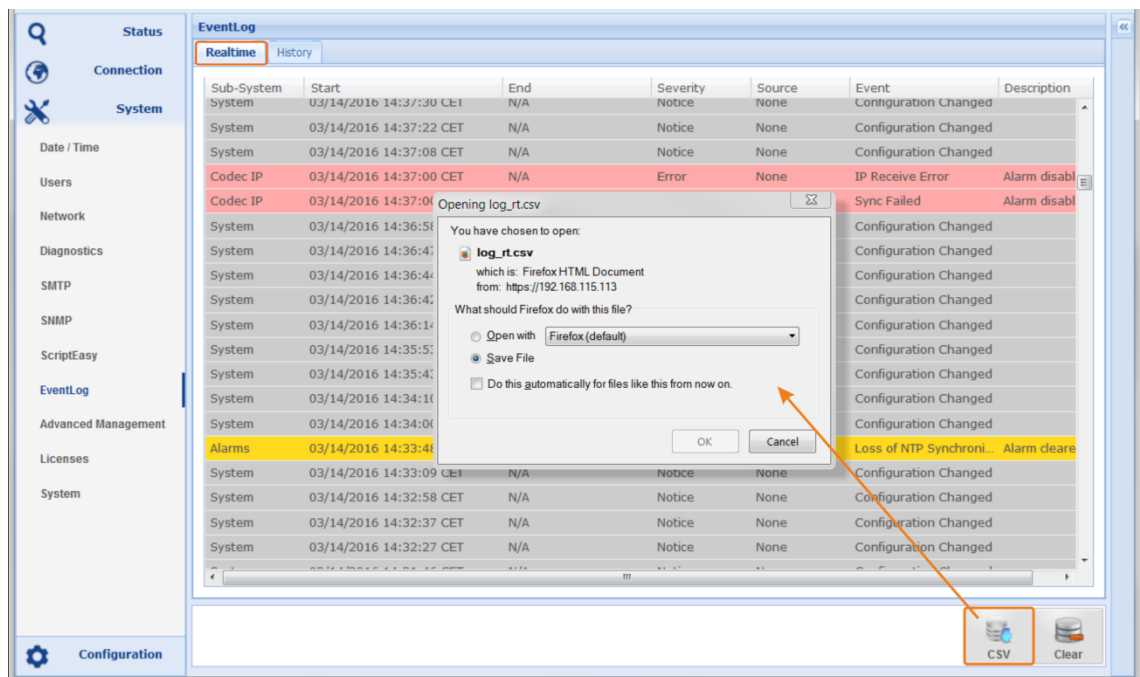


Figure 3-61: Shows the CSV formatted log file entries

### 3.5.8.2 Event Log History

Clicking on the “History” tab opens a page that allows searching for entries in a defined period. Opening this page, the first time will present an empty page. Clicking the “Search” button starts the retrieval process in accordance with the selected search options.

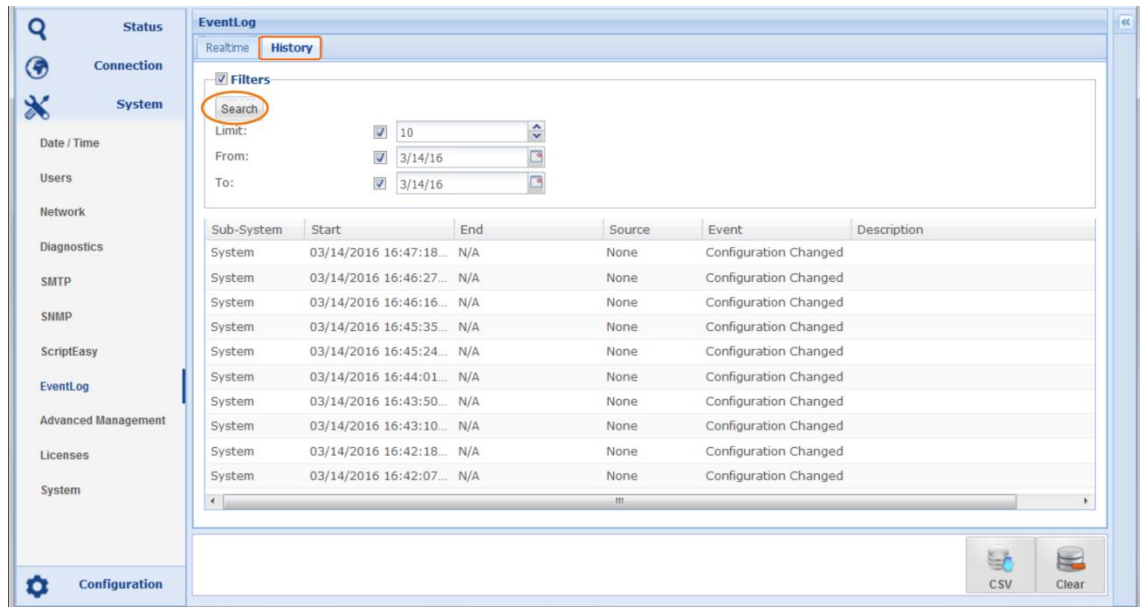


Figure 3-62: Shows the history retrieval options

The search options allow the definition of a period and the number of records that will be presented. All entries of the specified period will be listed but limited by the previously chosen number of records.


### 3.5.9 Advanced Management



This management page provides advanced system options on a single page.

#### 3.5.9.1 Backup/Restore Unit Configuration

Other than the SD card system backup, this option exports the unit configuration to offline storage like the hard drive of your PC. A backup consists of all unit parameters including ScriptEasy applications, user defined alarms and all parameters which may differ from the default values.

Different from other unit parameters, the network configuration is not automatically applied by restoring the backup file. You must re-apply the settings manually by clicking on the “Save” button on the network page.

 Without changing any value on the network page, the “Save” button is inactive. To activate the “Save” button, change temporarily any value (e.g., the ETH name).

-  Clicking on “Backup” opens the browser dialog for file storage
-  Clicking on “Restore” opens the file manager on your PC.

Navigate to the archive location and upload the .dat file to the unit and click on the backup file. A configuration file name consists of the unit’s serial number and date and time of creation, e.g. for IP Silver Encoder #I000123: backup-I000123-20170408-181525.dat.

**⚠** You can edit the file name only behind the Serial number part e.g., “backup-I000123-**My-IP-Silver-Encoder**.dat.” You must keep the word “backup and the serial number!

Confirming the restore action applies the backup file to the unit except the settings from the network page (main network configuration page).

The management system restarts, and the GUI prompts you to reconnect (it takes approx. 15 sec. before you can reconnect). If you need to apply the network settings from the backup file, open the network page and click on “Repair”. This will load the settings from the backup file to the current status; it overwrites your current IP addresses and requires a reconnect from the browser on the new address.

**⚠** Note, all other network related configurations are applied automatically (Advanced Network Configuration, Dynamic DNS, Virtual Interfaces, VLAN and Firewall).

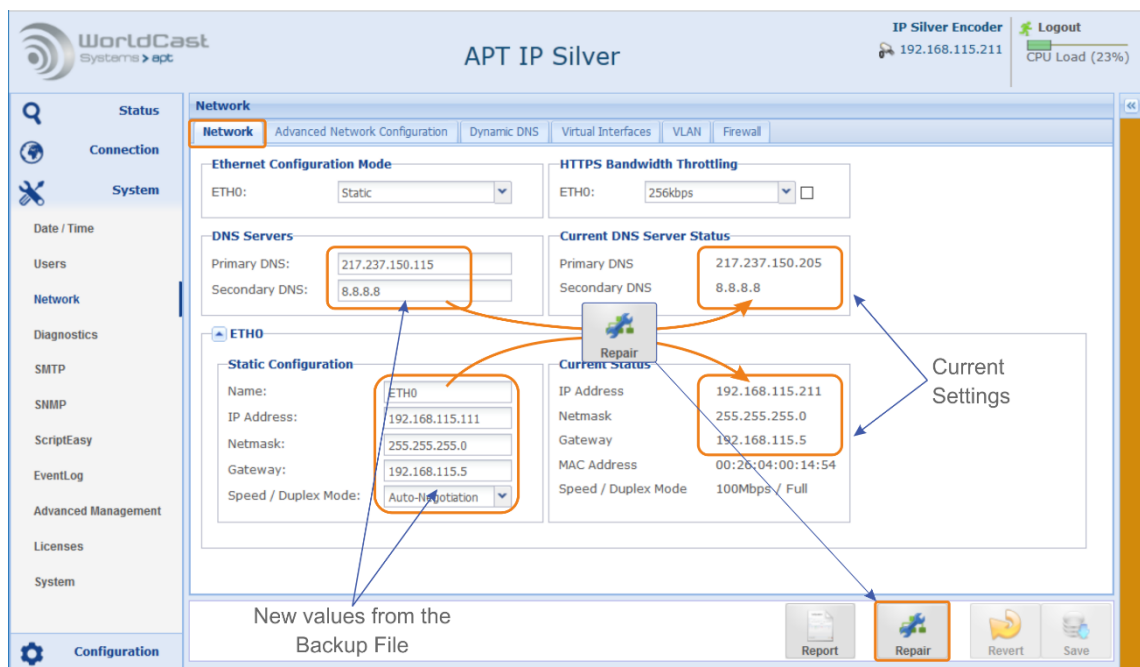


Figure 3-63 shows the network page after a backup file was loaded; network parameters are different from the current status. Clicking on “Repair” applies the network setting from the backup file.

### 3.5.9.2 Firmware Update

This section is the step-by-step instruction for performing a firmware update successfully. This is a straight forward procedure. The complete update procedure takes about 10 minutes. During this period, the unit MUST not be switched off! The GUI and the alarm LED on the front panel indicate the running procedure. During the firmware upload, the device is temporarily unavailable and disconnects from the web browser.

**i** *The firmware update does not affect previous user settings. A firmware update can be processed on the Admin Account only*

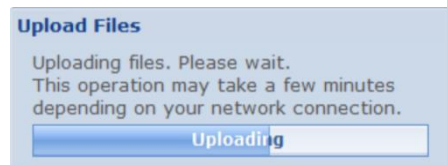
#### About – System Firmware

A Firmware release consists of a set of inter-compatible firmware files. These are system files for the DSP, the system operational system, and the WEB GUI. A system release will always be delivered as a Zip-Archive.

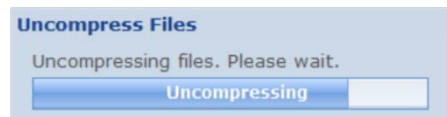
**⚠** You must never unzip the firmware zip-archive on your PC! The upload procedure requests this zipped archive.

Clicking on the “Update” button opens the PC file browser. Navigate to the folder where the firmware file is stored and select the zip-archive (SILVER-RCA-SR-2-2-0.zip). Confirm your selection and proceed with the firmware update.

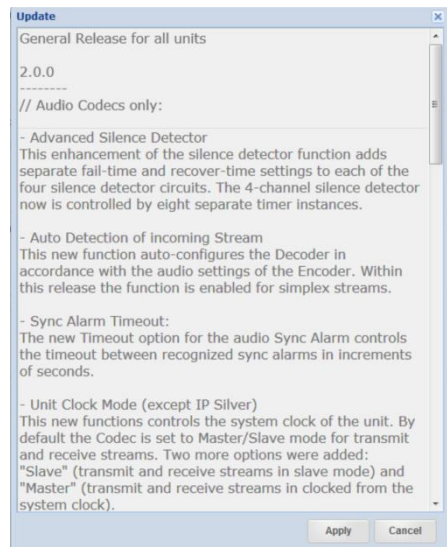
The progress bar indicated the status during the file upload.



After the file is successfully uploaded, the system starts uncompressing the archive.



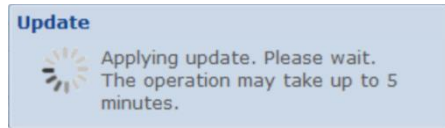
Once the firmware archive is successfully uncompressed and verified, the window with the release note appears. The release note contains the most important information about new features, bug-fixes and other changes in the new firmware.





## Firmware Update (*continued*)

Clicking on the “Apply” button continues the upgrade process. Applying the new firmware can take up to 5 minutes.



Once the update process is completed, the GUI prompts you to re-connect to the unit.

- ❗ *If the GUI does not respond for a longer time, press F5 to reload the GUI to the browser.*
- ❗ *The Firmware update process is a reliable procedure. Nevertheless, it is recommended to ensure that the power supply and the network connection are stable during the upgrade procedure to avoid undefined states.*

### 3.5.10 System Licenses

This page provides the Unit Details necessary for requesting optional licenses. Optional system licenses are SureStream and Digital MPXoIP transmission. Other licenses listed here are standard licenses.

- ➔ **Activation:** This license is applied as standard on purchased units. On demo units, this license may have an expiry date. If this license has expired, the unit cannot be used any longer.
- ➔ **ScriptEasy:** Since firmware 2.0 the ScriptEasy license is applied as a standard feature.
- ➔ **ScriptViewer:** License applied as standard with ScriptEasy (MasterView)
- ➔ **SureStream:** License applied as standard on the IP Silver units

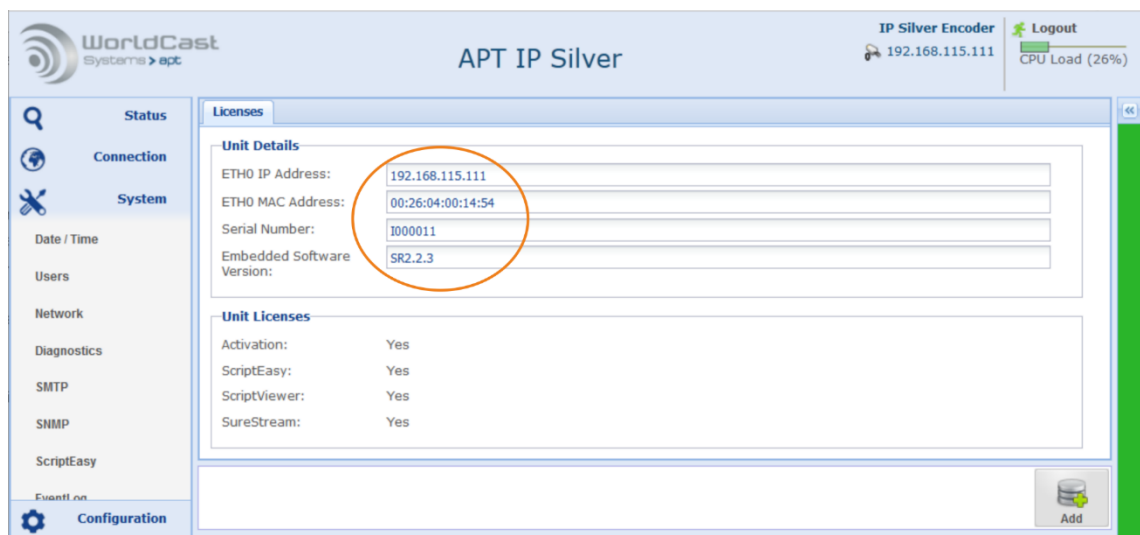


Figure 3-64: Shows the unit parameter for getting an options license

- ❗ *Currently, there are no more licenses available for the IP Silver units.*



## System Licenses (continued)

To request an optional system license, click on the link “Request an xxx license.” This opens your standard mail client with the support email address and unit details filled in. You will receive a quotation from your local APT sales office.

Once you have received your license key, click on the “Add” button to enter the license key. Once the key code is entered, click on “apply” to upload the key to the Codec hardware.

This license key is dedicated to the particular unit, and you cannot transfer it to any other unit. Once the license key has been applied, it cannot be removed and will not be overwritten by a firmware update.

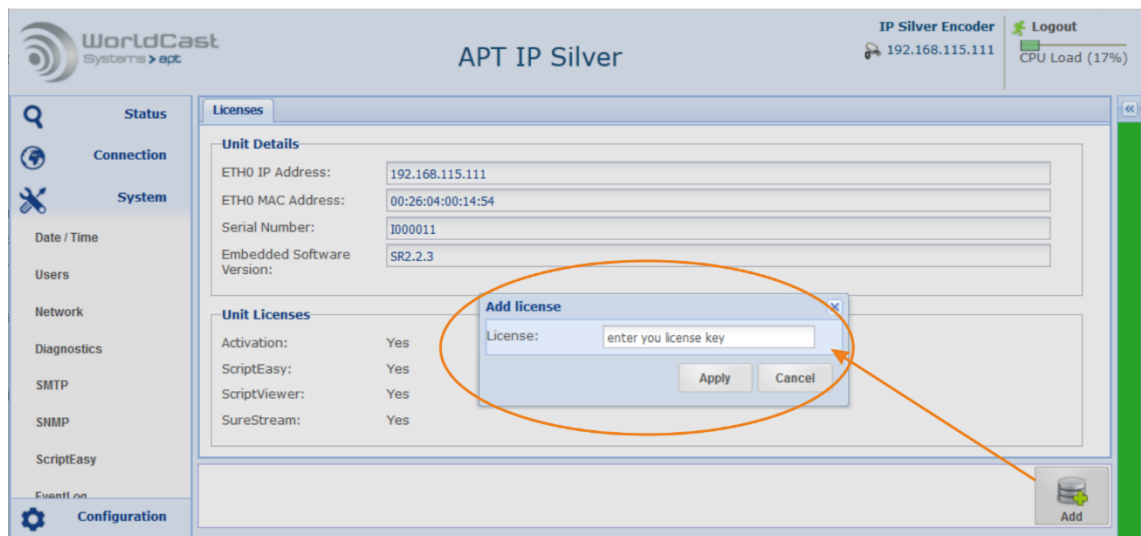


Figure 3-65: Shows how to apply a new license key to the system

### Notes:

---

---

---

---

---

---

---

---

---

---

### 3.5.11 System

This page displays the hardware and software version of the unit. It also provides system related configuration options.

#### **Unit Information**

- ➔ "Unit Name" allows entering an individual name for this unit. This name is displayed on the browser tab as well as on the unit's status page.
- ➔ "Contact" shows the support contact email address – this is a read-only display.
- ➔ "Location" allows entering a name or location description
- ➔ "SSL Certification Authority" provides the download of an SSL certificate for installing on your browser.

#### **System Information**

This section provides system information regarding software versions and already applied licenses.

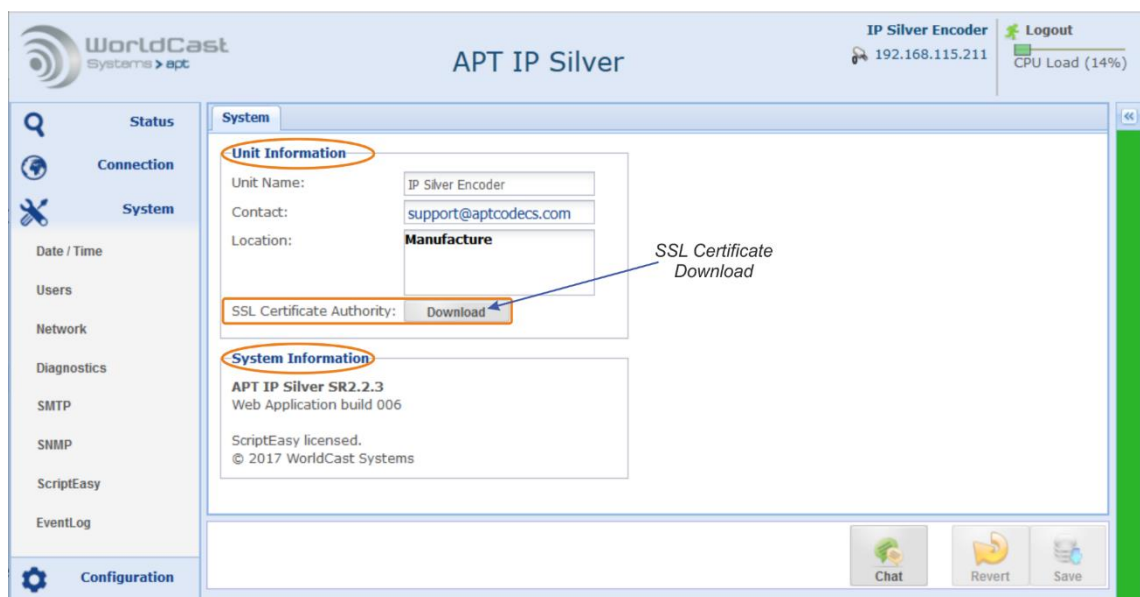


Figure 3-66: Shows the "System" page of the System menu

#### 3.5.11.1 SSL Certificate Authority

Download the SSL certificate as shown in Figure 3-66 and store it on your computer. You must install the certificate "ca\_WSC.crt" on your browser following the instructions of your browser brand. The certificate is an SSL Authority Certificate and must be imported in "Certificate Authorities". It appears as WorldCast Systems certificate.

You must install it only once; it is valid for all WorldCast Systems devices connected to this browser. Each browser needs its own copy of the "ca\_WCS.crt" file.

### 3.5.11.2 Chat Box

The System page also provides a little chat box which allows sending short messages to other logged in users. The "Screen Name" field on the user LogIn defines the name of the user that appears in the chat box.

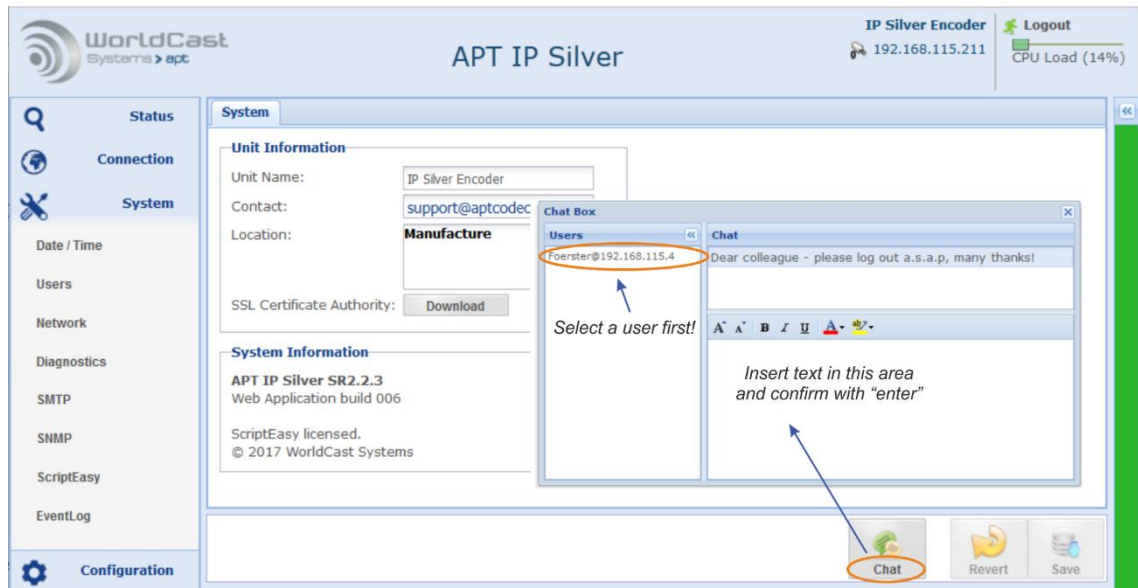


Figure 3-67: shows the "System" page of the System menu with Chat Box open

The chat box shows all currently logged in users regardless of the user status (Admin or Guest). You can send messages to any user by selecting the user and typing a text in the text area. Confirming with "Enter" sends the message.

On the receiving end, the chat box window displays the text message and the source where this message was sent from (see next page).

The chat box uses UDP datagrams for sending these messages.

**i** The username which appears on the chat box is the "Screen Name" entered in the logIn window.

### Chat Box (continued)

If a message is received, the chat box pops up on the GUI page that is currently open.

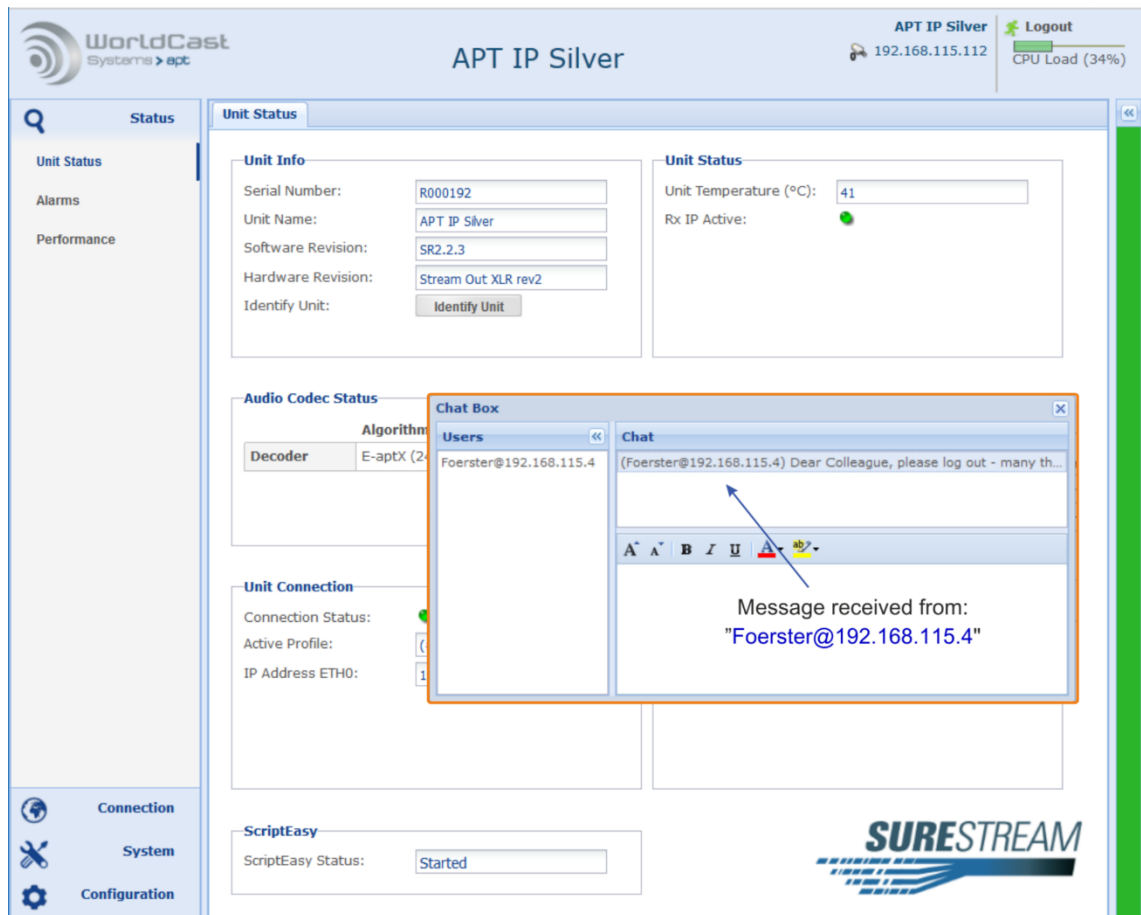


Figure 3-68: The chat box pops up when a message is received

### 3.6 Main Menu – Configuration

The configuration menu provides four submenu items:

- ➔ the Audio Configuration
- ➔ the Network Alarms
- ➔ the AUX Data page
- ➔ the Alarm Configuration

These are basic configurations controlling operational modes and system behaviors

#### 3.6.1 Audio Configurations

##### IP Silver Encoder

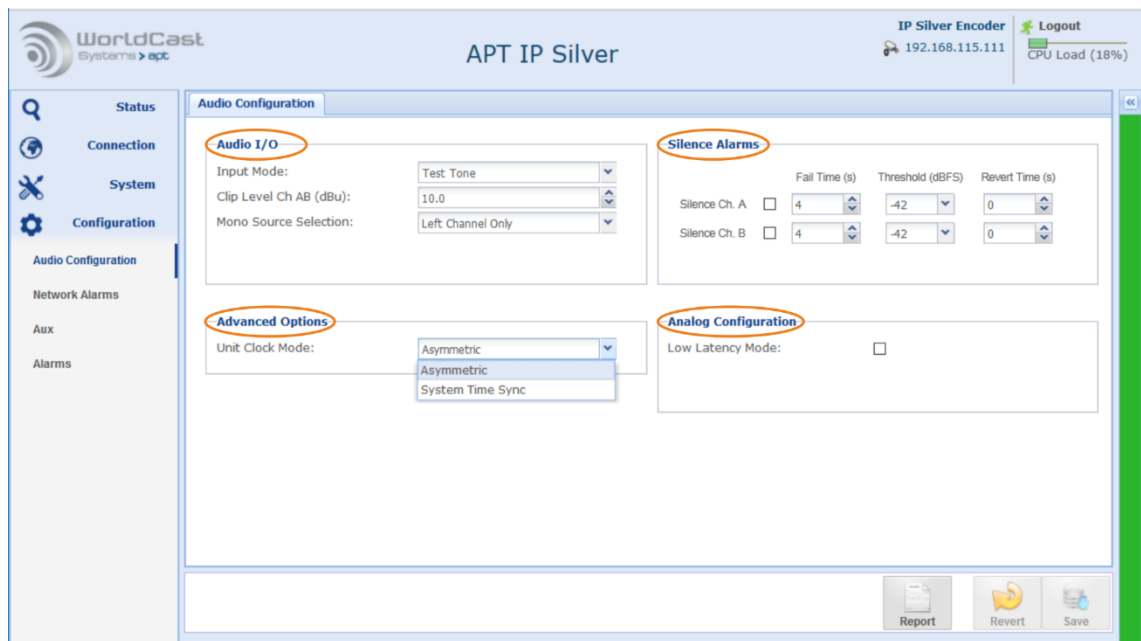


Figure 3-69: Shows the Audio Configuration page in the Encoder (RCA version)

The screenshot above shows the audio configuration page of a IP Silver Encoder with RCA connectors. The XLR version allows changing the Input or Output impedance in addition.

Table 1 outlines the configuration options on both versions.

#### Notes:

---



---



---



---



---

## IP Silver - Decoder

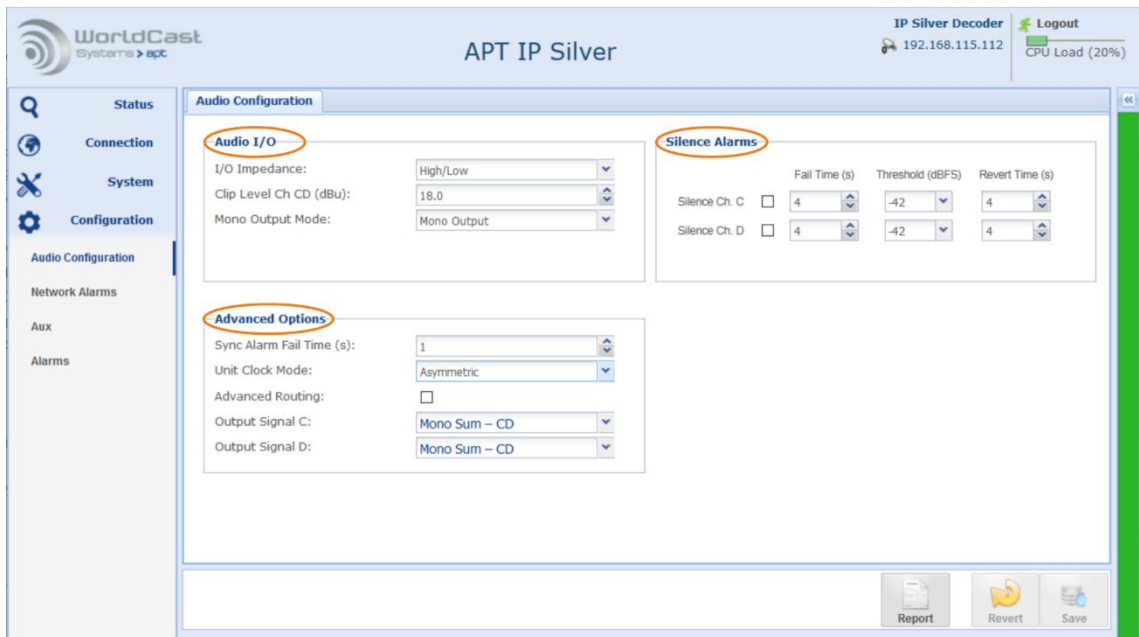


Figure 3-70: Shows the Audio Configuration page in the Decoder (Decoder XLR version)

The screenshot above shows the audio configuration page of a IP Silver Decoder with XLR connectors.

Table 1 outlines the configuration options on both versions.

### Notes:

---



---



---



---



---

### 3.6.1.1 Audio Configuration Options

- ➔ This section provides the audio configuration option of the Encoder and the Decoder. Audio Inputs/Outputs
- ➔ Silence Detection

Configuration	Options	Description
<b>Input Mode</b> Encoder	Analog Test Tone	Analog Inputs The internal test tone generator provides a 1 kHz signal for test purposes.
<b>Input Clip Level (AB)</b> RCA version	Values 0-10 dBu	Adjusts the analog Input level referenced to the digital dBFS in increments of 0.1 dB
<b>Output Clip Level (CD)</b> RCA version	Values 0-10 dBu	Adjusts the analog Output level referenced to the digital dBFS in increments of 0.1 dB
<b>Input Clip Level (AB)</b> XLR version	Values 0-24 dBu	Adjusts the analog Input level referenced to the digital dBFS in increments of 0.1 dB
<b>Output Clip Level (CD)</b> XLR version	Values 0-24 dBu	Adjusts the analog Output level referenced to the digital dBFS in increments of 0.1 dB
<b>Input Impedance</b> Encoder RCA Encoder XLR	High High/600 Ω	> 10 kΩ > 10 kΩ / 600 Ω selectable
<b>Output Impedance</b> Decoder RCA Decoder XLR	Low Low/600 Ω	RCA: <50 Ω <50 Ω / 600 Ω selectable
<b>Mono Source</b> Encoder	Left Channel only  Mono Sum ((L+R)/2)	This describes the signal source (input) for a mono audio algorithm.  This selection takes both signals (left & right) and divides it by 2 (-3 dB)
<b>Mono Output Mode</b> Decoder	Mono Output MonoFill <sup>1)</sup>	Output on left channel only MonoFill copies the signal also to the idle channel; mono output on L & R connectors
<b>Silence Alarms</b> Encoder A & B Decoder C & D	Enable/Disable Fail Time Threshold Level Revert Time (s)	Ticking the boxes enable Silence alarms Time until the alarm is activated Level setting from -3 dBFS to -42 dBFS Time until the alarm is deactivated

Table 1: Shows the Audio Configuration options of the Encoder and Decoder

<sup>1)</sup> MonoFill cannot be used together with the advanced routing option as the two features stay in a conflict.

## Analog Configuration (*continued*)

### 3.6.1.2 Analog I/O Clip Levels (XLR)

These settings allow adjusting the analog levels in reference to the digital level:


All level readings are internally referenced to the digital domain where 0 dBFS=24 dBu. For example, if the analog level of +6 dBu shall internally equal -9 dBFS then the analog **clip** level must be set to +15 dBu (0 dBFS =15 dBu hence -9 dBFS=+6 dBu).

### 3.6.1.3 Low Latency Mode

This “Low Latency Mode” effects the **analog** signal processing and improves the system latency by approx. -1.5 ms. This mode disables and bypasses the **input** Sample Rate Converter which is obsolete in these modes (Encoder only):

- Linear PCM at  $F_s = 48$  kHz (any linear PCM mode that uses 48 kHz Sample Frequency)
- Eapt-X<sup>®</sup> at  $F_s = 48$  kHz (any Eapt-X<sup>®</sup> mode that uses 48 kHz Sample Frequency)

Configuration	Options	Description
Low Latency Mode	Enable/Disable	Ticking this box enables the low latency mode

 **Note:** This latency improvement takes place on audio formats (as listed above) that run at 48 kHz sampling frequency. Whenever another mode is selected, e.g. Linear PCM with up to 15 kHz frequency response (equals  $F_s = 32$ kHz) then this mode is automatically deactivated regardless of the enable/disable status on this configuration page. If this mode is enabled it automatically takes place if an audio mode at 48 kHz is selected.

### 3.6.1.4 Encoder and Decoder Mono Modes

#### **Encoder**

The Encoder mono setting takes effect only if a mono algorithm is selected. The mono setting is ignored if a stereo algorithm is selected.

Encoder Source Selection:

- ➔ Left channel only
- ➔ Mono Sum  $((L+R)/2)$

#### **Decoder**

The Decoder mono setting takes effect only if a mono algorithm is chosen (mono stream). The mono setting is ignored if a stereo algorithm is selected.

- ➔ Mono Output (mono signal on left channel)
- ➔ Monofill (mono signal copy to Idle Channel)



## 3.6.2 Advanced Options

### 3.6.2.1 Sync. Alarm Fail Time (Decoder only)

The Sync. Alarm Fail Time defines the duration during which an audio Sync.-Alarm must exist before an alarm is raised. This setting can avoid a high number of flagged synchronization alarms in a short period of time. The system does not flag sync. alarms shorter than the here defined fail time.

### 3.6.2.2 Unit Clock Mode

➔ **Asymmetric:**

Asymmetrical clocking guarantees a flawless anywhere-to-anywhere streaming. In this mode, the Encoder is clocked from an internal while the receiving Decoder derives the system clock from the packet interval utilizing its VCXO. Asymmetrical clocking avoids buffer underrun and overflow events.

➔ **System Time Sync:**

This mode derives the audio IP clock from the system time. You can choose the source of the system time sync mechanism. Units using this mechanism should have NTP enabled as the system time source (refer to section Dates and Time 3.5.1). If NTP is not enabled this mode equals the Master Mode.

❗ *You can use "System Time Sync" together with the NTP system time source to adjust the overall link latency. This application is described in section 3.6.3.*

#### Notes:

---

---

---

---

---

---

---

### 3.6.2.3 Advanced Routing (Decoder only)

The decoder options are extended by two features combined in this section:

- ➔ Creation of Mono signals from incoming stereo IP streams
- ➔ Advanced Routing of the output signal

#### Advanced Routing & Mono Sum

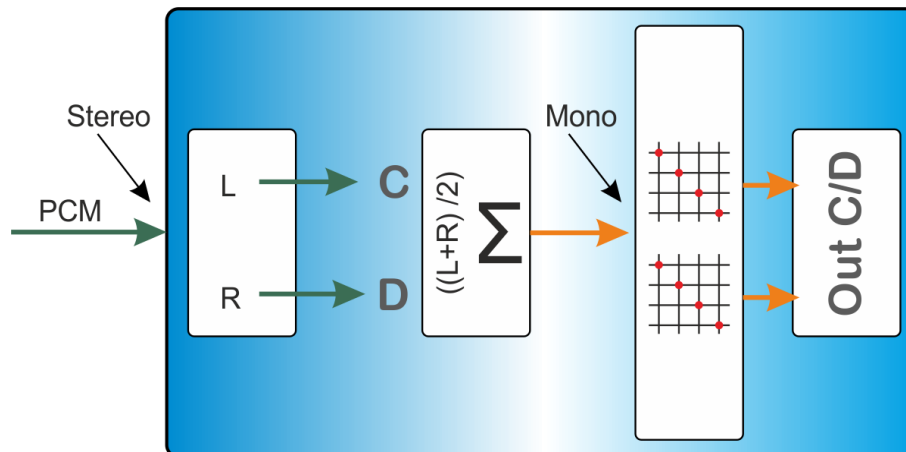


Figure: 3-71: Shows the principle of this feature of the Decoder

#### Decoder Mono Mode

This feature allows to create a mono signal (mono sum) from an incoming stereo stream. The mono sum is performed in the Decoder section and does not affect the stereo IP stream. Other than the mono sum option on the Encoder, the mono sum on the Decoder is algorithm agnostic. In a distribution network, the same stereo program can be decoded as stereo feed for e.g. FM supply and as a mono feed for an AM supply – the mono/stereo signal is generated from the same stereo stream.

#### Advanced Routing

This feature allows the routing of the decoded PCM signal from the DSP output to the physical output connectors on the rear panel of the Codec or Decoder. By default, and if the advanced routing feature is disabled, the signals are routed 1:1. For more details refer to the section below.

#### Advanced Routing & Decoder Mono Mode

- ➔ Advanced Routing must be enabled by the check box "Advanced Routing" and clicking on "Save" at the bottom of the page.
- ➔ "Output Signal C" and "Output Signal D" describe the physical outputs on the rear of the codec. The drop-down list shows the available signals:
- ➔ "Mono Sum – CD" this is the mono sum from the equation  $((C+D)/2)$ .
- ➔ Signal "C" and "D" represent the signals L/R from the received stereo stream.
- ➔ The advanced routing and mono mode feature offer the mono sum signal on both outputs C and D. This takes effect on the digital and the analog outputs.

### 3.6.3 Program Time Alignment

If you set your system time to NTP time (section 3.5.1) and select the "System Time Sync" clock mode (section 3.6.2.2), you can adjust the latency of an IP path with the size of the de jitter buffer relatively precisely. With this setting, the buffer clock is derived from the NTP time clock.

Setting the encoder in the same way achieves a latency stability of approximately 10 milliseconds. This latency stability is the same for all buffer sizes. The determining factor for the clock stability is the NTP protocol.

This application allows the use of different NTP servers without significant time shifts; i.e., the encoder may refer to the clock from a different time server than the decoder.

The precision of the NTP protocol allows a quasi-synchronization of the decoders, which is more than sufficient for the program synchronization. However, NTP is not suitable for frequency synchronization (SFN). The following graphic illustrates the principle of the application.

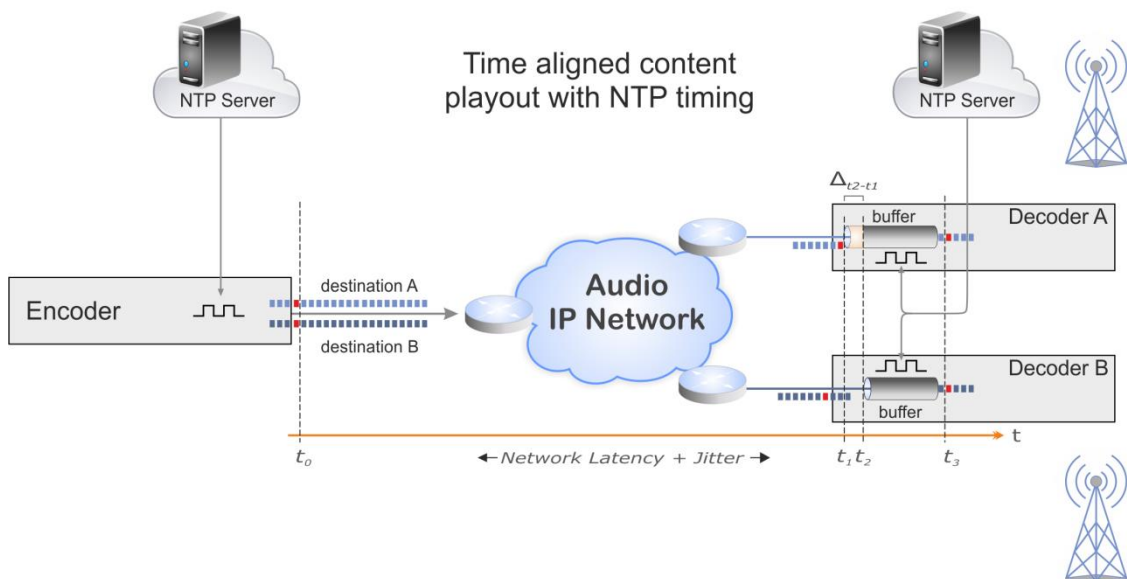


Figure 3-72 shows the principle of time aligned content payout

**Notes:**

---



---



---



---



---



---



---

### 3.6.4 Network Alarms

This page provides the alarm options of the Ethernet interface, Dynamic DNS and the “Loss of IP Connection”.

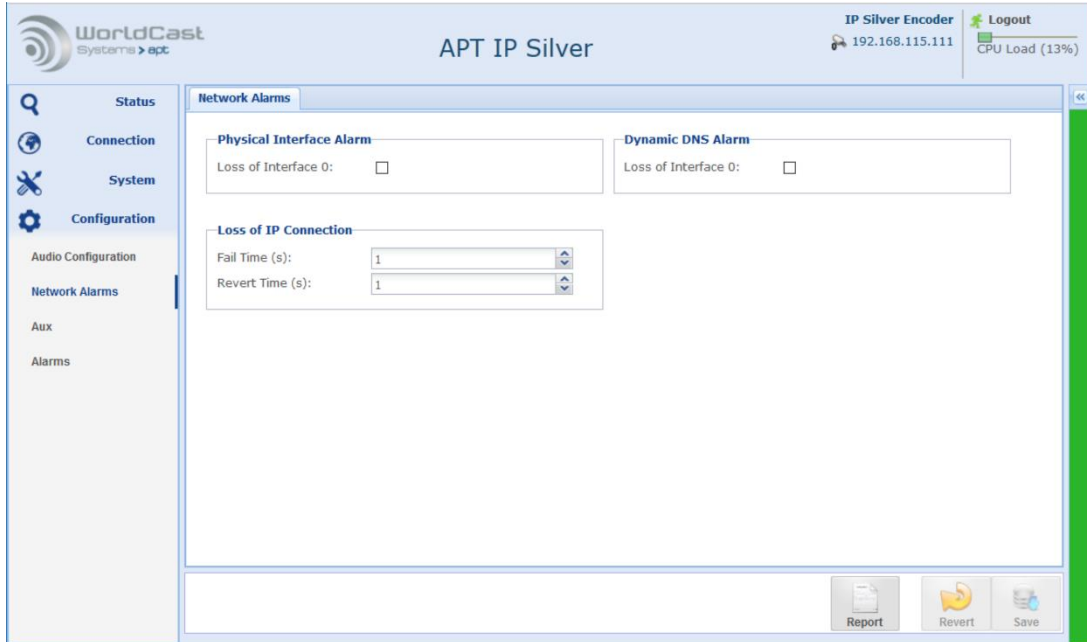


Figure 3-73: Alarm configuration options of Ethernet ports

#### **Physical Interface Alarm**

If this alarm disabled, a physical loss of connection will not be recognized as alarm at all.

#### **Dynamic DNS Alarm**

If this alarm is disabled, a loss of connection to the dynamic DNS service will not be recognized as alarm at all; this option is disabled on default.

#### **Loss of IP Connection**

A Loss of IP Connection describes a logical disconnection. This event occurs if the de-Jitter buffer ran empty. If this alarm is disabled, this alarm will not be recognized.

Notes:

---



---



---



---



---



---



---

### 3.6.5 AUX Data Configuration

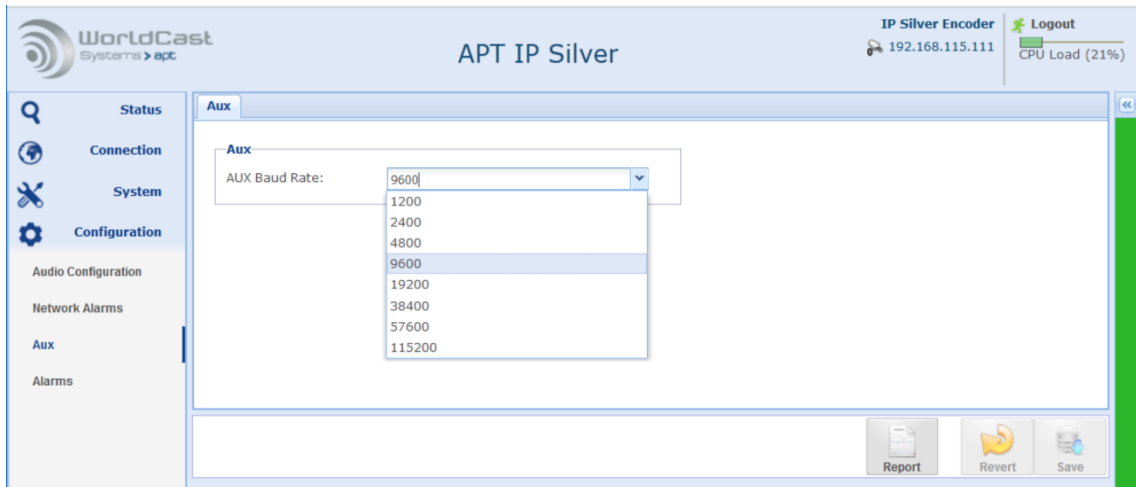


Figure 3-74: Shows the AUX Data configuration

Configuration	Options	Description
AUX Data Baud Rate Encoder and Decoder	Baud Rate	The drop-down list provides baud rate setting from 1.200 to max. 115.200 Baud.  The embedded mode supports up to 9600 Baud (algorithms and audio modes may limit capacity to a lower rate).

The data transmission of the AUX data can be configured in duplex. Both devices, the Encoder and the Decoder provide send and receive options.

**i** *The duplex function is only applicable if the AUX data is configured as a separate UDP stream. In embedded mode, the data is embedded in the simplex audio stream.*

**Notes:**

---



---



---



---



---



---



---

### 3.6.6 Alarms Configuration

The alarm configuration page presents all available alarms and provides options to control the alarm behavior. All system alarms are individually configurable.

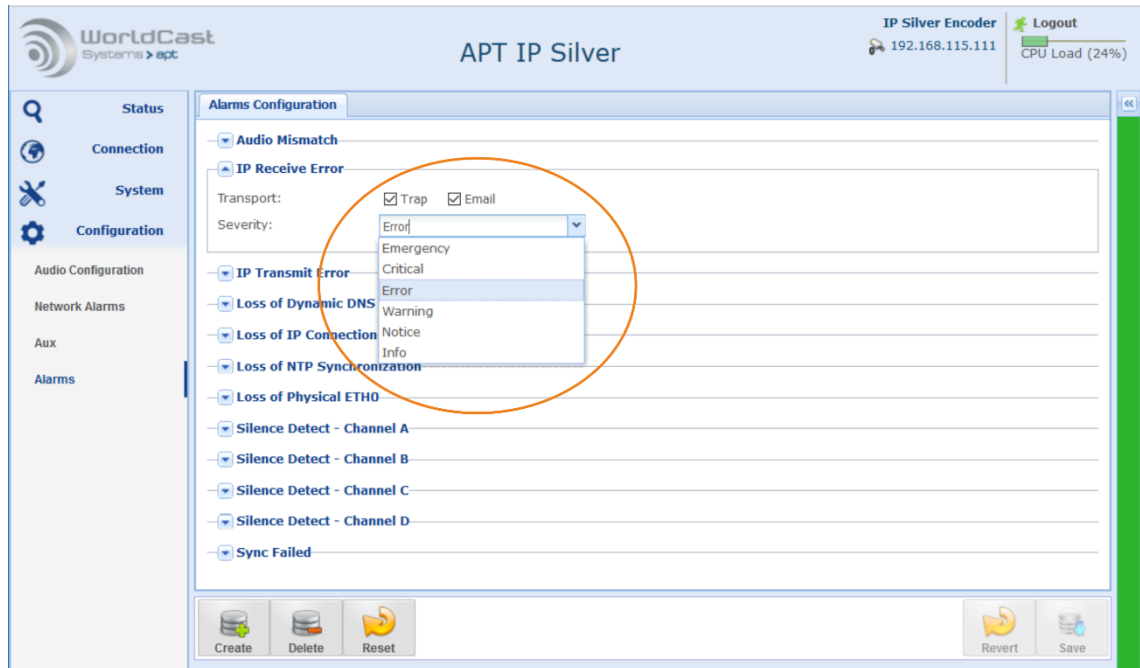


Figure 3-75: Shows the Alarms Configuration page

All system alarms are listed here. Clicking on the little arrow beside each alarm opens the configuration options. These options are:

#### **Sending an SNMP trap**

If this check box is enabled, this alarm sends a trap to the SNMP manager. The trap management is described in section 3.5.6 (SNMP).

#### **Sending an email alert**

If this check box is enabled, this alarm sends an email alert. Setup of the email service is described in section 3.5.5 (SMTP).

#### **Severity**

This drop-down list presents the severity levels. The alarms will be treated at all instances in accordance with these settings.

### 3.6.7 Customer Alarms

Creating an individual alarm allows building one or more groups of individual alarms where each group is considered as a single alarm. The group flags an active alarm if one or more alarms in the group become active (OR linkage). The advantage of this option is that a group of alarms (created here) can be assigned to a single relay and/or send via email.

#### How to Create a Custom Alarm

The alarm configuration page offers the option for creating and managing customized alarm groups. The figure below shows an example of “My Alarm”.

- ➔ Clicking on the “Create” button prompts you to enter a name for the alarm group (My Alarm). After applying the name, this setting must be saved first before the group can be configured.

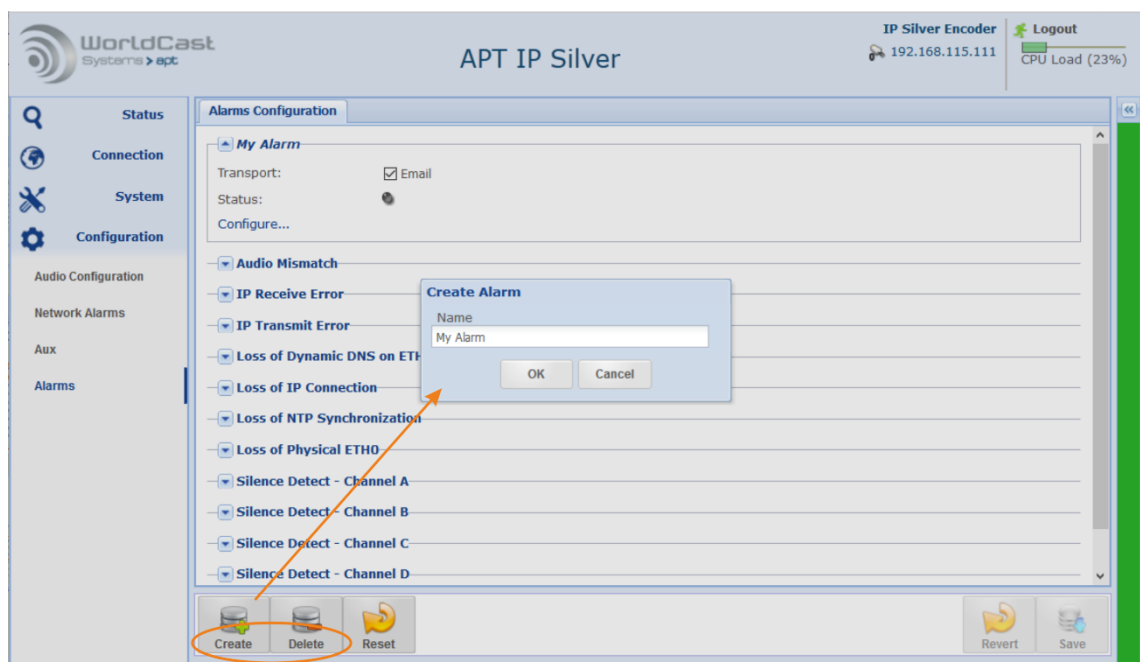


Figure 3-76: Shows how to create an alarm group

- ➔ After saving the “My Alarms” group, this alarm appears on the top of the list of alarms. As many groups as required can be created.

The tools for creating and deleting an alarm group are provided on the Tool Bar on the bottom of the page.

- ➔ Create: Create a new Alarm Group
- ➔ Delete: Delete the selected Custom Alarm
- ➔ Reset: Clicking on this button deletes ALL your custom alarms and all configurations you have changed on this page. All alarms will be reset to default states.

### 3.6.7.1 How to Create a Custom Alarm (*continued*)

- ➔ Once the new alarm is created, you must configure the group.
- ➔ Clicking on the little arrow opens the full alarm options and the “Configure...” link.
- ➔ Clicking on this link opens the Alarm configuration window. This window presents all available alarms on the left-hand side. Alarms can be added to the group on the right-hand side by selecting the desired alarms and clicking on the “Add” button.

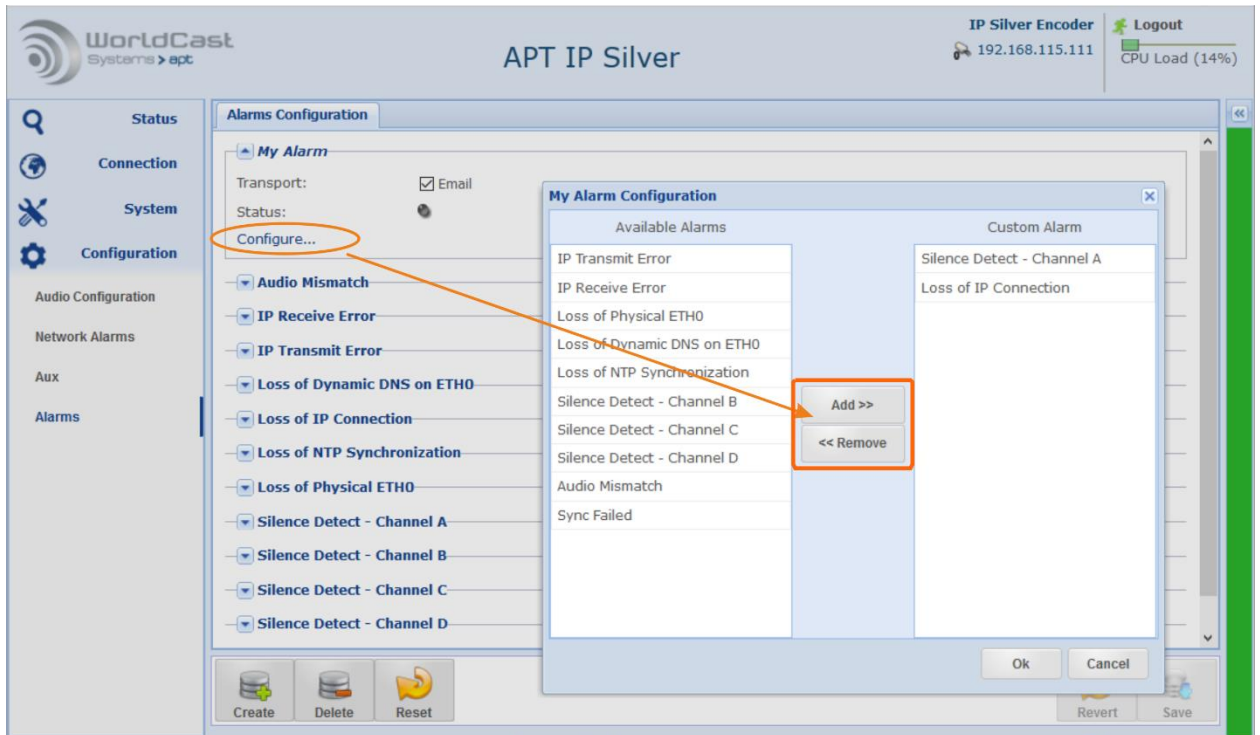


Figure 3-84: Shows how to create an alarm group

- ➔ Once this alarm group is created, the email alert can be enabled. This new alarm group is treated as a single alarm.

#### Notes:

---



---



---



---



---



---



---



## 4.0 SureStream

SureStream Technology is a standard feature of the Silver IP Streamer range and indicated by the SureStream Logo on the Status page.

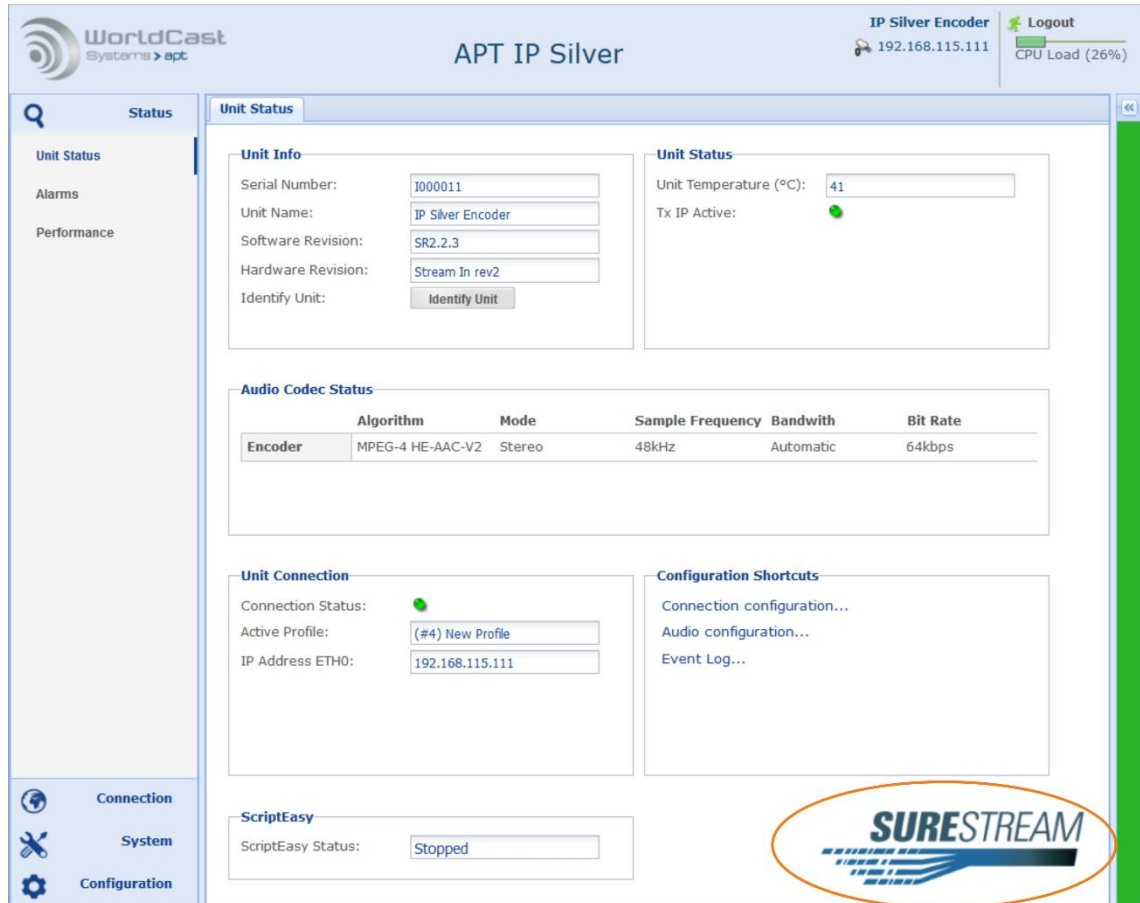


Figure 4-1: Shows the Status Page with SureStream enabled

### 4.1 About SureStream

SureStream technology is a revolutionary innovation from APT that enables broadcasters to use inexpensive IP links and still maintains professional broadcast-grade audio quality and reliability. It delivers the sound quality and reliability known from a synchronized TDM based link at a fraction of the associated cost.

The technology approach of SureStream relies on redundant streaming. SureStream replicates a single program audio stream and passes it through the Statistical Diversity Generator. Following this process, the redundant program streams appear on the network as separate streams generated from different or the same source (depending on the IP interface the stream is transmitted from).

In practice, redundant streams will be created on both ports. Nevertheless, this feature works on a single physical port as well, but with the limitation that a "Loss of Connection" cannot be covered by a single network access.

## About SureStream (continued)

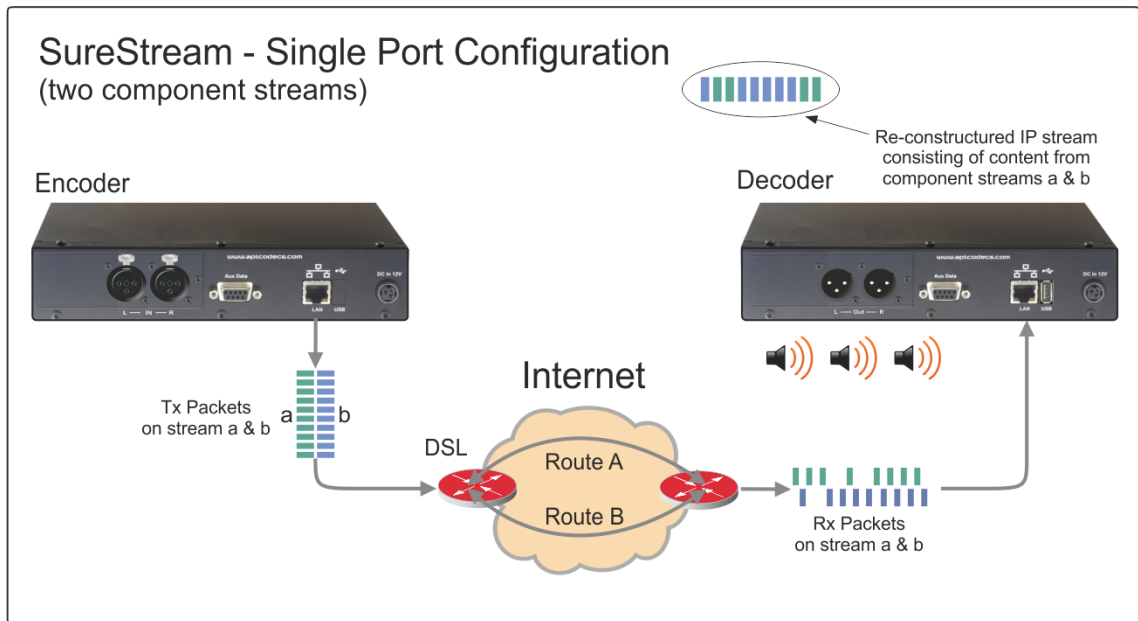


Figure 4-2: Shows a typical configuration running SureStream on a single IP port

The configuration example above shows a typical SureStream configuration using two SureStream component streams. This example uses the Internet with standard xDSL access services. Diverse streaming on the internet has the effect, that the access routers treat each SureStream component stream individually by passing it randomly on different paths to the destination IP address.

On the receiving end, the Enhanced Re-Sequencer generates from all component streams the single packet stream on a first-in-first-out packet basis. All duplicated/redundant packets will be dropped. The number of component streams is not limited by the SureStream technology.

SureStream is a powerful algorithm that protects an IP link against packet losses and Loss of Connection errors. The latter protection can be achieved only if the Codec device uses dual IP ports for streaming out the component streams.

- ❗ *On a single IP port device, like the IP Silver Encoder and Decoder, SureStream cannot protect the IP link against physical Loss of Connection errors.*

## About SureStream (continued)

The IP Silver units support virtual IP interfaces with and without VLAN tagging. You can extend the number of physical ports by an external (VLAN aware) switch.

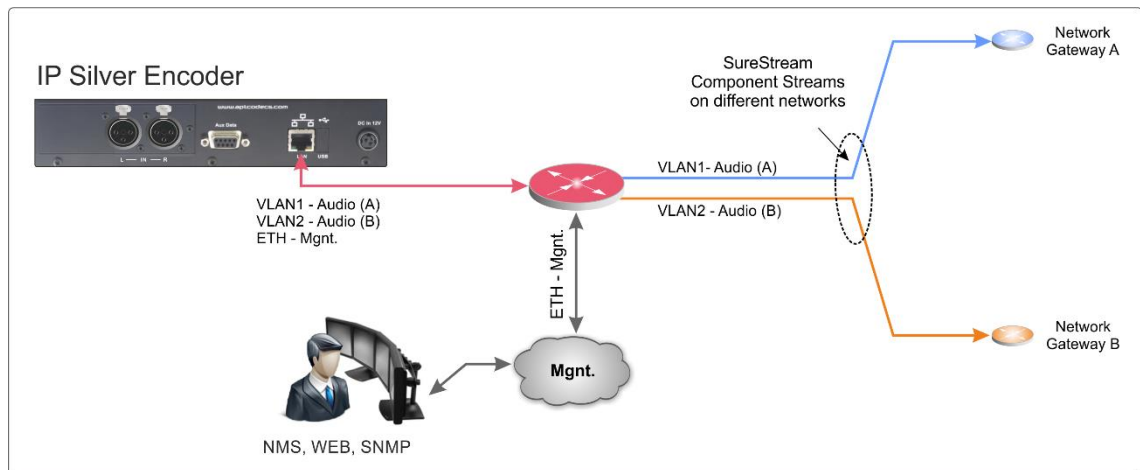


Figure 4-3: SureStream via two networks separated by VLAN tags.

### 4.1.1 SureStream Encoder

On the Encoder side, the heart of SureStream is the Statistical Diversity Generator. This generator ensures that the component streams appear on the network as diverse as possible. This generator runs an algorithm that can be set up with three different sets of parameters (called "levels") allowing the use of more than one component stream while keeping each stream divers from each other.

### 4.1.2 SureStream Decoder

Once SureStream has generated duplicated streams with the same payload intended to reach the same receiver, the Decoder on the receiving end must cope with a massive number of redundant packets arriving from a single or different network. Allowing the Decoder to cope with duplicated packets it must run the complementary algorithm as on the Encoder side; this is the Enhanced Packet Re-Sequencer Engine.

#### Notes:

---



---



---



---



---



---



---

## 4.2 SureStream – Encoder Configuration

Creating a SureStream component stream follows the same procedure as a normal stream configuration. A component stream will be automatically identified as part of a SureStream group by the same data source. A data source is defined by the stream type (audio, AUX, or forwarding).

The screen shot below shows a SureStream group from the Encoder site. The packet size within a SureStream group of streams must be the same for all streams. Therefore, the packet size configuration of the streams in a group is linked together. If you change the packet size on one stream, all the other streams follow automatically.

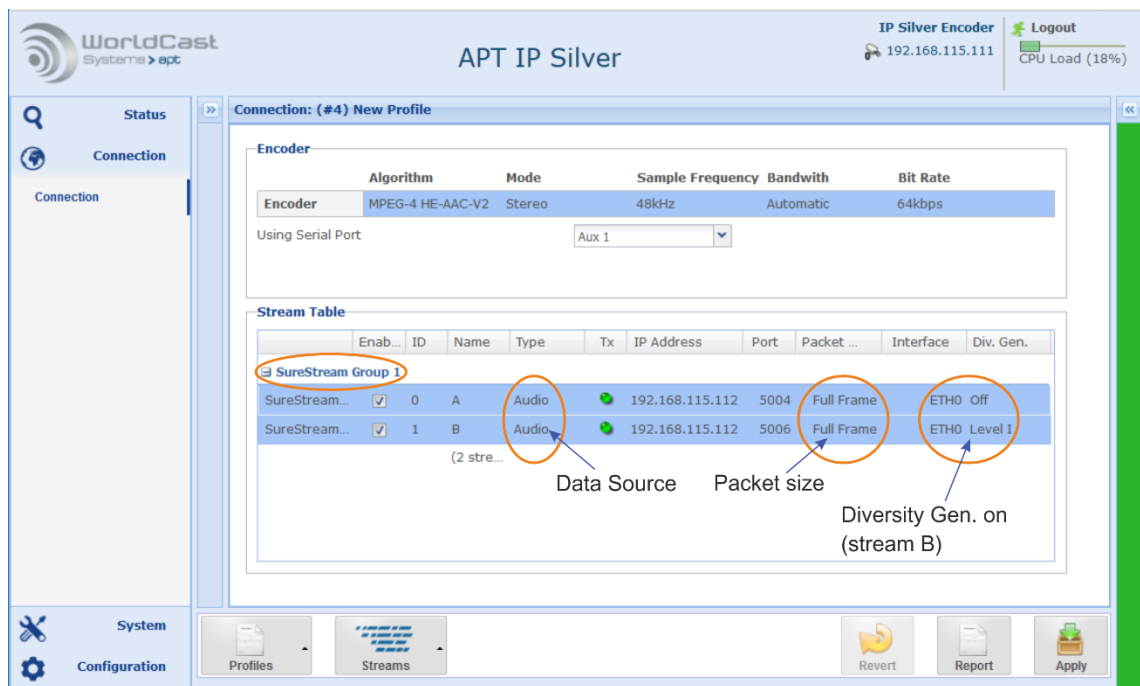


Figure 4-4: Shows a SureStream configuration on the Encoder

**ⓘ** A SureStream group (i.e. SureStream 1) will be displayed only if the packet sizes on ALL component streams are equal!

The figure above shows a working Encoder configuration with two streams are assigned to the same destination IP address, hence they are received on a single port at the Decoder. This implies that both streams are sent through the same ETH port on the Encoder into a single network. – In a real-world application, this configuration will protect the IP link against packet losses very efficiently as explained above.

The next section outlines the recommended and mandatory settings for a group of component streams.

**ⓘ** It is recommended to enable the Diversity Generator in this configuration to achieve a sufficient diversity.

## SureStream – Encoder Configuration (*continued*)

The diversity generator has been activated for one of the two component streams to increase the network diversity. For the transmission over only one network, the use of the diversity generator is recommended.

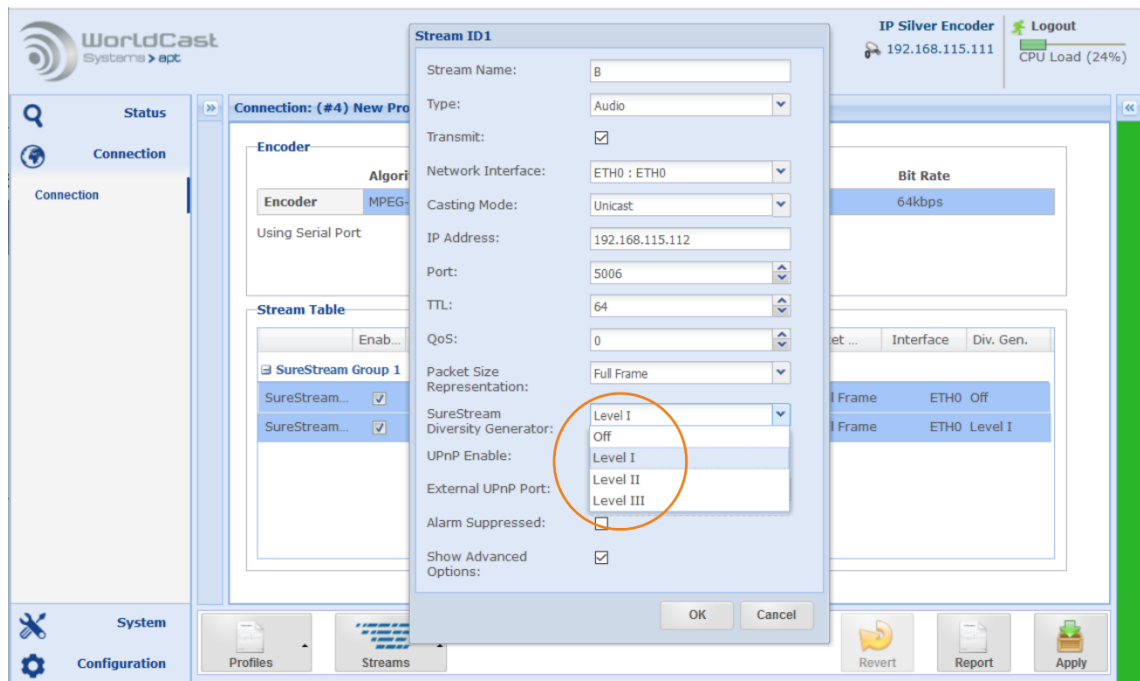


Figure 4-5: Shows the Diversity Generator options on the stream configuration window

### 4.2.1 About Diversity Generator Levels

The SureStream Diversity Generator can be either disabled or set from “Level I” to “Level III”. A “Level” does not indicate the degree of severity of SureStream. A “Level” is a set of parameters used by the Diversity Generator to ensure the stream diversity. All three “Levels” work on the same degree of severity but differently from each other.

Having three sets of parameters allows for configuring more than one redundant stream and keeping all streams processed individually by the Diversity Generator. It has sometimes been seen that a particular “Level” delivers better results than another.

Therefore, it is worthwhile to trying out what Level delivers the best results in a specific network environment.

- ❗ *Whenever a set of SureStream component streams are created for a single network, one of them should have the Diversity Generator Level set to off. All other component streams should run on a different level (I-III).*

#### 4.2.2 Creating a Set of Component Streams

A set of component streams processed by the Diversity Generator is not limited to a particular number of streams. In practice, a set of two component streams work reliably. However, the system allows for creating more than one redundant stream on both ETH ports.

Field (SureStream)	Description
Stream Name	A name must be given – there are no constraints applying a name
Stream Type	SureStream supports "Audio" streams only (RTP)
Transmit Mode	SureStream supports "Transmit" mode
Receive Mode	SureStream supports "Receive" mode
Mode	SureStream supports "Unicast and Multicast"
Destination IP Address	This can be the same for all streams, but SureStream works more efficient if more than one ETH port is used (physical and virtual), hence the destination IP address can be different. In a single ETH port configuration, the target IP address is the same on all component streams.
IP Port	For each stream - the IP port <b>must be different</b>
TTL	For all streams - the TTL value <b>must be equal</b>
QoS	For all streams - the QoS setting <b>must be equal</b>
Packet Size	For all streams - the Packet Size <b>must be equal</b> (linked)
Rx Latency	The buffer size of the component streams is linked together in a SureStream group. If you change the latency on one stream, the other streams follow automatically. The latency must be the same for all streams.
SureStream Diversity Generator	The three sets of parameters are different and allow the Diversity Generator to create a variety of different component streams if more than one component stream is configured on the same Ethernet interface.

### 4.3 SureStream – Decoder Configuration

Configuring the Decoder for using SureStream follows the standard procedure creating as many as necessary receive streams (component streams).

A SureStream group will be set up from streams with the same data endpoint. A data endpoint is indirectly defined by the stream type, e.g. an "Audio" stream. An audio stream is always decoded while the data of the stream type "Media Forward receive" is never decoded but can be forwarded to another data endpoint.

It is important that the buffer size (Rx Latency) is the same on all streams in a SureStream group. In the same way as the packet size at the Encoder settings, the buffer setting is linked through all streams in a group. Changing the size on one stream will copy this change to all other streams.

On the Decoder, the recombiner, and the resequencer are the complementary parts of the stream diversity.

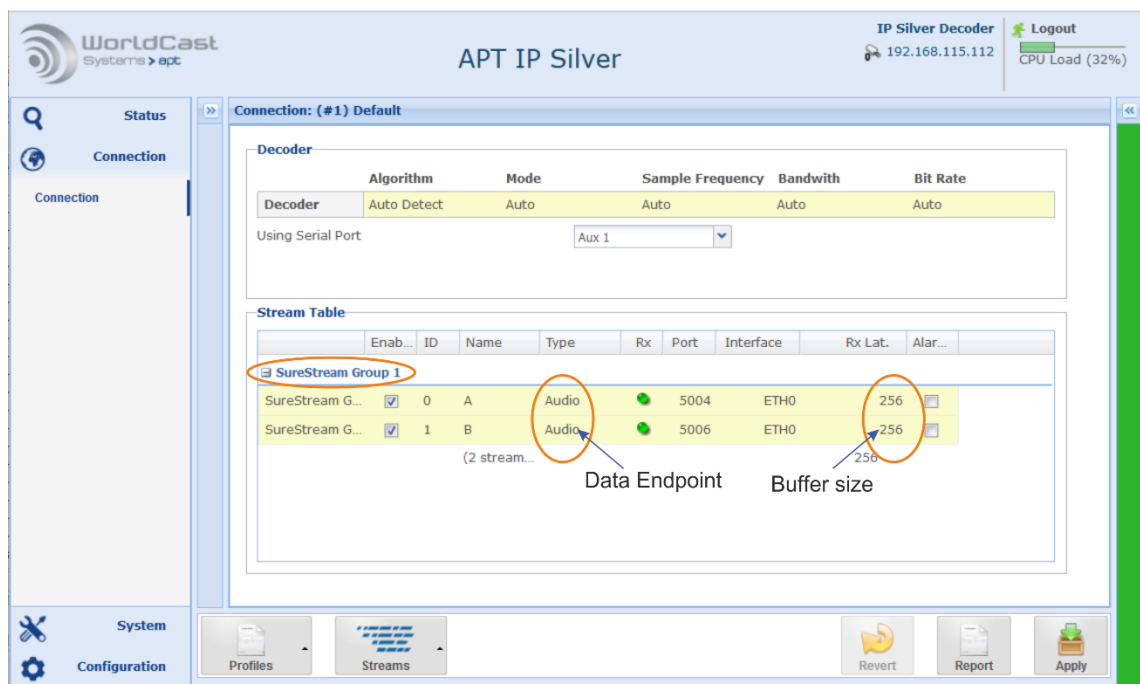


Figure 4-6: Shows a SureStream configuration on the Decoder with two streams received

The figure above shows a working Decoder configuration. Two component streams are received on the physical ETH port; hence they are transmitted on a single port at the Encoder end (as shown in the Encoder section).

### 4.3.1 SureStream – Decoder Performance

The performance monitor delivers precise information about the component streams and the performance of the recombined data stream. The recombined stream is the result of the combination of the component streams and consists of packets from all sources.

Only this recombined stream supplies the packets that are decoded or forwarded. Because it is generated locally with the recombiner, it is not directly visible on the performance monitor.

There are two ways of monitoring the SureStream performance:

- ➔ Creating a monitor stream, making the recombined stream visible
- ➔ Deriving Performance Information from the Component Streams

#### 4.3.1.1 Reading performance information from the component streams

Without a monitor stream, the recombined stream is presented by the highest stream ID (stream B). The screen shot below shows the principle.

Stream B includes the recombined packets of A AND B. In a perfect network, the number of duplicated packets is 50% of the total packet rate (displayed as “Duplicated Packets”). The statistics of stream B shows the packet count of streams.

Another critical indication is the number of dropped packets and the LOC events in the bottom line below the highest stream ID (highlighted). If you see a zero at both columns, then the recombined stream is error-free.

The bottom line on the screenshot shows:

- ➔ 0 Dropped Packets of decoded content
- ➔ 1043 Duplicated Packets
- ➔ 0 LOC Events of decoded content

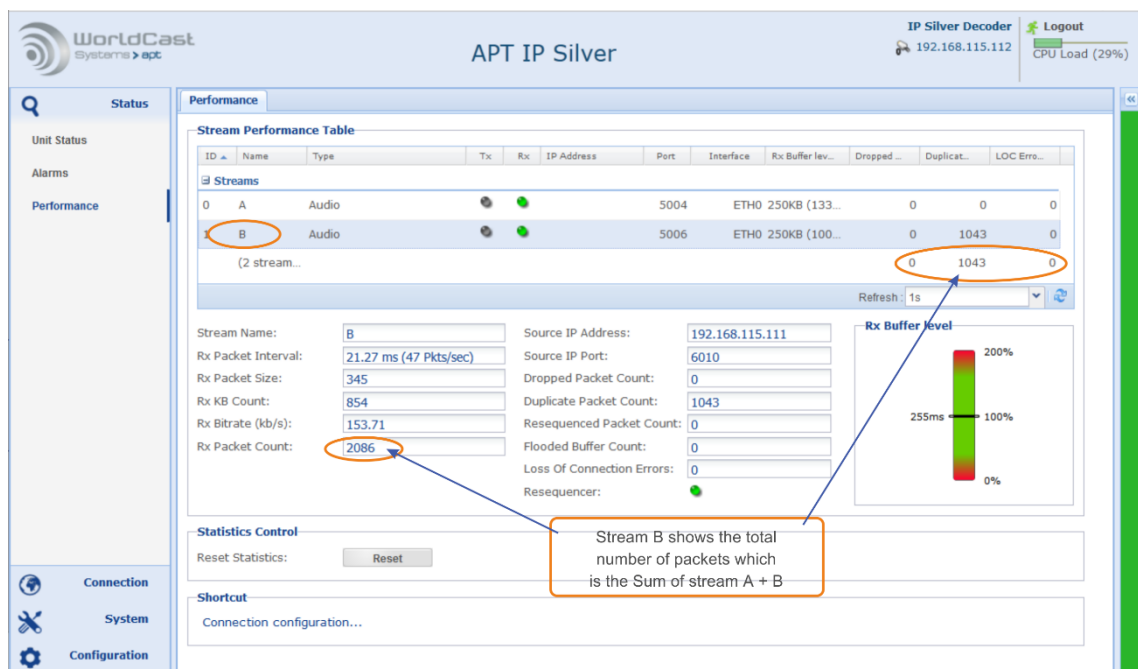


Figure 4-7: Shows the stream performance of component streams and the SureStream group



### 4.3.1.2 Creating a Monitor Stream

A monitor stream is one additional stream in a SureStream group on the DECODER. It is used to visualize the performance of the recombined stream, which supplies the data content for decoding or forwarding.

Adding the third stream allows monitoring of the combined stream, and separately monitoring each component stream. The monitor stream can be seen as a virtual stream because it is not received from the network but is generated by the re-combiner in the decoder.

- ➔ The monitor stream must be the same type of the component streams. In the example below, this is an Audio Rx stream.
- ➔ The monitor stream must have the highest Stream ID. Stream ID's are assigned in the order streams are creating. In the example below, this is ID 2.

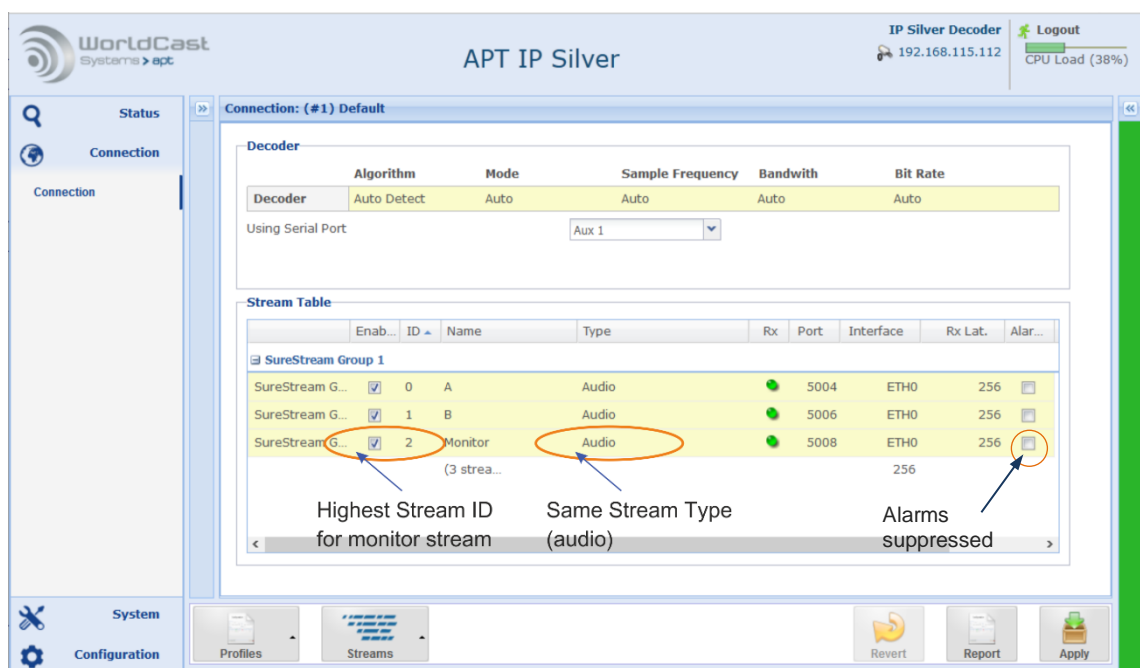


Figure 4-8: Shows a SureStream group with two component streams and a monitor stream

The stream table of the screen shot above is the same configuration as on Figure 4-6 but with the Monitor Stream. The monitor stream must be an audio Rx stream like the component streams.

**⚠** Because the Monitor Stream it is not a real stream the IP address must be 0.0.0.0 or "null".

The monitor stream should not flag any alarm for any reason. Therefore, the Alarms of this stream are suppressed (alarm suppressing checkbox enabled).

### 4.3.1.3 Performance Information with a Monitor Stream

Other than performance monitoring without the monitor stream, all information of the recombined stream is displayed directly by the Monitor Stream.

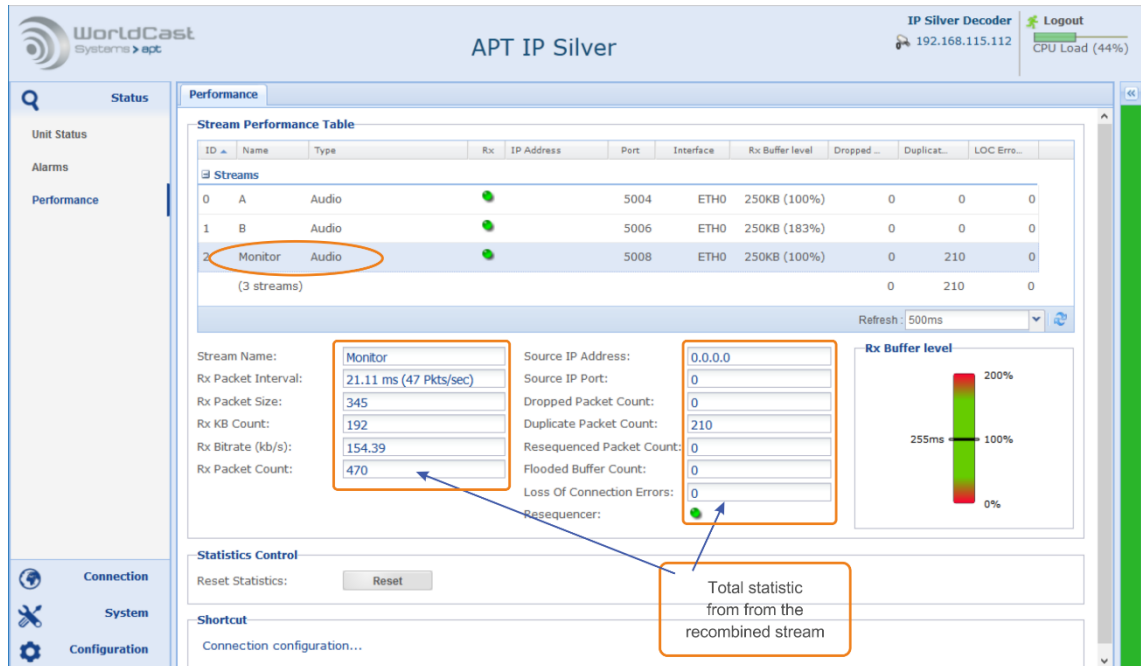


Figure 4-9: Shows the performance of the SureStream monitor stream

The monitor stream represents the recombination of all component streams. Any dropped packet or LOC event on this stream affects the data decoding and may be audible. Ideally, the statistics of dropped packets and LOCs should be 0.

#### Notes:

---



---



---



---



---



---



---

## 5.0 The WorldCast Management System (NMS)

The WorldCast Network Management System (NMS) allows viewing multiple units from one control point. The program has an intuitive look and feel that is easy to understand by both the experienced technician and the casual user.

The graphical user interface provides access to an embedded WEB GUI to the Silver IP Streamer when accessed from the NMS family tree view. The presentation of the GUI of the Silver units is the same when opened from the family tree view (NMS) or directly from a WEB browser.

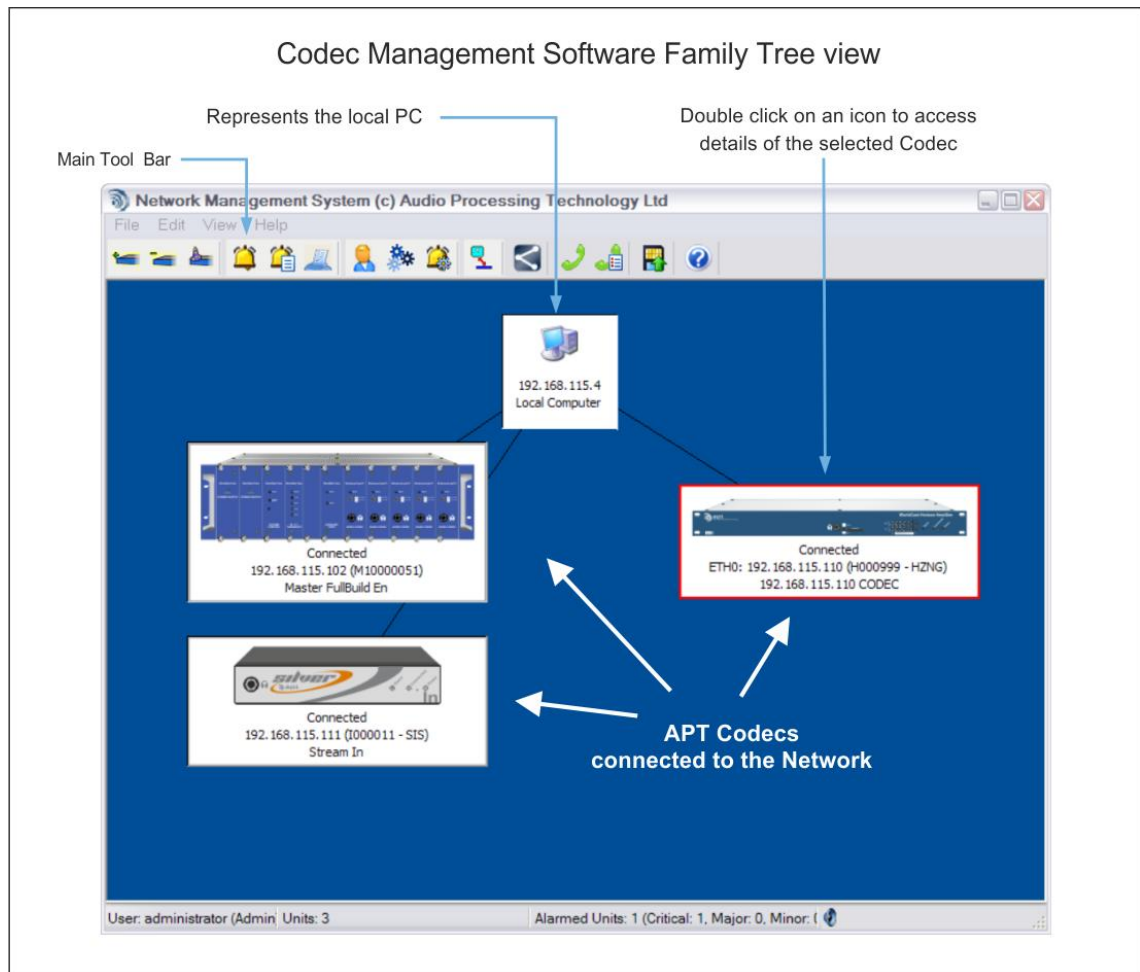


Figure 5-1: Family Tree of the Network Management System (NMS)

- ① The presentation of the IP Silver configuration pages is the same whether it is opened from the family tree view (NMS) or directly from a WEB browser.
- ① The NextGen codec range provides a context menu by right-clicking on the device (once it is connected). This context menu provides an option called "Open Free View" – this option opens as many independent views of the GUI as required but only one instance in read-write mode. All other instances are locked to read-only mode.



## 5.1 Installing the Network Management System

Prior to installing and running the NMS software, please ensure that your service PC meets the minimum hard- and software requirements:

- ➔ Microsoft Windows® XP, Windows® Vista, Windows® 7/8/10
- ➔ 30 MB free Hard Disc space
- ➔ 1024 px x 768 px Screen Resolution or better
- ➔ CD ROM Drive (optional)

**i** *Running any NextGen-Codec with the current system release on the NMS software requires the NMS build version #1193 or higher (supplied with the Codec).*

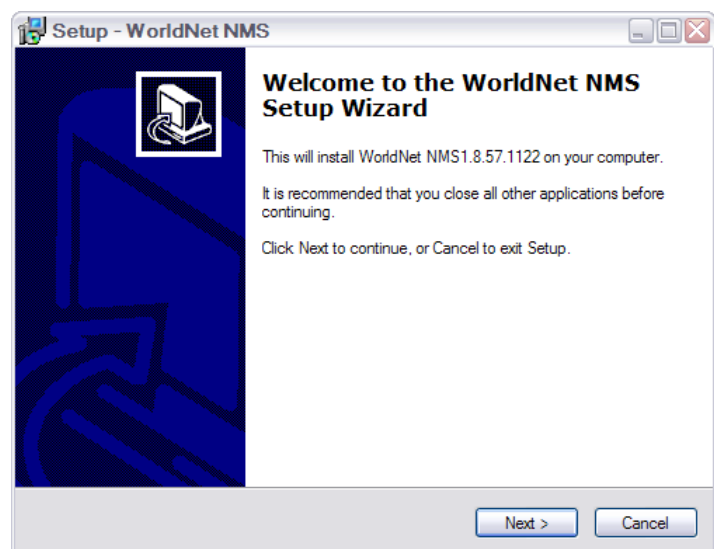
**i** *The NMS requires IP port 7777 and 7778 to be opened on your network!*

The NMS software is generally supplied as a self-extracting application. Run the application and follow the instructions of the following screens:

### First Screen

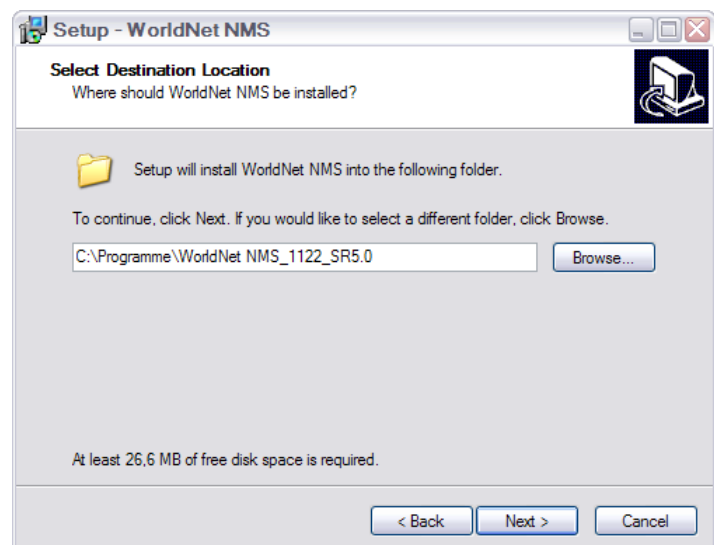
It shows the NMS build version; please make sure that you're installing the correct version, this example shows #1122.

**i** *SR 3.0.x requires NMS version 1193 or higher!*



### Next Screen

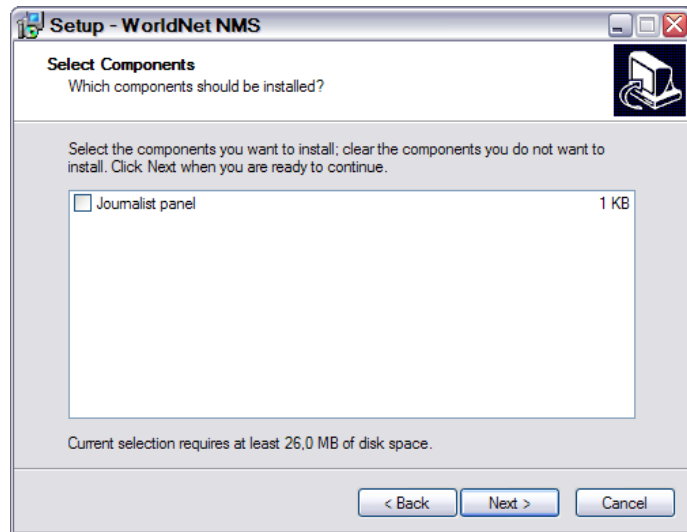
Please choose the folder where you like to install the NMS application.



## Installing the Codec Management System (*continued*)

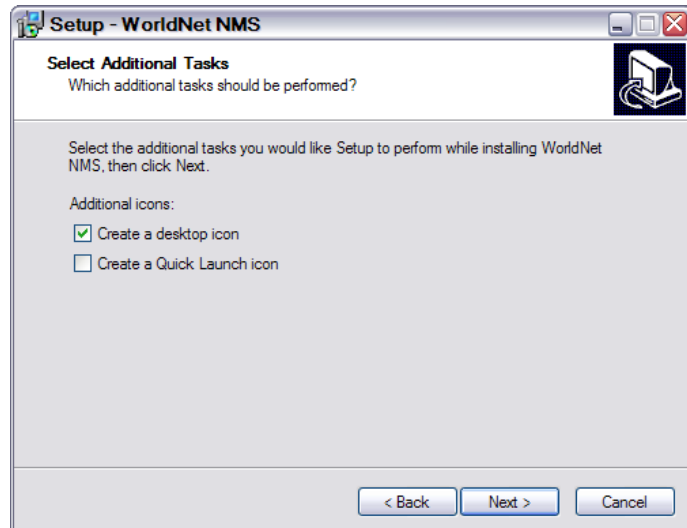
### Next Screen

Journalist Panel is available for the APT IP/ISDN Codec only – do not select it unless you are also running APT IP/ISDN Co-decs in your network.



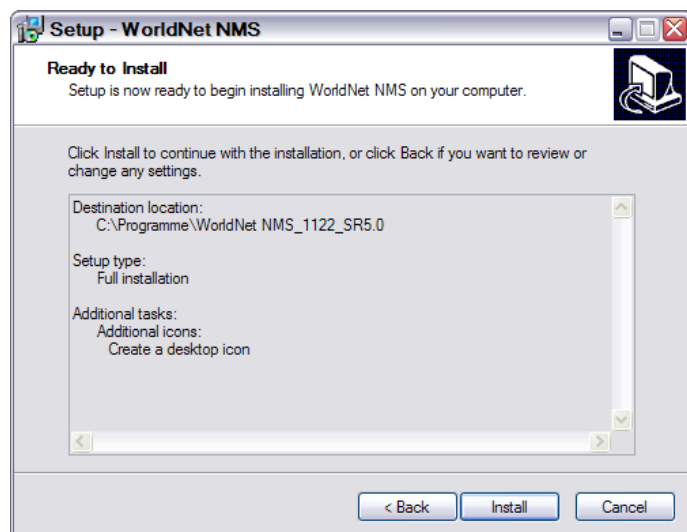
### Next Screen

You can create a desktop, and/or a quick launch icon as required.



### Final Screen

Now you need to complete the installation by clicking on "Install".



## 5.2 Getting Started

Before you can launch the Management System please ensure the following pre-conditions of your network settings:

- ❶ *To get started with the NMS application, ensure that the cabling is properly connected from the Codec to the PC, and that your service PC's Ethernet cards has an IP address within the range of 192.168.100.0 to 192.168.100.255. The IP Silver Encoder and Decoder are set to an IP address within this range as a factory default – usually 192.168.100.110.*
- ❶ *The NMS application will remain inactive until a link is established between the service PC and an active Codec device.*

Launch the Management System application. You will find the program located in the Windows Start Menu under "Program ▶ WorldNet NMS". Start the program and you will be prompted to log in:

### NMS Log-In:

There are three levels of access to the WorldNet Codec Management System:



All accounts, the "Administrator", "Normal" and the "Read Only", require Username and Password login. When shipped only an Administrator account is configured with the default login. We recommended that you change the Administrator login as soon as possible.

- ➔ Default Username: **administrator**
- ➔ Default Password: **password**

- ❶ *Do not forget to change the default password before connecting to an unprotected network!*

The manual of the WorldCast NMS system is provided with the software. You will find the full documentation as help file: Click on the menu "Help->Help"

End of Document