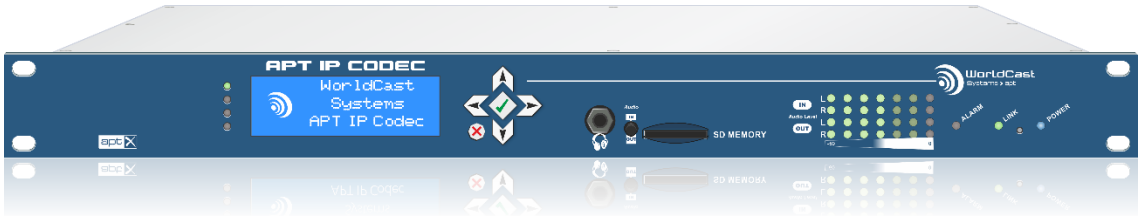
WorldCast Systems
apt > ecreso > audemat

POWERFUL PERFORMANCE | POWERFUL CONTROL | POWERFUL SAVINGS

WorldCast Systems
APT IP Codec
User Manual



System Release 3.0.x | Document Version 2.6 | release/update: May 2018

WorldCast Systems S.A.S (previously Audemat S.A.S)
20 avenue Neil Armstrong – 33700 Mérignac (Bordeaux Métropole) – France
www.worldcastsystems.com

DECLARATION OF CONFORMANCE

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

We, hereby, certify that APT IP Codec 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).

IEC 61000-4-2	(2008)	IEC 61000-4-6	(2008)
IEC 61000-4-3	(2006) + A1 (2007)	IEC 61000-4-8	(2009)
IEC 61000-4-4	(2004) + A1 (2010)	IEC 61000-4-11	(2004)
IEC 61000-4-5	(2005)	NF EN 55022	(2012)

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

⚠ 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.

Installation and Operational Manual for **APT IP Codec** and **APT IP Decoder***

**IP Decoder is a legacy product, but full support is still provided.*

ⓘ *In the year 2015, all WorldCast Systems products were re-named in order to harmonize the product ranges throughout the WorldCast System brands. This APT IP Codec was formerly named as Horizon NextGen. It is the same product, but the name has been changed.*

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 email to:

apt-cust-support@worldcastsystems.com

Table of Contents

Safety Notices

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

(GB) Important Safety Notice

This unit complies with the safety standard EN60950. To ensure safe operation and to guard against potential shock hazard or risk of fire, the following must be observed:

If the unit has a voltage selector, ensure that it is set to the correct mains for your supply. If there is no voltage selector, ensure that supply is in the correct range for the input requirement of the unit.

Ensure fuses fitted are the correct rating and type as marked on the unit.

The unit must be earthed by connecting to a correctly wired and earthed power outlet. The power cord supplied with the unit must be wired as follows:

Green/Yellow = Earth	*Blue = Neutral*	*Brown = Live*

The **green/yellow** colored wire must be connected to the supply plug terminal marked with the letter E or by the earth symbol (I) and is colored green or green/yellow.

The blue colored wire must be connected to the supply plug terminal marked with the letter N or colored black or blue.

The brown colored wire must be connected to the supply plug terminal marked with the letter L or colored red or brown.

The unit shall not be exposed to dripping or splashing and no objects filled with liquids, such as coffee cups, shall be placed on the equipment.

(D) Wichtiger Sicherheitshinweis

Dieses Gerät entspricht der Sicherheitsnorm EN60950. Für das sichere Funktionieren des Gerätes und der Unfallverhütung (elektrischer Schlag, Feuer) sind folgende Regeln unbedingt einzuhalten:

Verfügt das Gerät über einen Spannungswähler, muss dieser Ihrer Netzspannung entsprechend eingestellt sein.

Die Sicherungen müssen zu jeder Zeit in Typ- und Stromwert mit den Angaben auf dem Gerät und den Hinweisen in diesem Handbuch übereinstimmen.

Die Erdung des Gerätes muss über eine geerdete Steckdose gewährleistet sein.

Das mitgelieferte Stromkabel muss wie folgt verdrahtet werden:

Braun = Phase	*Blau = Nullleiter*	*Grün/Gelb = Erde*

Das Gerät darf nicht mit Flüssigkeiten (Spritzwasser, usw.) in Berührung kommen. Stellen Sie niemals Gefäße mit Flüssigkeiten, z.B. Kaffeetassen auf das Gerät!

(F)

Important – Note de Sécurité

Ce matériel est conforme à la norme EN60950. Pour vous assurer d'un fonctionnement sans danger et pour prévenir tout choc électrique ou tout risque d'incendie, veillez à observer les recommandations suivantes:

Le sélecteur de tension doit être placé sur la valeur correspondante à votre alimentation réseau.

Les fusibles doivent correspondre à la valeur indiquée sur le matériel.

Le matériel doit être correctement relié à la terre.

Le cordon secteur livré avec le matériel doit être câblé de la matière suivante :

Brun = Phase	*Bleu = Neutre*	*Vert/Jaune = Terre*

Ne pas exposer cet appareil aux éclaboussures ou aux gouttes de liquide. Ne pas poser d'objets remplis de liquide, tels que des tasses de café, sur l'appareil.

(I)

Norme di Sicurezza – Importante

Questa apparecchiature è stata costruita in accordo alle norme di sicurezza EN60950. Per una perfetta sicurezza ed al fine di evitare eventuali rischi di scossa elettrica o d'incendio vanno osservate le seguenti misure di sicurezza:

Assicurarsi che il selettore di cambio tensione sia posizionato sul valore corretto.

Assicurarsi che la portata ed il tipo di fusibili siano quelli prescritti dalla casa costruttrice.

L'apparecchiatura deve avere un collegamento di messa a terra ben eseguito; anche la connessione rete deve avere un collegamento a terra.

Il cavo di alimentazione a corredo del l'apparecchiatura deve essere collegato come segue:

Marrone = Filo tensione	*Blu = Neutro*	*Verde/Giallo = Massa*

Il prodotto non deve essere sottoposto a schizzi, spruzzi e gocciolamenti, e nessun tipo di oggetto riempito con liquidi, come ad esempio tazza di caffè, deve essere appoggiato sul dispositivo.

(E)

Avicio Importante De Seguridad

Esta unidad cumple con la norma de seguridad IEC65. Para asegurarse un funcionamiento seguro y prevenir cualquier posible peligro de descarga o riesgo de incendio, se han de observar las siguientes precauciones:

Asegúrese que el selector de tensión esté ajustado a la tensión correcta para su alimentación.

Asegúrese que los fusibles colocados son del tipo y valor correctos, tal como se marca en la unidad.

La unidad debe ser puesta a tierra, conectándola a un conector de red correctamente cableado y puesto a tierra.

El cable de red suministrado con esta unidad, debe ser cableado como sigue:

Marrón = Vivo	*Azul = Neutral*	*Verde/Amarillo = Tierra*

La unidad no debe ser expuesta a goteos o salpicaduras y on deben colocarse sobre el equipo recipientes con líquidos, como tazas de café.

(NL)

Belangrijke veiligheids voorschriften

Dit apparaat voldoet aan de veiligheidsnormen volgens de EN60950 standaard. Om veilig gebruik te waarborgen en mogelijke spanningsschokken of brand te voorkomen is het belangrijk de volgende regels in acht te nemen:

Als het apparaat over een spanningskeuze schakelaar beschikt, zorg dan dat het juiste voltage gekozen is. Indien er geen spanningskeuze schakelaar beschikbaar is, verzeker u er dan van dat de lokale netspanning binnen het ingangsbereik van de voeding valt.

Zorg ervoor dat de gebruikte zekeringen van de juiste waarde en type zijn, zoals aangegeven op het apparaat.

Het apparaat moet geaard worden via een correct aangesloten en van randaarde voorzien stopcontact. De bij het apparaat meegeleverde spanningssnoer moet op de volgende manier aangesloten zijn:

Groen/Geel = Aarde	*Blauw = Neutraal*	*Bruin = Fase*

De groen/geel gekleurde draad moet verbonden worden met het aardpunt van de stekker, gemarkeerd met de letter E of met het aarde symbool (I) en heeft de kleur groen of groen/geel.

De blauw gekleurde draad moet verbonden worden met de neutrale pin van de stekker, gemarkeerd met de letter N of een zwarte of blauwe kleur.

De bruin gekleurde draad moet verbonden worden met de fase pin van de stekker, gemarkeerd met de letter L of een rode of bruine kleur.

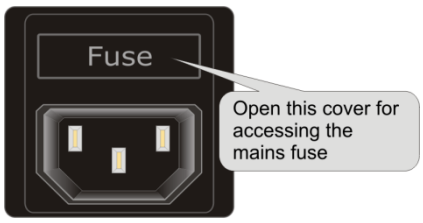
Het apparaat mag niet gebruikt worden in een vochtige omgeving, en dient ook niet gebruikt te worden als onderzetter voor drinkbekers of andere voorwerpen die vloeibare stoffen bevatten.

Power and Low Voltage Ports

Main Fuse Characteristics

The mains supply fuse is located on the rear panel inside the IEC power receptacles.

Voltage rating (Vu)	= 250VAC
Current rating	= 1AH
Characteristics	= Quick Blow



⚠ Any replacement of fuse must be conformal to IEC127 specifications with the same above characteristics.

SELV Ports

- SELV stands for Safe Extra Low Voltages as defined in EN60950.
  All SELV ports must only be connected to SELV type equipment.

TNV1 Ports

- TNV1 stands for Telecommunications Network Voltages type 1.
  All TNV1 ports must only be connected to TNV1 networks.

Output XLR Connectors

- Do not supply any power source including the phantom power to the Output XLR connectors. Failure to observe this warning may cause your unit to malfunction and invalidate your warranty.

General Precautions

- **Reduced Air Flow** - To avoid overheating ensure that the ventilation slots are not blocked. If the equipment is placed in a closed area, such as a rack or a case, ensure that proper ventilation is provided and that the internal rack operating temperature does not exceed the maximum rated temperature at the location of the unit.
- **Mechanical Loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Reliable Earthing** - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- **Radio Interference** - Class-A ITE Warning - 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.

1.0 About this Codec Manual

Thank you for purchasing the Audio Codec from WorldCast Systems. We have developed this unit to be as user-friendly as possible, and it contains many advanced features that are designed to make the use of this product simple and straightforward.

This operations manual is intended for installers and operators of the Audio over IP network transmission links, and it describes the function, the installation and use of the unit.

It is recommended that new users 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 describes the APT IP Codec and IP Decoder and is the primary reference covering the configuration, installation, operation and troubleshooting.

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

As of this publication date, this document is the current manual revision. We recommend checking with your distributor or on the APT website for updates.

1.1.1 Standard Applications for SR 3.0.x:

- **ScriptEasy version 2.8.7.001**
- **MasterView 2.1.0 web application** (desktop version not supported anymore)

1.2 Critical Network Security Advice

1.2.1 This IP Audio Codec is a network device!

As a network appliance, the IP Codec can create security vulnerability between your internal LAN and the WAN domain. The IP Codec provides 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 3.5.3)!*

ⓘ *Before connecting to your Network, please check the SNMP community strings. Don't use the trivial default names (refer to section 3.5.7.1)*

1.3 Company Profile

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, E1/T1, and 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 integrated 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 repeatedly been 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 clients and has achieved IS0 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 your local sales office or to WorldCast Systems HQ.

Check that the list of contents is complete as follows:

APT IP Codec / IP Decoder Unit

Serial Number located on the rear panel:

IP Codec:	**H-**
IP Decoder:	**J-**

(please complete)

- **Power Supplies**

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

- **Cables**

A power cord is provided with the unit together with any other special cables as ordered.

- **CD box**

A CD where you can find the documentation for this product. If a Codec is not labeled with an individual IP address, then the default addresses are valid:

Ethernet Port	Default IP Address	Port	DHCP / Static
ETH0	192.168.100.110	http 80, https 443	Static
ETH1	192.168.101.111	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. Please do not connect the system to the network or apply power to the unit if you are in any doubt about the contents as this could cause damage to the hardware.

ⓘ *More information about connection and installation is provided in section 2 of this document.*

Notes:

_____

_____

_____

_____

1.5 Introduction

The "Next Generation" audio Codecs are based on the new APT Codec core engine. This engine is designed to be as flexible and versatile in use as possible. The core is powerful and addresses more than ever the needs of professional IP audio transmissions.

The APT IP Codec is a full duplex, multi-algorithm audio codec offering conventional analog left and right audio connections and AES/EBU digital audio connections operating through IP, while the IP Decoder uses the same hardware, but it is limited to decoder operations.

The new Codec generation incorporates the enhanced versions of the aptX® algorithm (real time transmission on the network with data reduction by factor 4:1), Linear PCM 16 and 24-bit, MPEG 1/2 Layer II and the full MPEG 2/4 AAC suite of algorithms including MPEG 2/4 HE-AAC. MP3 for decoding (MPEG 1/2 L III) and an Auto Detect mode have been added to the Decoder path.

As an option, the IP Codec allows the transmission of a digital MPX signal fed into the AES interface and sampled at 192/128 kHz.

The units can deliver high-quality audio used for inter-studio networking, remote/outside broadcasts, and STL/TSL applications. The new generation is even more suitable for use in either AM, FM, DAB and many other broadcast and professional audio environments.

The APT IP Codec and the IP Decoder run an embedded WEB GUI that can be accessed from a web browser or the APT NMS. A headphone socket provides for additional monitoring of the audio input or output. The rear-panel audio inputs can be switched to accept either analog or digital signals, and if required the digital output can be synchronized with an external digital reference signal.

Additional interfaces allow for the connection of auxiliary data, alarms, and optocoupled control inputs.

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.

The IP Decoder is identical to the APT IP Codec except it is a decoder only product, so it has no audio inputs.

⚠ The IP Decoder is a legacy product but still supported.

1.5.1 System Options

The following soft- and hardware options are available:

- **Redundant PSU:**

Increase the reliability of your Codec

- **SureStream** (license required):

Reliable and lossless connectivity over lossy IP networks and the Internet

- **Digital MPX over IP** (license required):

This software option provides a digital signal path with 128 kHz or 192 kHz FS through the AES input of the unit. With this option, a digital MPX signal can be transmitted either as 16 or 24 Bit linear PCM stream (license required). Two MPX modes are available, full MPX or MPX for audio and RDS only (MPX bandwidth 64kHz).

Notes:

1.6 Getting Connected

This chapter outlines how you can quickly connect your APT IP Codec and start sending audio. The following chapter describes all of the interfaces in more detail.

Begin by connecting mains power to the unit.

Making a connection and send audio:

- set up the APT IP Codec for analog or digital audio
- set up the configuration
- apply these settings to the unit

The audio connections are made on the rear panel using XLR-3 connectors for analog and digital connections.

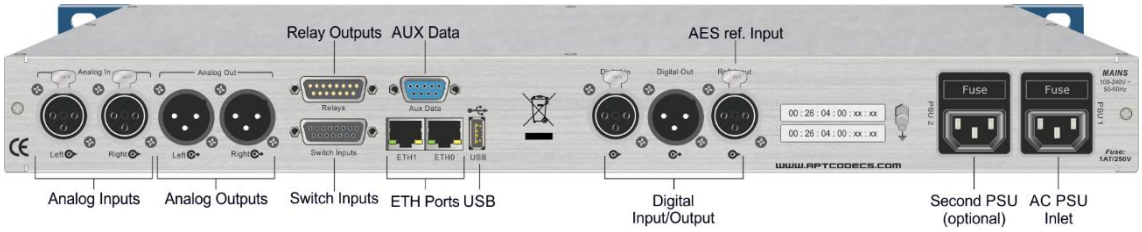


Figure 1-1: APT IP Codec rear panel view

Figure 1-2: IP Decoder rear panel view

***Note**: The APT IP Codec and the IP Decoder provide analog and digital audio output always simultaneously. Selecting the analog or the digital mode affects the signal inputs only.*

1.7 IT Security Recommendations

1.7.1 IP Codec/IP Decoder – Network Connection

As a network appliance, the IP Codec can create security vulnerability between your internal LAN and the WAN domain. The IP Codec and the IP Decoder 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.

The image below shows the principle of the network connection via two ETH ports. Both ports are configured for different networks.

You can configure either ETH ports or only one for management access. Nevertheless, care must be taken that the management port is inaccessible on the streaming network (the external network).

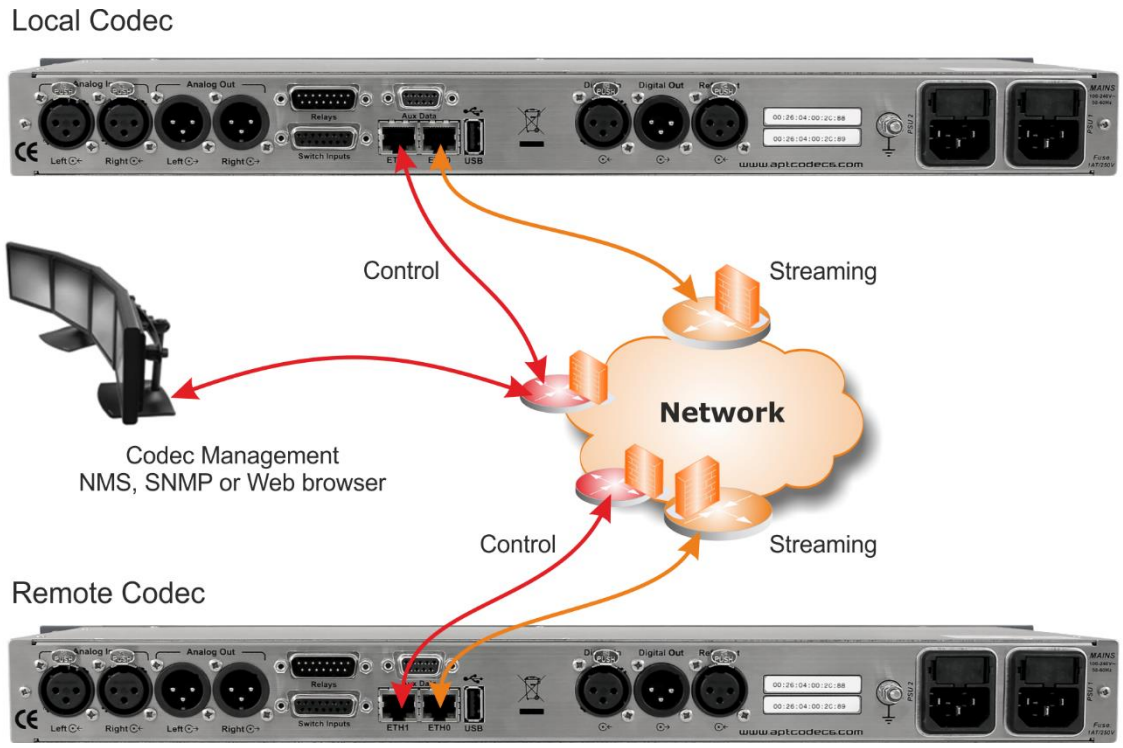


Figure 1-3: Shows how your LAN is securely protected by your external firewall and the internal firewall of the IP Codec.

On the example above, ETH 1 is used for management and ETH 0 for audio streaming. It is a user decision to use either a single port for management and data streaming or to separate the services using both ports.

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

1.8 Connecting via 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 both Ethernet ports; 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
ETH1	192.168.101.111	http 80, https 443	Static

1.8.1 IP Codec Firewall – 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 both ETH interfaces individually (3.5.4.8).

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	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

A user login protects the Web GUI. It should be obvious that any default password is insufficient for regular use. Furthermore, it is negligent behavior if this default login is not changed before connecting to a network. Please refer to section 3.5.3on how to improve 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 (refer to section 3.5.3).

SNMP

The default names of the community strings should also not be considered sufficiently secure for regular operation. 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 more "cryptic" community strings. Refer to section 3.5.7.1 on how to change the community string name.

⚠ Before connecting to your Network, please check the SNMP community strings. Do not use the default names; even if SNMP is not used (refer to section 3.5.7.1).

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 schemes of the APT IP Codec rear panel connectors. This section consists of two parts:

- Preparing for installation of the APT IP Codec
- 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, depending on your APT IP Codec configuration.

Tools:

One flat and Phillips screwdriver suitable for M 5/6 rack mounting bolts. A basic electronics toolkit is useful for special cabling.

Network connection cables

For Ethernet connections, you need one or more CAT5/6 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 connection and configuration of more than one APT IP Codec simultaneously.

Cables for audio signals:

At least one male or female standard audio cable, equipped with balanced wired XLR connectors.

Power cables:

AC power cables are supplied with the APT IP Codec.

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

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

2.2 Pre-Installation Notes

Always pre-test the system on the bench with the intended configuration prior to installation at a remote site.

Do not allow the audio level to light the red "clip" LED on the front panel LED or on Level meter on the GUI, as this causes severe distortion (digital audio overload).

All network interface ports, as well as the mains power connection, must be externally protected from lightning strikes (if appropriated) because damage from lightning strikes is not covered by the warranty.

Radio Interference – Class A ITE Warning:
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

2.3 Front panel Components

Figure 2-1: APT IP Codec front panel components with the front panel display option

ⓘ *The front panel display is an option; the IP codec with this option must be ordered explicitly.*

2.3.1 Power Connection and Alarm Status

The Power indicator LED indicates that power is applied to the unit
The Alarm indicator LED indicates that an alarm condition exists. There is a number of alarm conditions which can be enabled on the APT IP Codec or IP Decoder – refer to section 3.6.5 for more information.
The Connected LED shows the presence of a connection. The following table shows the different states of the LED.

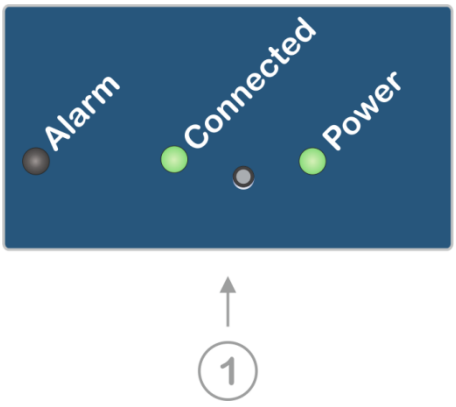


Figure 2-2: Status indications

Connected LED Color:	Off/Grey	Green	Red
No Stream enabled	X		
Receiving & Transmitting ok		X	
Connection Error			X

2.3.2 Reset to Default IP Addresses

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 APT IP Codec & IP Decoder to the default addresses, insert a small tool until and press the switch. Hold it in place until the Connected LEDs start to flash (about 5 seconds) – then remove it.

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

Ethernet Port	Default IP Address	Port	DHCP / Static
ETH0	192.168.100.110	http 80, https 443	Static
ETH1	192.168.101.111	http 80, https 443	Static

2.3.3 Audio Level Indication

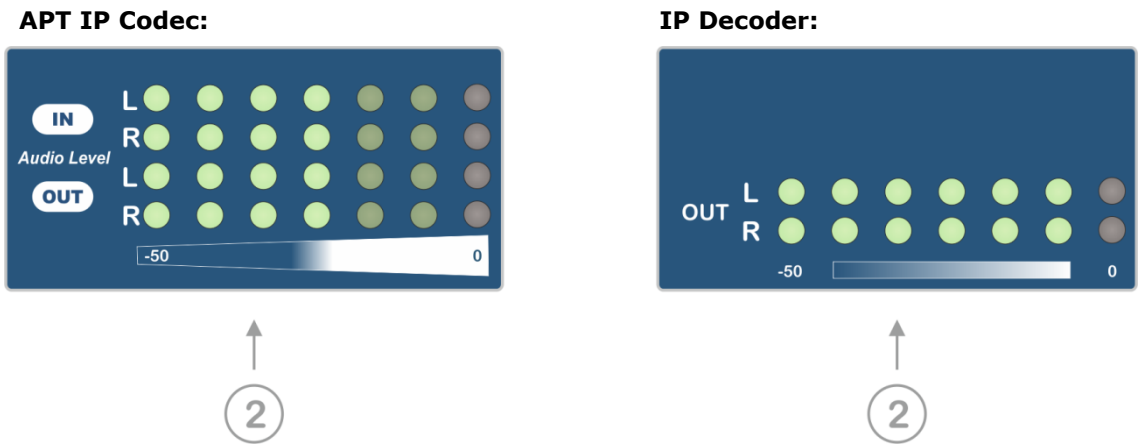


Figure 2-3: Audio Level Indication on APT IP Codec and IP Decoder (outputs only)

The Input and Output level LEDs on the front panel indicate the level of the digital Input ("0" equals full-scale dBFS) or the digital equivalent of the attenuated analog signal. The WEB GUI allows adjusting the analog clip levels on the Input and Output in reference to the digital signal.

The front panel audio level indicators display levels for audio Inputs and audio Outputs and for both Left and Right channel.

ⓘ *Note that the IP Decoder only as output level meters.*

2.3.4 Monitoring and SD-Card

The 6.3mm jack socket provides audio monitoring with a headphone or active monitor speaker. It is possible to monitor either the audio input or audio output; selected by pressing the small selector switch beside the jack socket.
The SD-Card has two functions, for system configuration backup and audio file storage. With the system backup, the full configuration can be copied to another IP Codec (cloning).

The Audio file storage is used in cases of no network connectivity; program audio can be played out from the SD-Card

Figure 2-4: Monitoring facility and SD-Card slot

2.4 Front Panel Display

With the front panel display, you can access the basic configuration parameters and operate the units in a simplified way. The following section describes the options provided by the front panel display.

ⓘ *The front panel display is an option; the IP codec with this option must be ordered explicitly.*

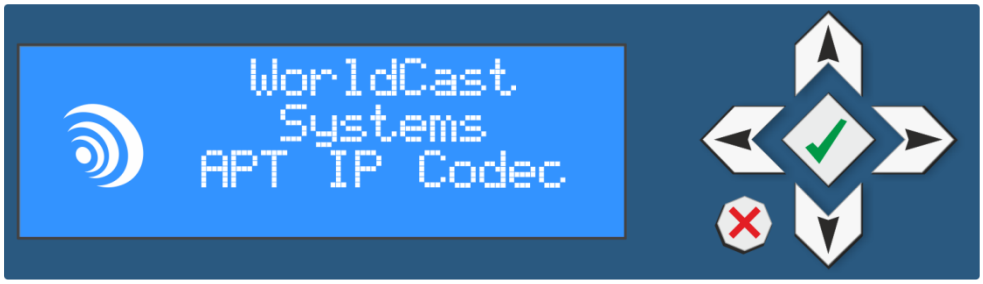


Figure 2-5 Shows the front panel display option during boot-up

Some 'Management', 'Configuration' and 'Monitoring' parameters may be viewed or set using the front display application.

The IP Codec front display is active from the moment you start the unit. It can go into sleep mode (dark), pressing any of the buttons will re-activate it.

Use the keypad to the right of the screen to navigate the front screen application:

- Use the arrow keys to navigate through a menu or to a value, and to change values.
- Use the central green checkmark key "✓" to confirm/enter and to switch to edit mode.
- Use the red "✗" key to cancel or return to the previous screen.

Notes:

2.4.1 Display Screens

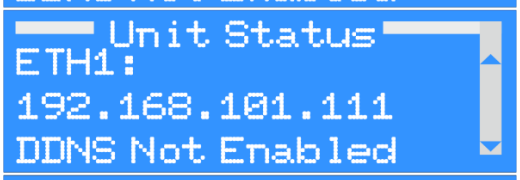
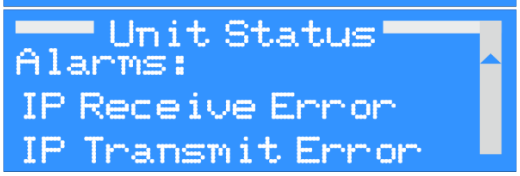
After the unit has booted, the screen shows the current Unit Status; pressing the green checkmark key switches to the main menu.

Most of the menus have more than one screen. Use the arrow keys to navigate through all the screens.

2.4.1.1 Display - Unit Status

This "Unit Status" screen is read-only – there are no options to change the parameter.

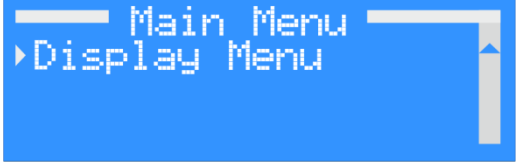
Use the central green checkmark key "✓" to enter the main menu.

Unit Status Screens – read only	
Screen 1 Shows the unit Name Default: APT IP Codec	
Screen 2 Shows the current IP address and Dynamic DNS status of ETH0	
Screen 3 Shows the current IP address and Dynamic DNS status of ETH1	
Screen 4 Shows the active Connection Profile with the number and profile name: (#02) Loop Test	
Screen 5 Shows the currently active alarms: - IP Receive Error - IP Transmit Error All current alarms are shown (check the arrows on the scroll bar to identify another screen).	

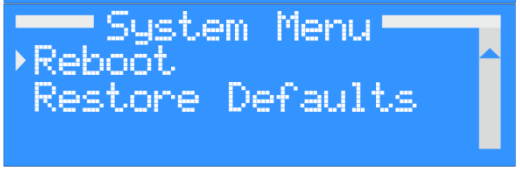
Notes:

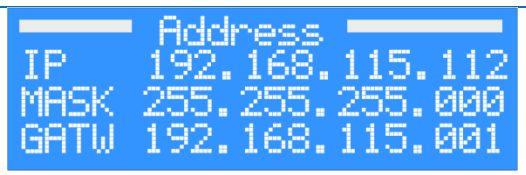
2.4.1.2 Display - Main Menu

The Main Menu provides access to all submenus. Use the arrow keys to navigate to the sub-menus.

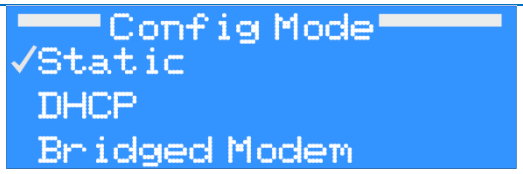
Main Menu	
Screen 1	
Screen 2	

2.4.1.3 Display - System Menu

Main Menu - System	
Screen 1 provides the access to the network configuration of ETH0 and ETH1. "Version" shows the serial number of the unit and the software release loaded.	
Screen 2 "Reboot" starts a soft reboot of the unit. "Restore Defaults" deletes all customer settings and load factory default values. ⓘ *Refer to section 3.5.5!*	

Main Menu – System - Network	
Screen 1 "Address" for IP Address setting "Config. Mode" for DHCP, static IP address or "Modem Bridged" "MAC Address" shows the MAC of the unit	
Address Screen provides the access to the IP address parameter of ETH0 and ETH1. Change the values with the arrow keys and confirm your configuration with the green checkmark key.	

2.4.1.4 Display – System Menu

Main Menu – System - Network	
Screen 1 "Address" for IP Address setting "Config. Mode" for DHCP, static IP address or "Modem Bridged" "MAC Address" shows the MAC of the unit	
Config Mode IP address configuration mode options. For configuration details, refer to section 3.5.4.1 (Network Configurations).	

2.4.1.5 Display – Audio Menu

Main Menu - Audio	
Screen 1 provides options for analog or digital inputs, digital output sampling frequency and the analog input clip level.	
Screen 2 provides options for the analog output clip level. For configuration details, refer to section 3.6.1.	

2.4.1.6 Display – Profile Menu

Main Menu – Profile	
Screen 1 provides all available Connection Profiles and shows the current active connection (Loop Test)	

2.4.1.7 Display – Display Menu

Main Menu – Display	
Screen 1 provides the setting of Brightness and Contrast of the screen.	

Notes:

2.5 Wiring Information

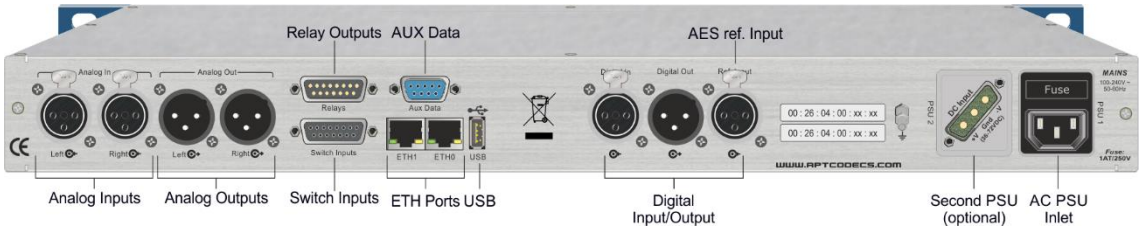


Figure 2-6: APT IP Codec rear panel components

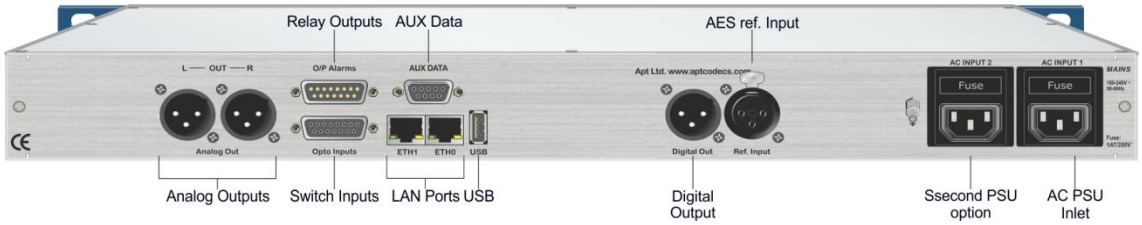


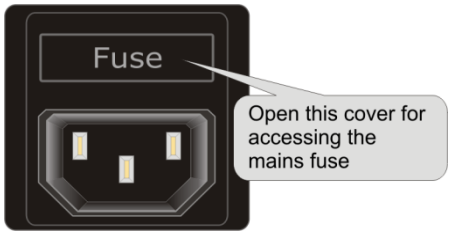
Figure 2-7: IP Decoder rear panel components

2.5.1 Power Supplies

AC Power Inlet

The AC power interface is provided in an IEC inlet and allows the connection of a suitable AC supply between 100 V and 260 VAC.

This inlet also holds the AC mains fuse. Please refer to the safety instructions for replacement.

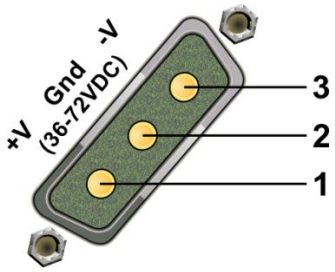


AC Power inlet (IEC)

DC Power Inlet

The DC power input is supplied on a 3 pin D-Type male power connector and allows the connection of a suitable DC supply between 36 V DC to and 72 V DC. The DC input is floating (isolated from ground); please take care of the correct polarity!

Connection to incorrect pins may result in damage to the power supply!



DB-3 Power D connector, view to the pins (not to solder side)

Power Supply:

Max. Input: 72 VDC between Pin 1 and 3
Max current: 0.6 A (full load)
DC always apply between pin 1 and 3

Pin	Description
1	+ ve (pos. voltage relative to GND)
2	Ground
3	- ve (neg. voltage relative to GND)

2.5.2 Audio Inputs and Outputs

Standard XLR-3 female socket

Input analog or digital

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

Digital audio levels are fixed (AES3).
Analog input levels can be adjusted in reference to the digital level via the Web GUI in increments of 0.1 dBu. The input impedance is selectable between 600 Ω and >10 kΩ via the Web GUI.
The digital input impedance is fixed at 110 Ω.

Standard XLR-3 male socket

Output analog or digital

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

Digital audio levels are fixed (AES3).
Analog output levels can be adjusted in reference to the digital clip level via the Web GUI in increments of 0.1 dBu.
The output impedance is selectable between 600 Ω and 50 Ω via the Web GUI.
The digital output impedance is fixed at 110 Ω.

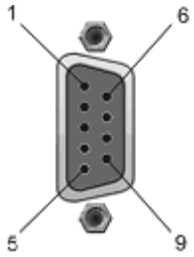
Standard XLR-3 female socket

Digital reference input

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

This AES11 reference input accepts an AES/EBU clock signal to synchronize the Sample Rate Converter (SRC) at the AES/EBU outputs to a master (house) clock. Ideally, the sampling frequency of the incoming audio signal should be at the same frequency as the reference signal. However, if the two frequencies differ by a factor of less than 16:1 then the SRC module will function satisfactorily and pass audio to the output. The sampling rate of the output audio will be up- or down- converted to match the frequency of the reference signal.

2.5.3 Auxiliary Data Interface



9 pin female connector contact view

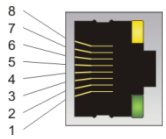
This is a SELV connection and must only be connected to other SELV ports.

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 APT IP Codec unit offers continuous data transfer rates from 1.200 to 115.200Baud (non-embedded on AUX IP-Streams).

2.5.4 Ethernet Interfaces



10BaseT socket wiring scheme

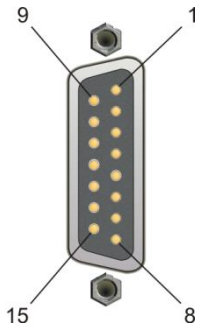
Ethernet Interfaces (ETH0/1)

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

These Ethernet interfaces are available for both connecting to a PC running the WorldCast NMS (or WEB browser) and for sending and receiving audio data.

These ETH ports are 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.

2.5.5 Relay Contact Closures (GPO)



15 pin male connector
contact view

Relay Contact Closures (GPO)

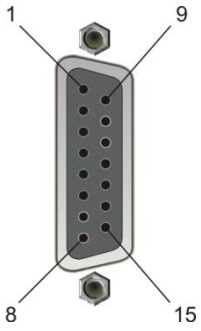
Pin	Description	Function
1	Relay 1 com	Configurable
2	Relay 1 n.c.	Configurable
3	Relay 1 n.o.	Configurable
4	Relay 2 com	Configurable
5	Relay 2 n.c.	Configurable
6	Relay 2 n.o.	Configurable
7	Relay 3 com	Configurable
8	Relay 3 n.c.	Configurable
9	Relay 3 n.o.	Configurable
10	Relay 4 com	Configurable
11	Relay 4 n.c.	Configurable
12	Relay 4 n.o.	Configurable
13	Alarm 5 com	Not Configurable
14	Alarm 5 n.c.	Not Configurable
15	Alarm 5 n.o.	Not Configurable

* n.c. = normally closed
* n.o. = normally open
* N-C = not connected

This relay port supplied on a 15 pin D-type male connector provides five relay contact closures to indicate either the status of the assigned alarms; or these relays are used as GPOs (general purpose output). Each relay provides three contacts where the "com" pin is toggling between normally open (n.o.) and normally closed (n.c.). The summary alarm (relay #5) is also indicated by an LED on the front panel.

Relays #1-4 are configurable for any alarm event, and relay #5 is assigned to the summary alarm.

2.5.6 Switch Inputs (GPI)



15 pin female connector
contact view

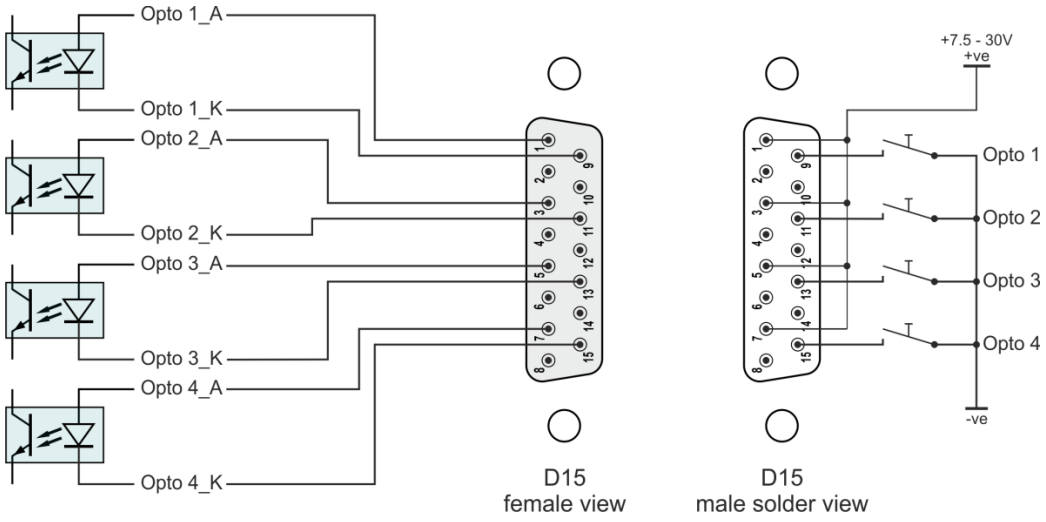
Switch Inputs (opto-isolated)

Pin	Description	Function
1	+ve Opto 1	Opto-coupler 1 Input
2	N-C	
3	+ve Opto 2	Opto-coupler 2 Input
4	N-C	
5	+ve Opto 3	Opto-coupler 3 Input
6	N-C	
7	+ve Opto 4	Opto-coupler 4 Input
8	N-C	
9	-ve Opto 1	
10	GND	Ground
11	-ve Opto 2	
12	GND	Ground
13	-ve Opto 3	
14	GND	Ground
15	-ve Opto 4	

* N-C = not connected

The switch inputs accept any mix of up to a maximum of four DC inputs. An input is active whenever a voltage is applied between +ve and -ve connections (7.5 to 30 V). These signals are then converted and transmitted over the IP link. GND is not connected to –ve; but for a common connection PIN 9, 11, 13 and 15 can be connected to (chassis) GND.

Switch Input – Wiring



3.0 WorldCast WEB-Browser GUI

The WorldCast Web GUI is the control and monitoring tool which communicates with the APT IP Codec, the IP Decoder, and the Silver IP-Streamer. All the next generation units 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 APT IP Codec configuration options.

3.1 The WorldCast WEB GUI - Overview

The WorldCast Web GUI allows you to view and control a single instance of the APT IP Codec, IP Decoder or the Silver IP-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.

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 both Ethernet ports; 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 Codec requires installing the WorldCast Systems SSL Certificate. You can download the certificate from the unit (refer to section 3.5.12.1)

3.1.1.1 Browser Cache

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

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

- after firmware update
- if any page error appears (corrupted appearance)
- if an IP address is re-used, that was previously assigned to another device.

3.1.2 Default Network Settings

The IP Codec provides two IP interfaces: ETH0 and ETH1. You can use both interfaces for control/management, LAN connection, and WAN connections. Both Ethernet interfaces are open by default to connecting to your Web browser. The GUI allows you to manage the services available on each interface at any time.

ⓘ *By default, HTTP browser requests to port 80 are automatically redirected to HTTPS port 443. HTTPS is the standard protocol used for the Web browser access*

ETH	IP Address	Netmask	Gateway
0	192.168.100.110	255.255.255.0	192.168.100.1
1	192.168.**101**.111	255.255.255.0	192.168.**101**.1

Notes:

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.

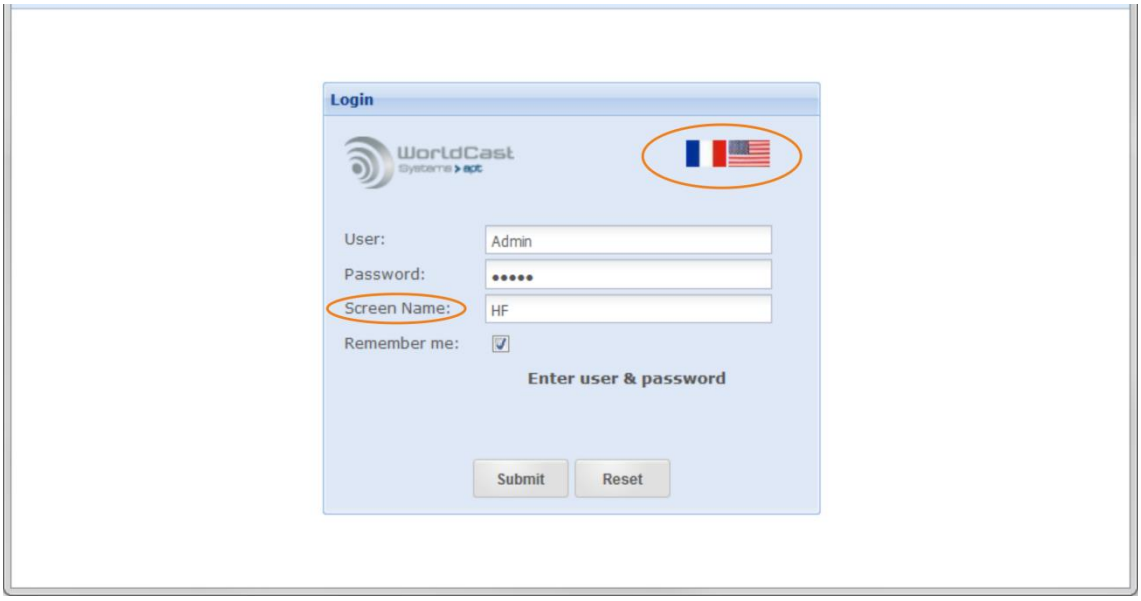


Figure 3-1: The WEB GUI LogIn screen

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. The chat box is described in section 3.5.12.2.

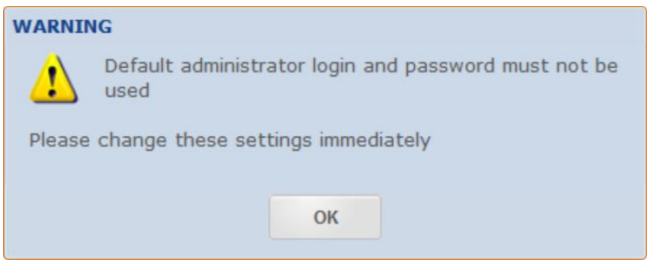
Activating the tick box "Remember me" allows the browser to remember your last LogIn for a new session.

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.

ⓘ *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.

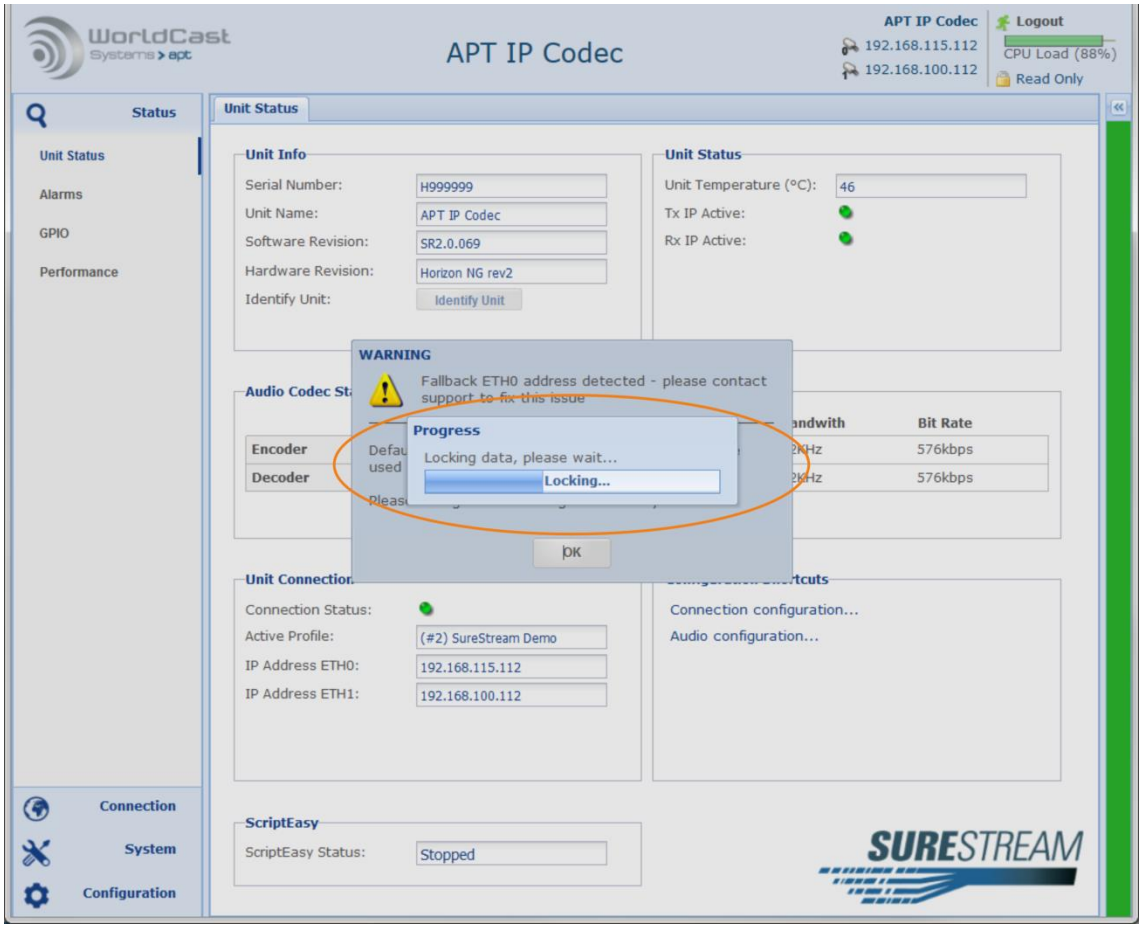


Figure 3-2: After loading the status page the GUI tries to lock the current session for read/write access

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 Codec 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.

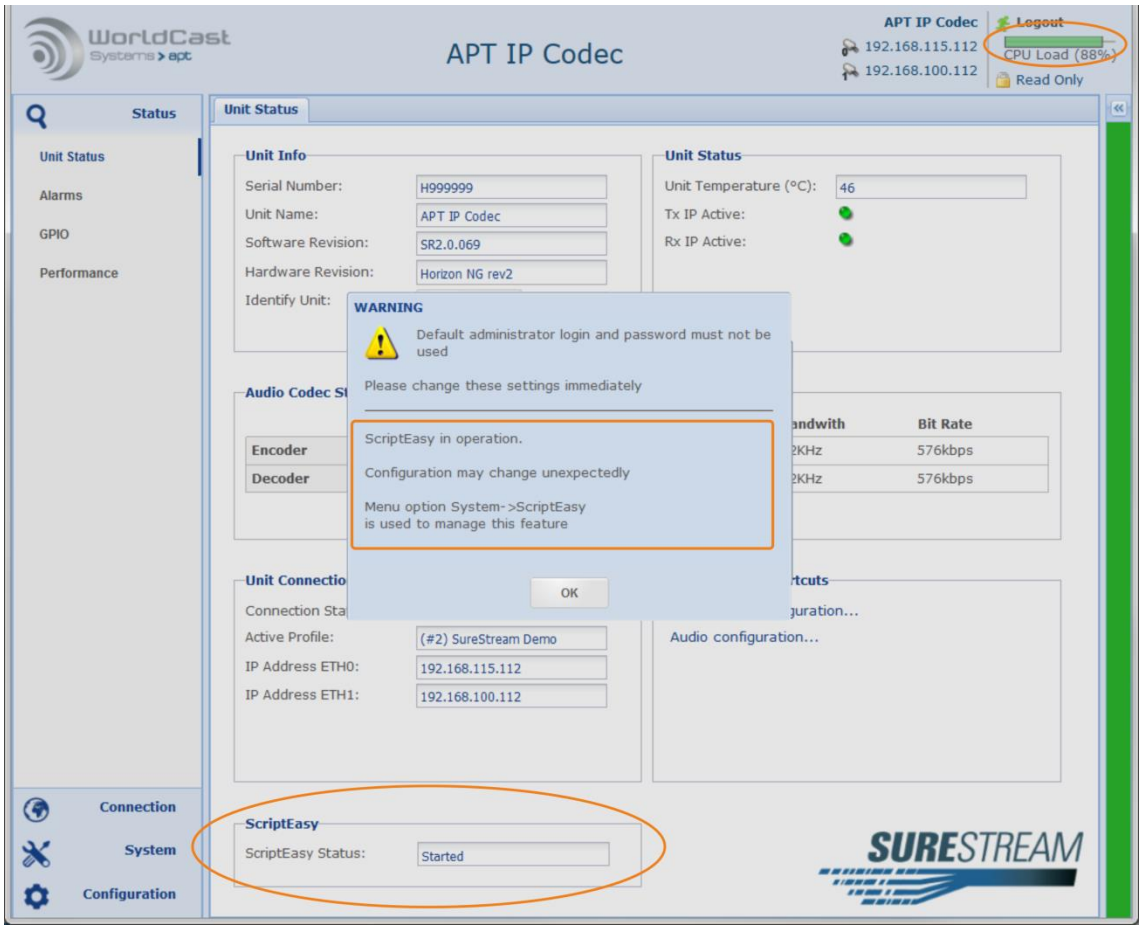


Figure 3-3: S*hows the warning window during start-up listing various information and SureStream license applied*

ⓘ *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 3.5.8.*

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 Codec, 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.

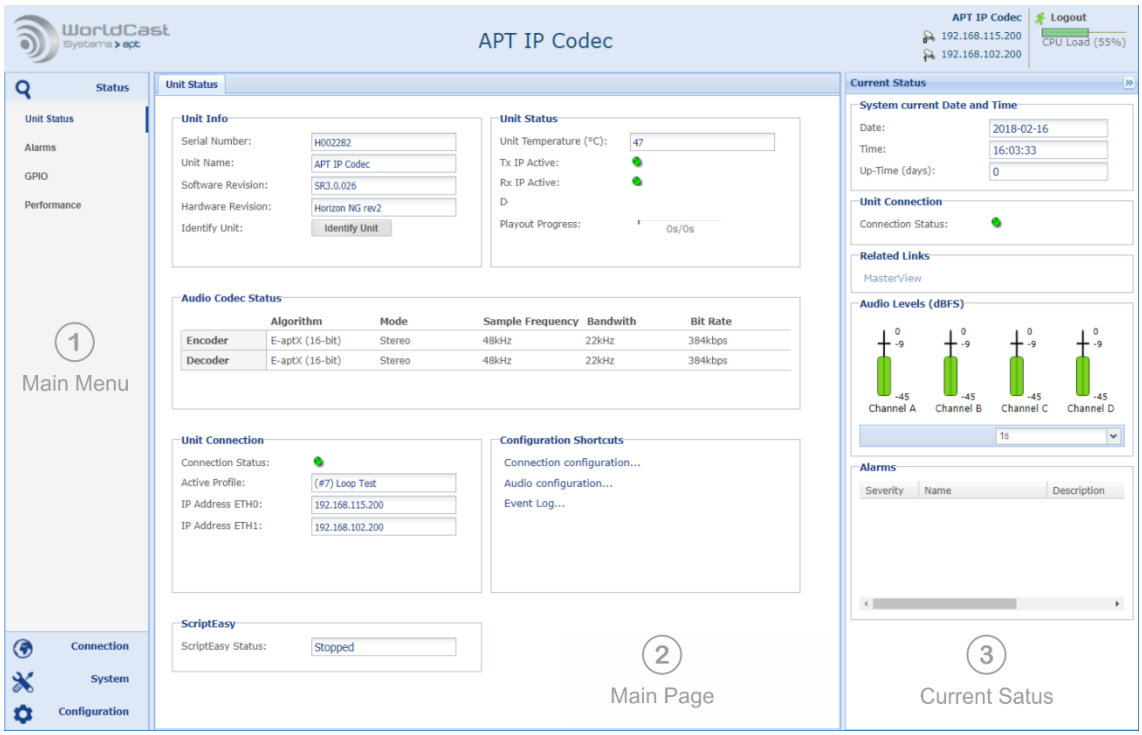


Figure 3-4: Shows the Main Page with "Current Status" frame open

The default Main Page (2) is always the Unit Status page summarizing the situation 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). It also may show additional features depending on applied option licenses (e.g. SureStream).

3.2.5 Session Close - Session Time Out

The Web GUI of the IP Codec 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 accidently.

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.

ⓘ *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.

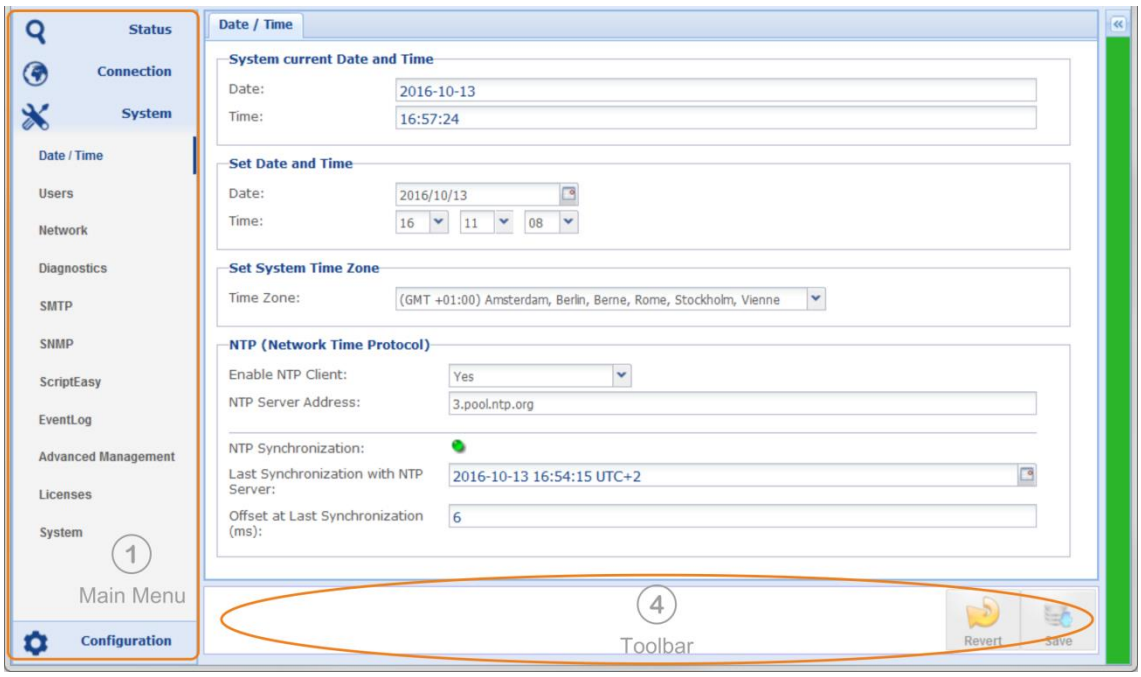


Figure 3-5: The Main Menu expands depending on the selected menu item. The "Current Status" frame is hidden and actually indicated by the green bar on the right-hand side ("good" condition).

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.

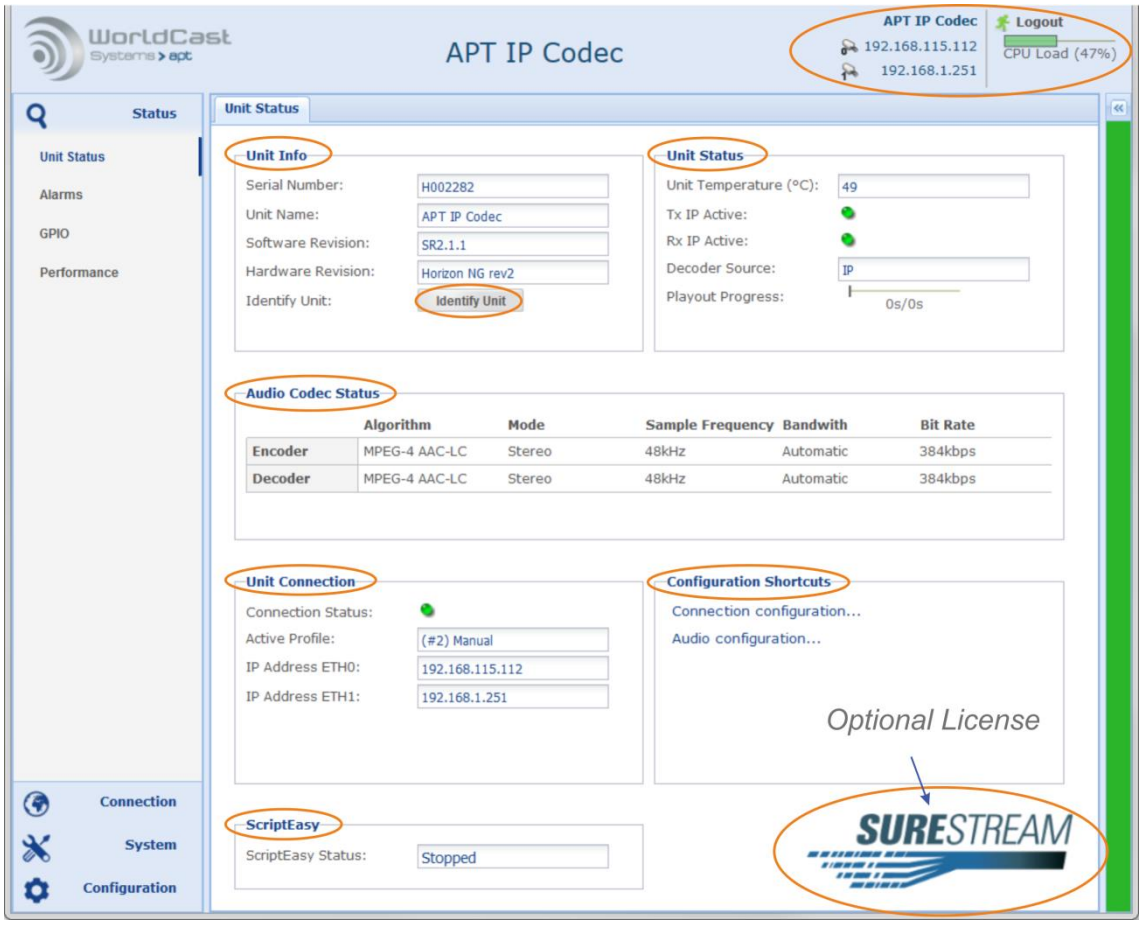


Figure 3-6: Main Menu Status - Unit Status page

Main Frame

In the upper right corner of the main browser frame, you can find the IP address of ETH0 and ETH1, 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 for two reasons; the emitted noise and fans are wear and tear items which need to be replaced periodically.

- IP Transport Status

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.

- Decoder Source

The Decoder source can be data from the IP stream (normal mode) or "SD Card". SD Card means that the decoder is decoding a backup file from this storage. Possible options are "IP", "IP/SD Backup" and "SD Card".

- Playout Progress

The playout progress bar displays the duration of the selected audio file on the SD card in seconds and the current progress (in seconds).

Audio Codec Status

The APT IP Codec can be setup for asymmetric audio operation. This section provides information about the currently active Codec configuration for the Encoder and the Decoder.

Unit Connection

This section shows the currently active connection, i.e. the status, the name of the currently loaded profile and the IP address of both Ethernet ports (ETH0/ETH1). The stylized LED also indicates any network related error on any active IP interface if a stream is assigned to the interface

Configuration Shortcut

This section provides direct links to:

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

Optional Licenses Information

Depending on the applied options licenses, this page also shows status information about these options, e.g. for SureStream the SureStream logo.

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 a popup window.

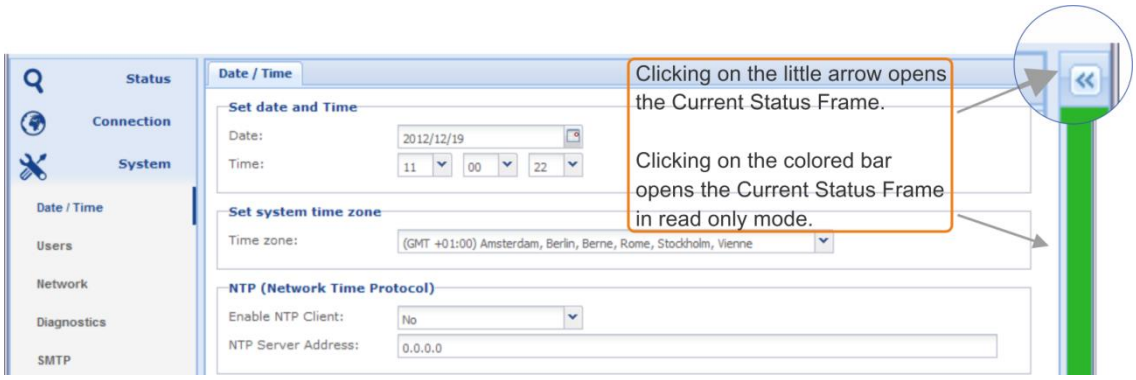


Figure 3-7: Two methods to open the "Current Status" frame; as a re-sizable (read-only) pop-up or with a fixed size and editable.

ⓘ *Note: 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 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)

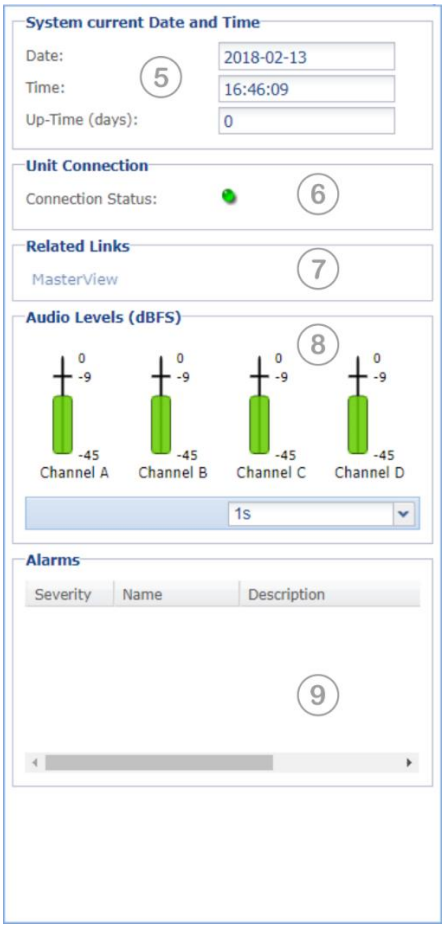
If a ScriptEasy application is loaded, this link to MasterView becomes active. It opens MasterView in a new browser tab.

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. If the second PSU fails, it will rise as a warning and show a yellow alarm.

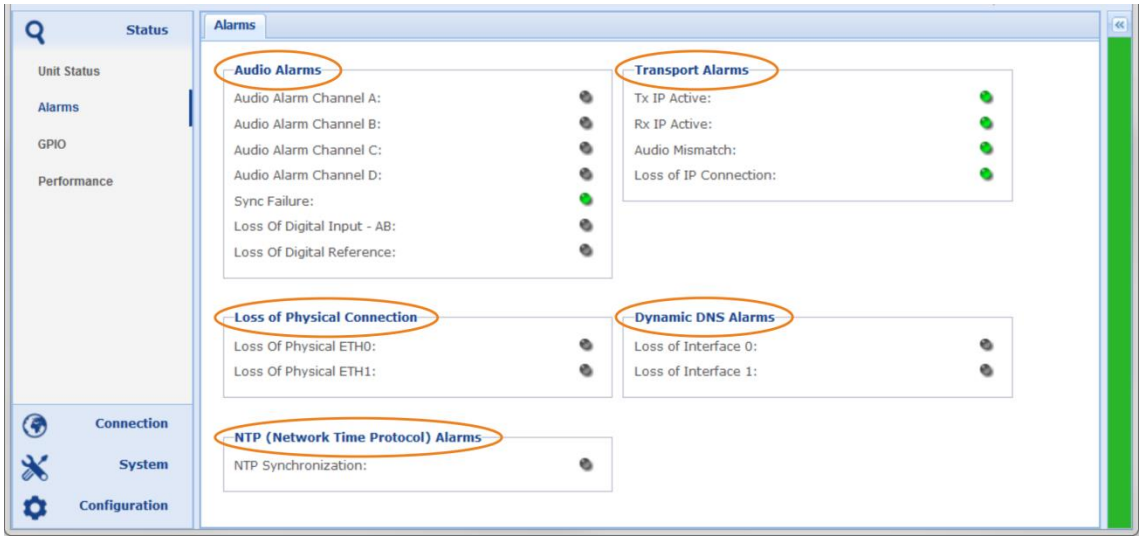


Figure 3-8: Main Menu Status – Alarms page

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 A/B/C/D, Sync alarm, Loss of Digital Input, Loss of Digital Reference, Audio Mismatch and I/O Card (rear panel) detection.

Audio Alarms (Silence Detection)

The Audio signal has decreased below the threshold and 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 on the TX side, 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

Status- Alarms Page (*continued*)

- **Loss of Digital Input**

This alarm indicates the loss of the AES input signals A/B.

- **Loss of Digital Reference**

This alarm indicates the loss of the external AES clock.

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**

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 co-dec.

- **IP Receive (Rx) Error**

Packets are not arriving at the Codec, and it is expecting to see traffic. This can be caused by stream being dropped on the Transmit Codec, a network fault or mismatch in audio algo-rithm 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).

ⓘ *Loss of IP Connection is the only Alarm that triggers the audio backup from the SD card.*

3.3.2.3 Loss of Physical Connection (ETH0/1)

Physical loss of connection to the network on ETH0 or ETH1 (CAT 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 GPIO Status

The following screen shows the GPIO switch and relay status.

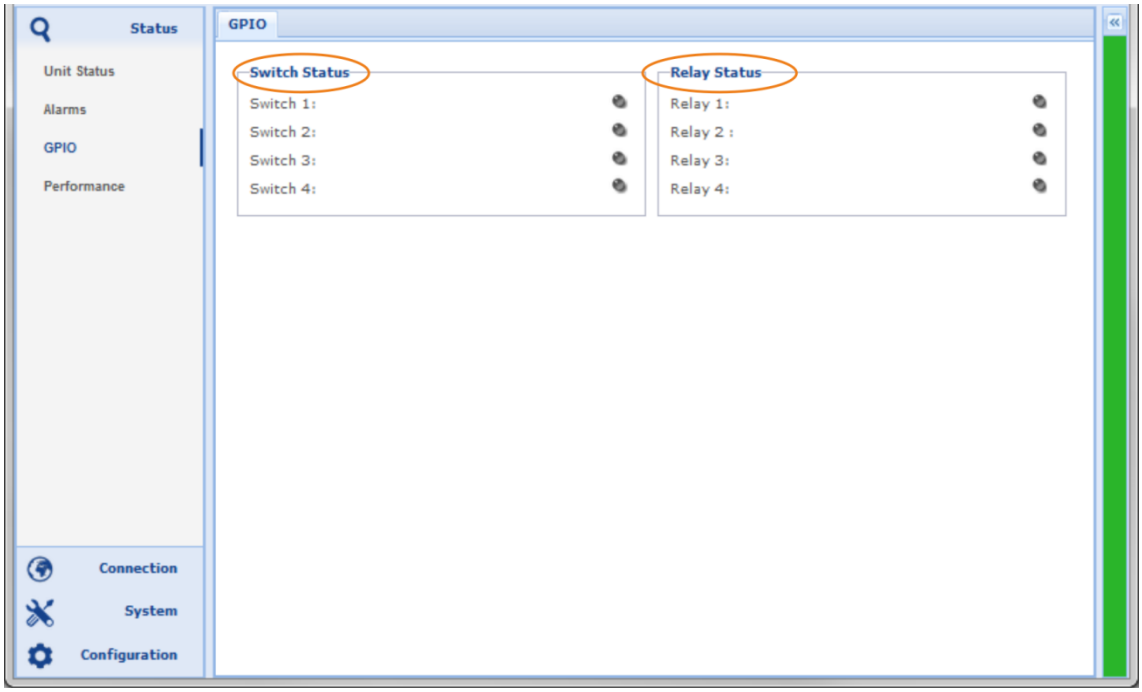


Figure 3-9: Main Menu Status - GPIO page

Switch Status

This section displays whether the switch input is active by showing a green LED on the particular switch. Grey the switch input is inactive.

Relay Status

This section displays whether the relay is active by showing a green LED on the particular relay number. Grey means the relay is inactive.

ⓘ *Note, an inverted relay output shows a green LED (refer to section 3.6.4).*

3.3.4 Stream Performance Monitor

The Performance Monitor is for all active transmit and receive streams. Clicking on an individual stream in the Stream Performance Table will display the performance details below the table. Depending on the selected stream type, the IP statistics displays transmit or receive or both values.

The time interval for the data update is set to 1 second by default, but it is user selectable from 10s to 500ms. 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."

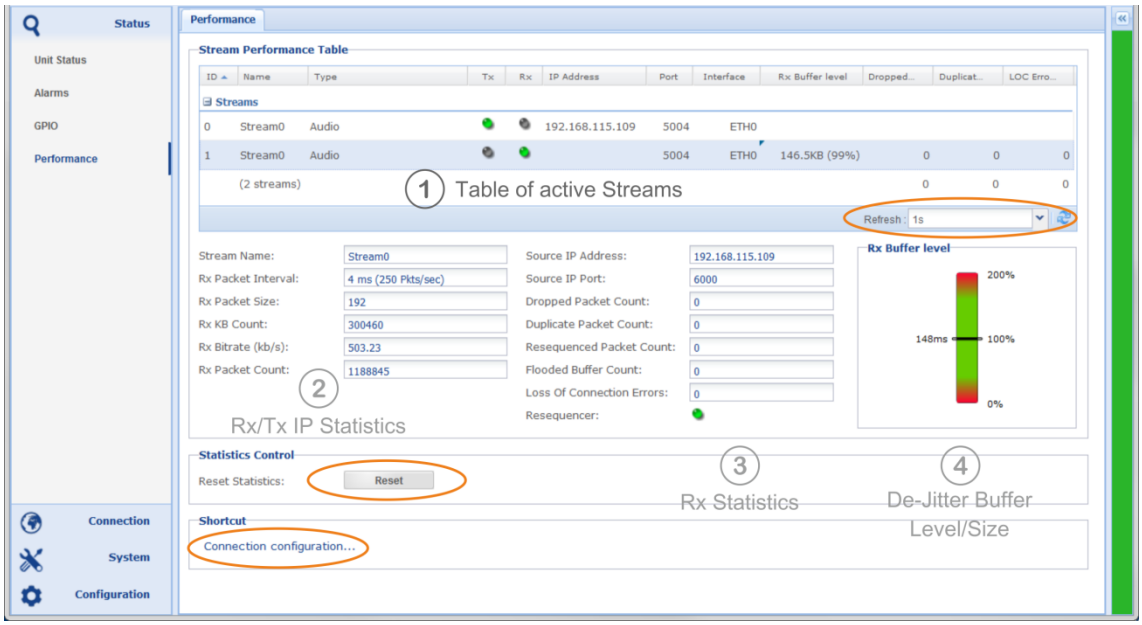
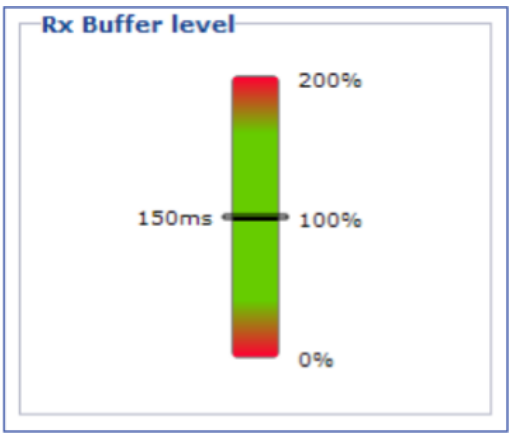


Figure 3-10: Status Menu - Performance Monitor page of an Rx stream

3.3.4.1 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 maker 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 midpoint.

A high deflection of the level marker indicates that the nominal buffer level may be too low. Increasing the nominal level reduces these deflections.

3.3.4.2 IP Statistics – Details

This section shows the IP statistics (2) & (3) of Figure 3-10 of a selected stream. The table below provides the description of each of the statistics.

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	A 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)

Statistics records can be reset by clicking on the "Reset" button (refer to Figure 3-10).

3.3.4.3 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 (also refer to section 3.4.10 pos. 14); the re-sequencer is always enabled. Even with a validation warning, the Resequencer stays active.

3.3.4.4 About Streams Tables (general)

In general, a Stream Table (1) 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.

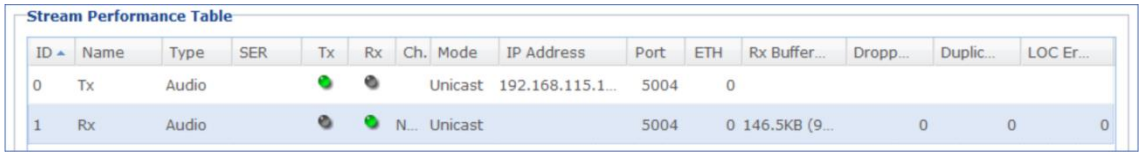


Figure 3-11: Shows a Stream Table with two active streams in read-only mode (Performance Monitor)

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.

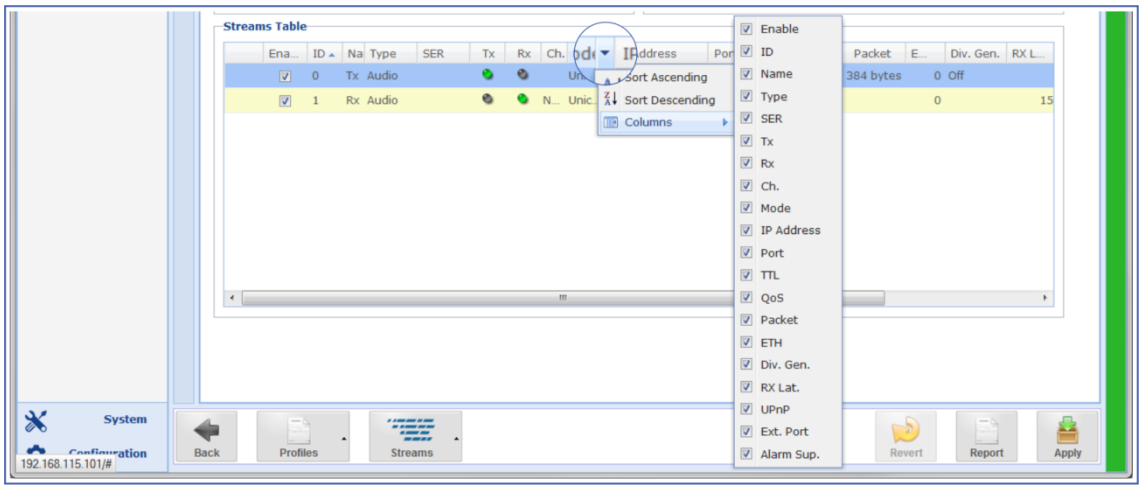


Figure 3-12: Exposure options on the Streams Table (connection page)

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. The connection profile stores Codec, and IP streams settings.

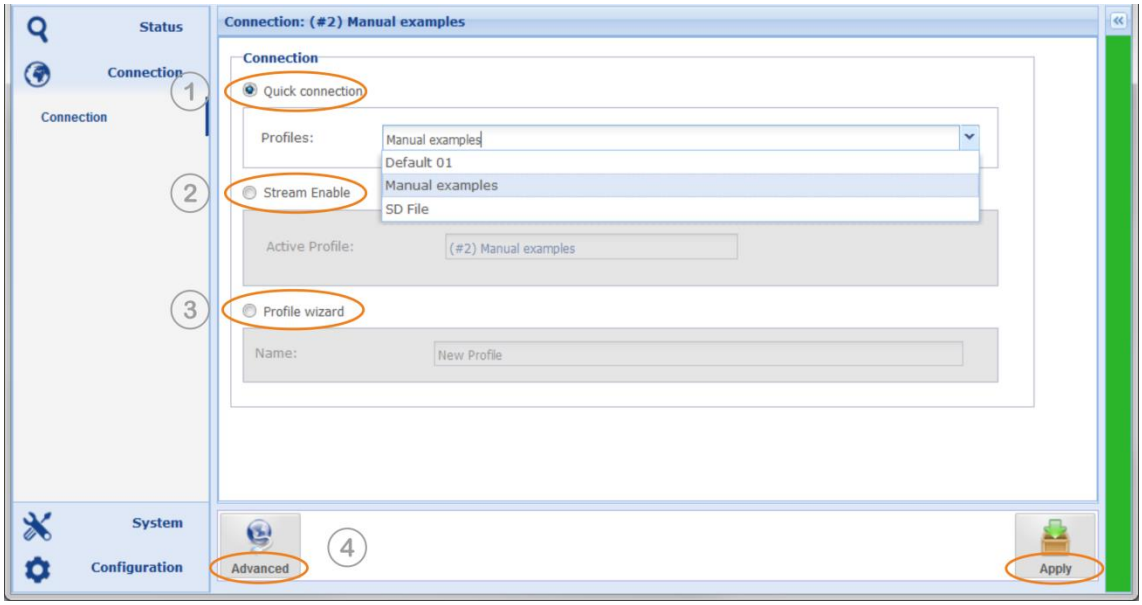


Figure 3-13 shows the Connection Page with all options

The WEB GUI offers three ways to create, manage and to apply a Connection Profile:

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

ⓘ *Note: All changes made on the WEB GUI can be reverted and will not become active until it was applied to the Codec hardware!*

Connection Page (continued)

Quick Connection (1)

A "Quick Connection" is a pre-configured and previously stored profile. This profile was created and merged from a Codec 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, it can be applied seamlessly to the Codec by clicking the "Apply" button in the bottom right corner.

Stream Enable (2)

This section allows enabling or disabling every single stream of the active profile. The profile on the screen shot below has two streams. Clicking on the "Push to Enable" / "Push to Disable" button enables or disables this stream immediately. It is not necessary to apply this change; therefore, the "Apply" button disappears for this function.

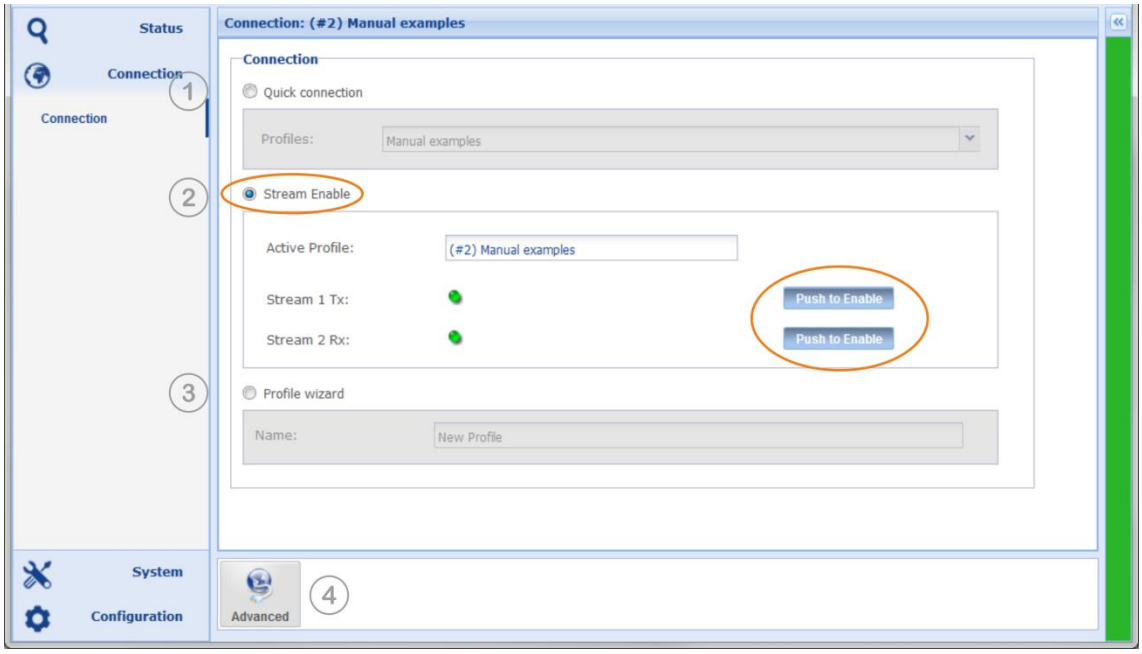


Figure 3-14 shows the Connection Page – Stream Enable

Profile Wizard (3)

The "Configuration Wizard" guides the user through a step-by-step procedure to create a connection profile; once a profile is created it appears on the Quick Connection drop down list.

Advanced Configuration (4)

The "Advanced" configuration procedure provides all configuration and management options on a single page. Unlike the Configuration Wizard, the "Advanced" configuration allows modifications on the currently active profile and configuration. It also provides choices and tools to edit already created profiles.

3.4.1 Profile Wizard – Creating a Profile

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.

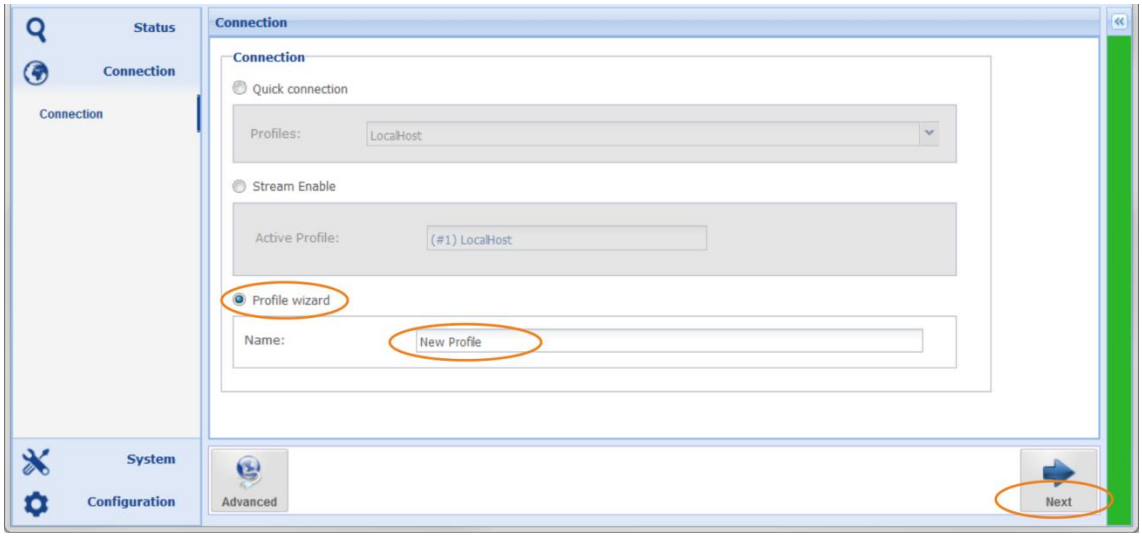


Figure 3-15: Shows the Profile Wizard's first page

Notes:

3.4.2 Profile Wizard – Encoder Settings

The next page guides the user to the Audio Codec settings. The IP Codec allows asymmetric audio configurations. Hence, separate Encoder and Decoder configuration pages are provided. These Codec settings allow configuring simplex modes as well (i.e. dual encoding or dual decoding). If a simplex mode is selected, this page shows dual Encoder or dual Decoder settings.

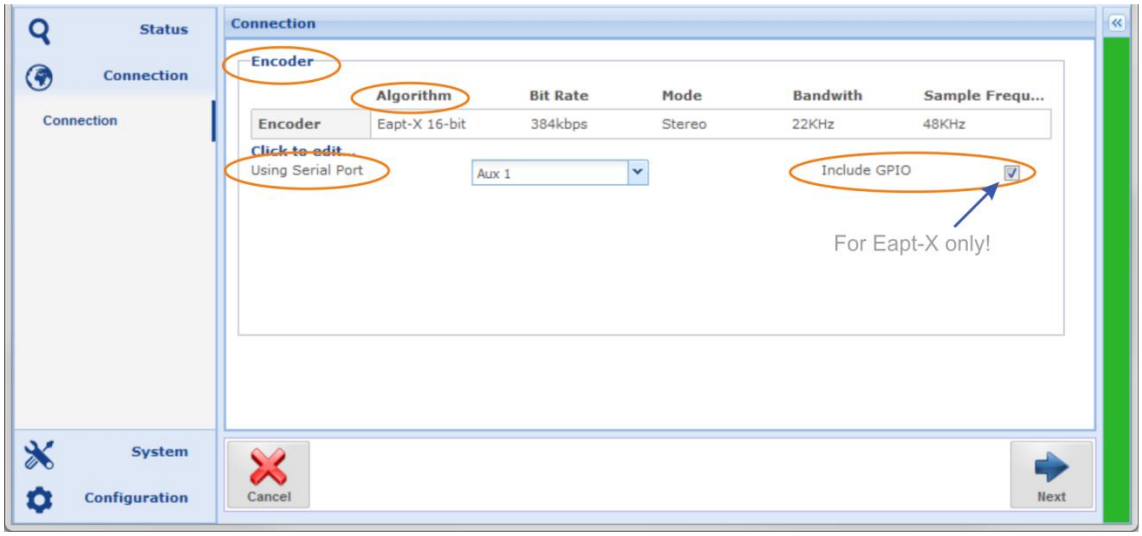


Figure 3-16: Encoder options of the profile wizard

3.4.3 Embedded AUX Data

Serial Aux data can be embedded in the Audio Data Stream. For most audio algorithms (except Liner PCM) auxiliary data can be embedded. Once an audio algorithm is selected and configured, the Serial Port drop-down list becomes active. The embedded data channel accepts RS232 data up to 9600Baud. Audio algorithms may have baud rate constraints depending on the selected audio bit rate.

Include GPIO

This checkbox is available for aptX® Enhanced only and, if checked, it includes the GPIO signals into the second embedded data channel.

Only aptX® Enhanced provides a second data channel for GPIO signals

Profile Wizard – Encoder Settings (continued)

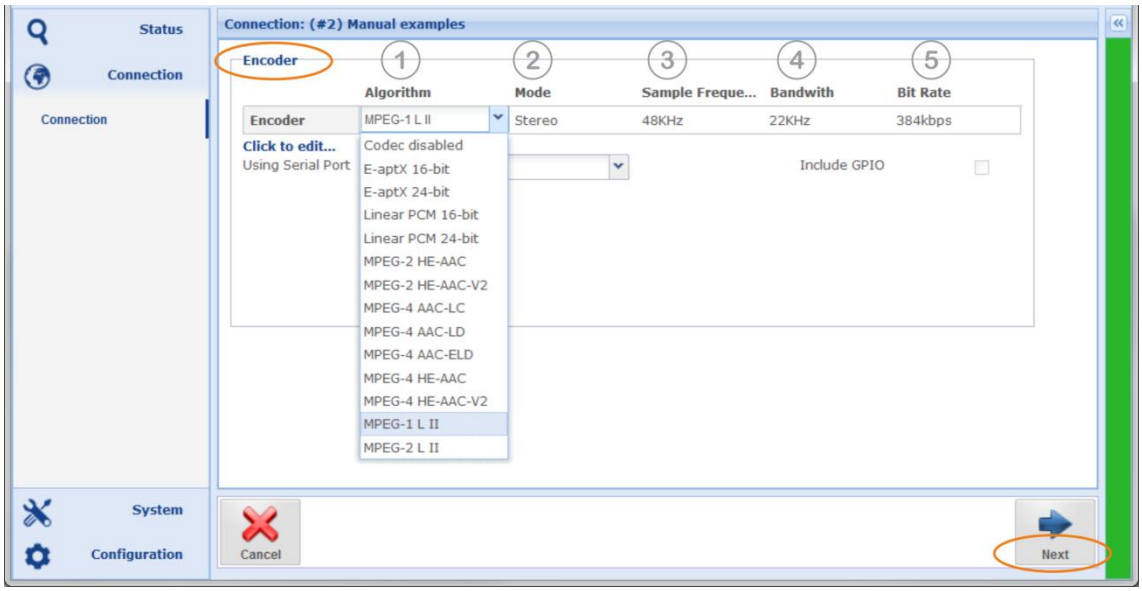


Figure 3-17: Shows the Encoder configuration page

(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.

Notes:

3.4.4 Profile Wizard – Decoder Settings

Once all parameters for the Encoder part have been set, click on the "Next" button to enter the configuration page for the Decoder path (if the duplex mode was selected). The principle of the Encoder and Decoder configuration is almost identical.

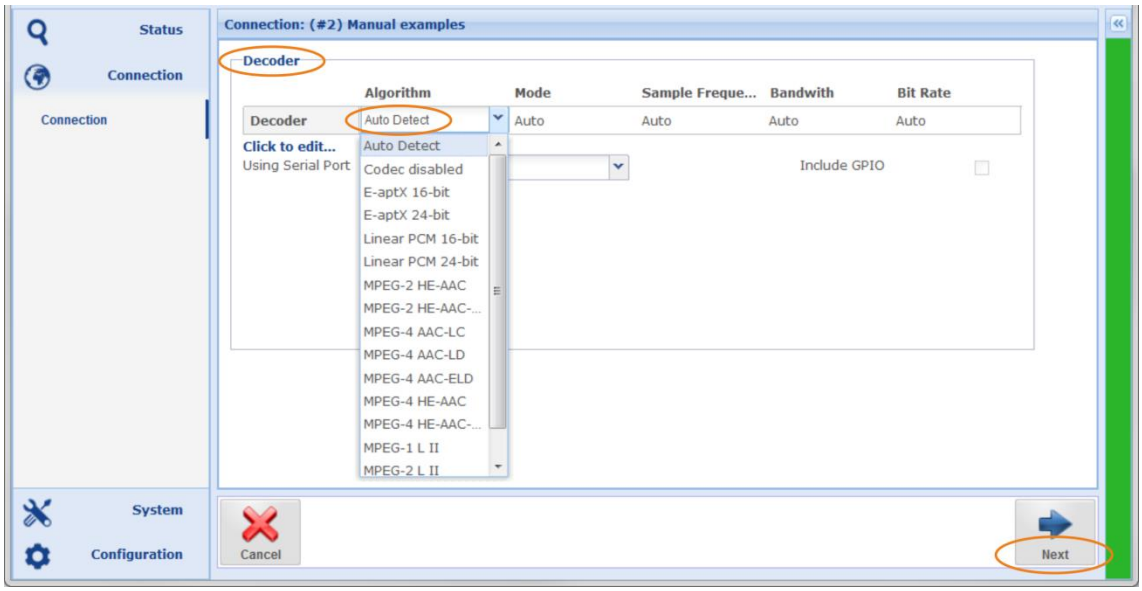


Figure 3-18: Shows the Decoder configuration page

3.4.4.1 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.

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

Notes:

3.4.5 Profile Wizard – IP Streams Configuration

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

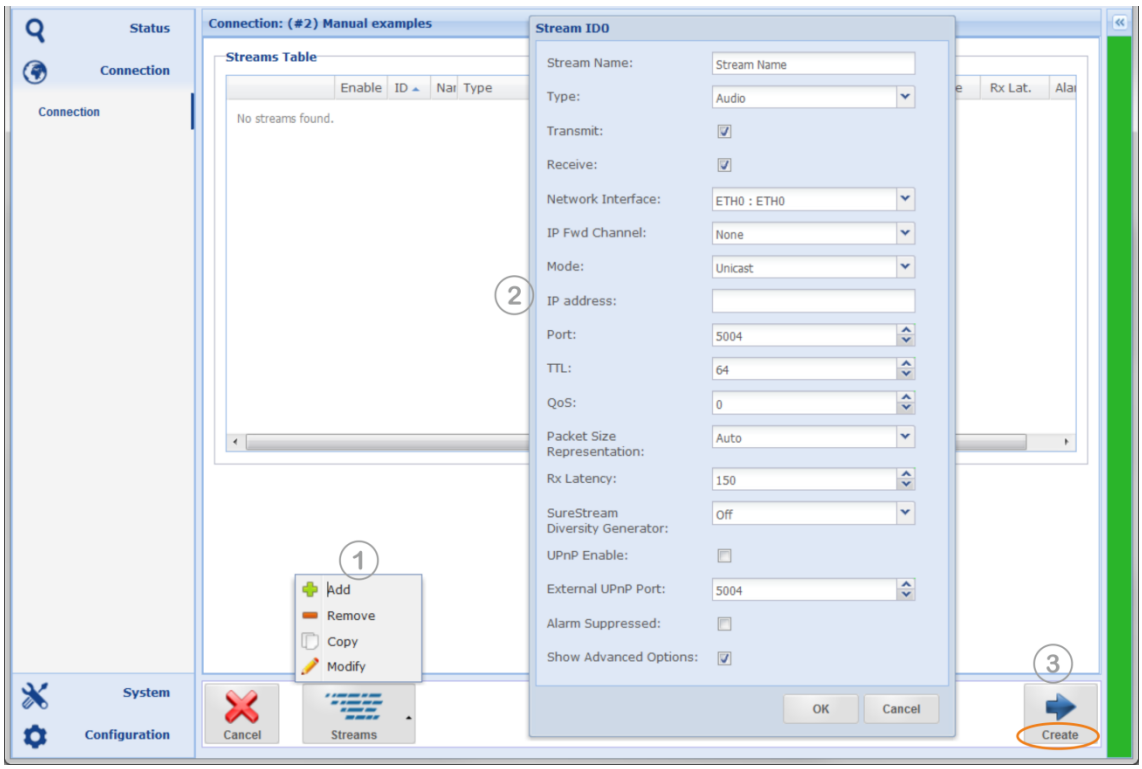


Figure 3-19: Shows the IP Stream configuration page with the stream setup window open

From the audio settings page, the Wizard first presents an empty stream table.

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 stream 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.

Clicking on the "Cancel" button, deletes all configurations including the audio settings and the profile name.

3.4.6 Profile Wizard – Saving a Profile

After all desired streams are created; they appear on the Streams Table. The little blue marker on the table fields indicates that the configuration was not yet saved in a profile and can still be modified.

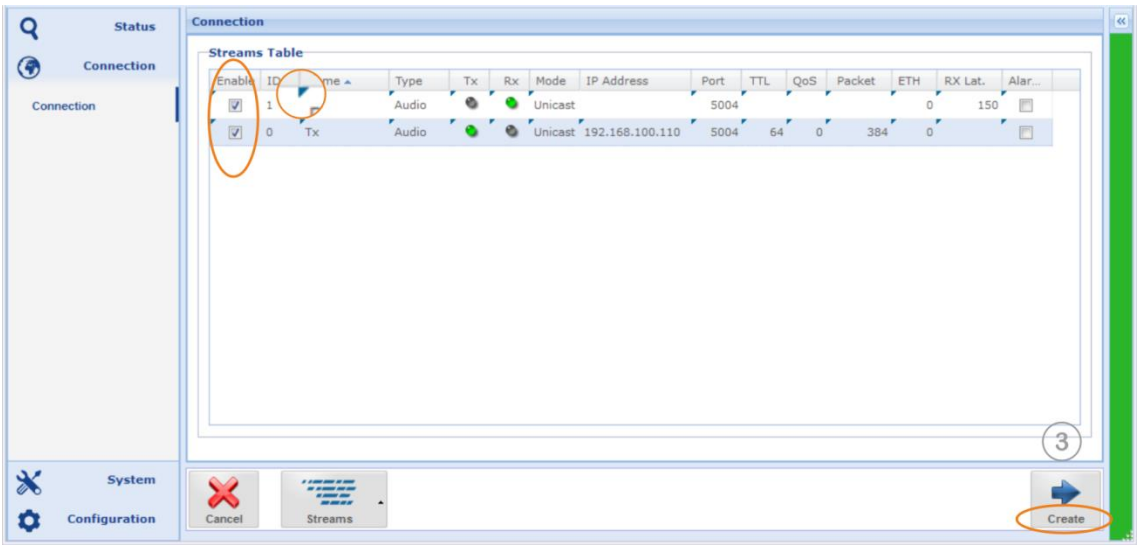


Figure 3-20 shows two streams ready for being merged into a profile

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.

ⓘ *The "Advanced" configuration page (section 3.4.16) provides all options on a single page. A shortcut link on the status page opens the advanced configuration page directly.*

Notes:

3.4.7 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.

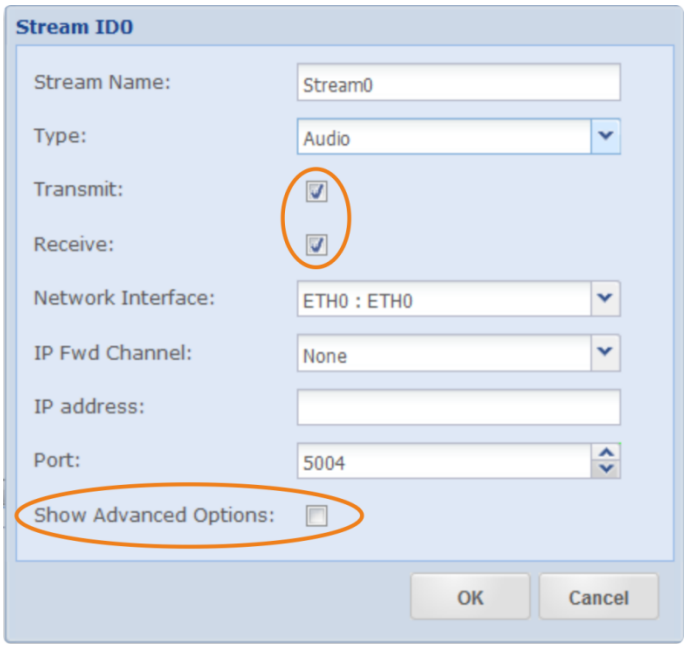


Figure 3-21: Shows the basic configuration options for Audio streams

Enabling the "Show Advanced Options" tick box expands the configuration window presenting all stream options.

ⓘ *Note: Depending on the selected stream type, the options provided are different.*

3.4.8 About Stream Types

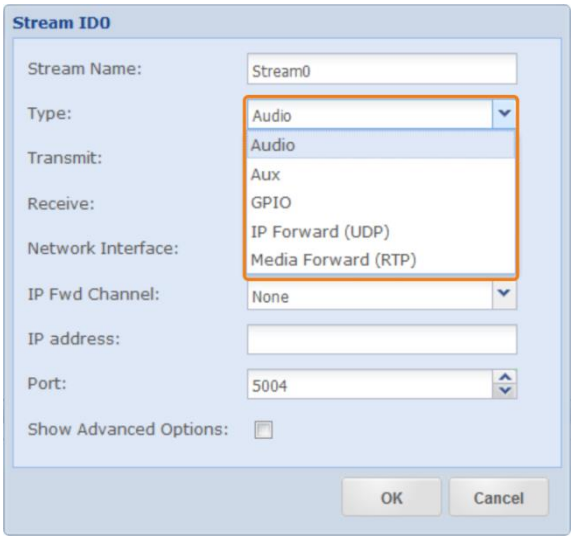


Figure 3-22: Shows the stream type selection menu

Audio Stream

Audio streaming via RTP/UPD; the possible streaming modes are:

- Simplex (Rx or Tx)
- Duplex (Rx AND Tx)

AUX Data Stream

AUX data streaming (data from Rs232) as UDP stream; this is different from the RTP/UDP mode of audio streams. An AUX stream does not pass the de-jitter buffer on the receiving decoder, and packets have no sequence numbers. Due to this fact, an AUX data stream is not exactly synchronized with the audio content – it is always a bit faster than the audio by the amount of time of the de-jitter buffer size.

- Simplex only (Rx or TX)

GPIO Stream

This stream type is the same nature of the AUX Data stream.

- Simplex only (Rx or TX)

Packet Forwarding

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

The possible streaming modes are:

- Simplex or duplex
- IP Forwarding (UDP)
- Media Forwarding (RTP)

3.4.9 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).

3.4.9.1 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 Codec)
- IP Forward Transmit (stream sent from the Codec)

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.

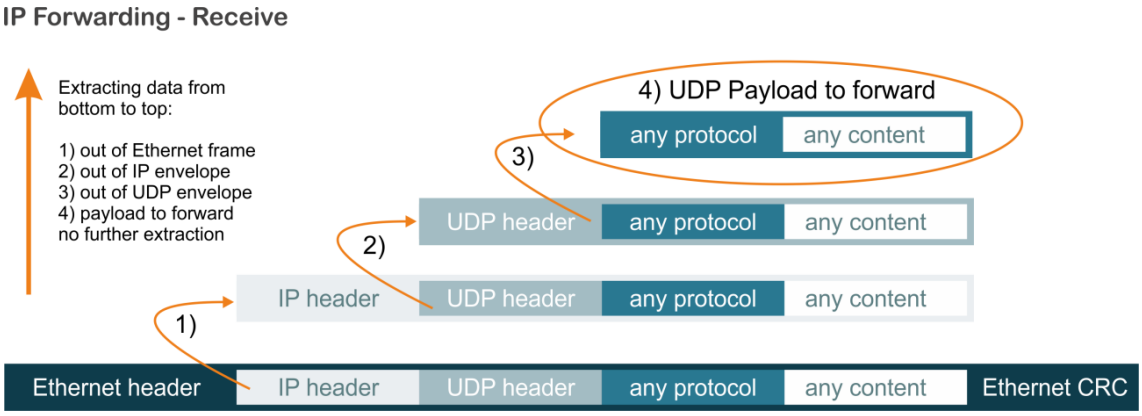


Figure 3-23: Shows how "IP Forward receive" extracts the payload of a receiving stream from the bottom to the top of the image - this mode is payload agnostic.

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 received data to the destination.

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

In case the link is a duplex link, the IP Forward "Transmit" method returns the UDP stream to the originator on the Encoder site.

The encapsulation process flows from the top to the bottom.

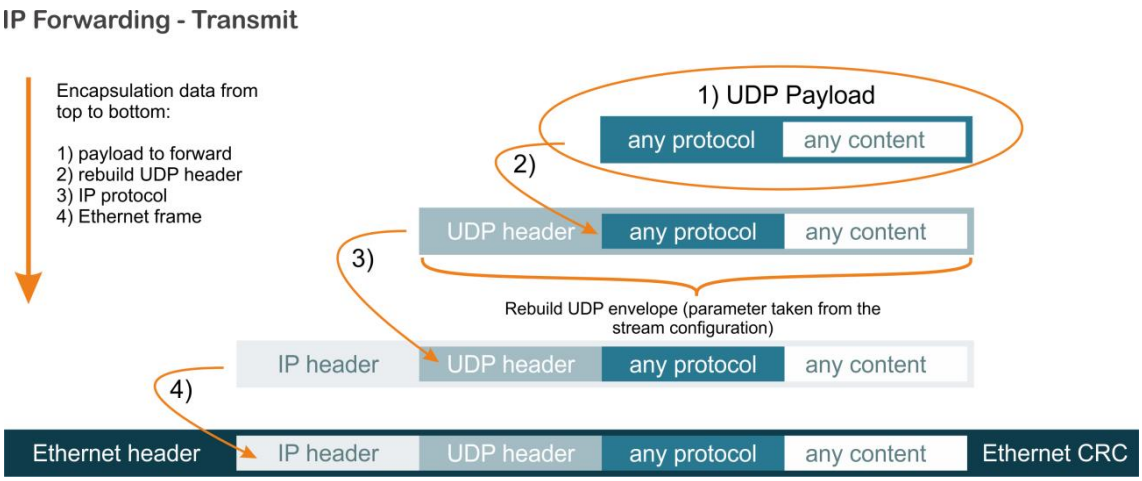


Figure 3-24: Shows how IP Forward "Transmit" encapsulates the payload on a transmit stream from the top to the bottom of the image.

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

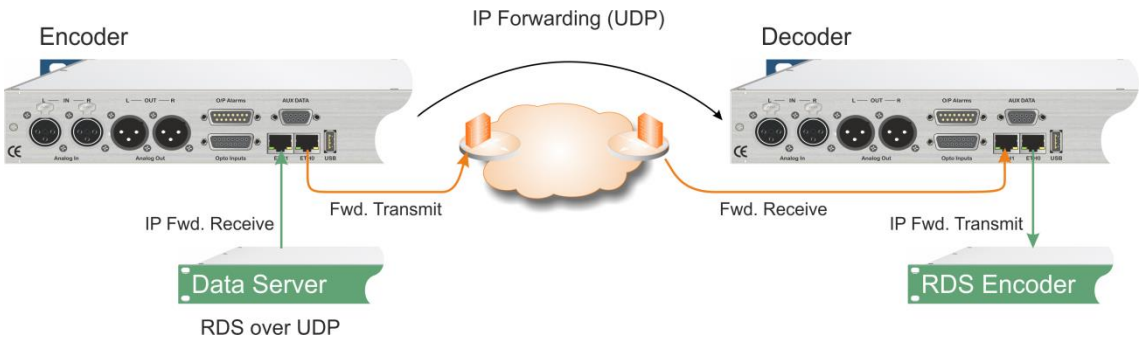


Figure 3-25: Shows an example of IP Forwarding for RDS data over UDP.

3.4.9.2 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.

- Media Forward Receive (stream received at the Codec)
- Media Forward Transmit (stream sent from the Codec)

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 3.4.9.

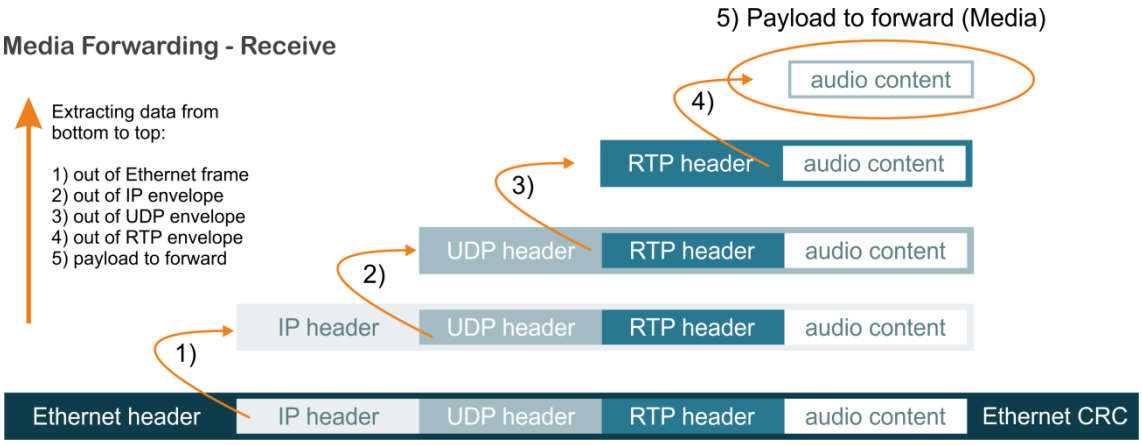


Figure 3-26 shows how Media Forward "Receive" extracts the payload on a receiving stream from the bottom to the top of the image - this mode is payload agnostic.

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).

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 3.4.9.

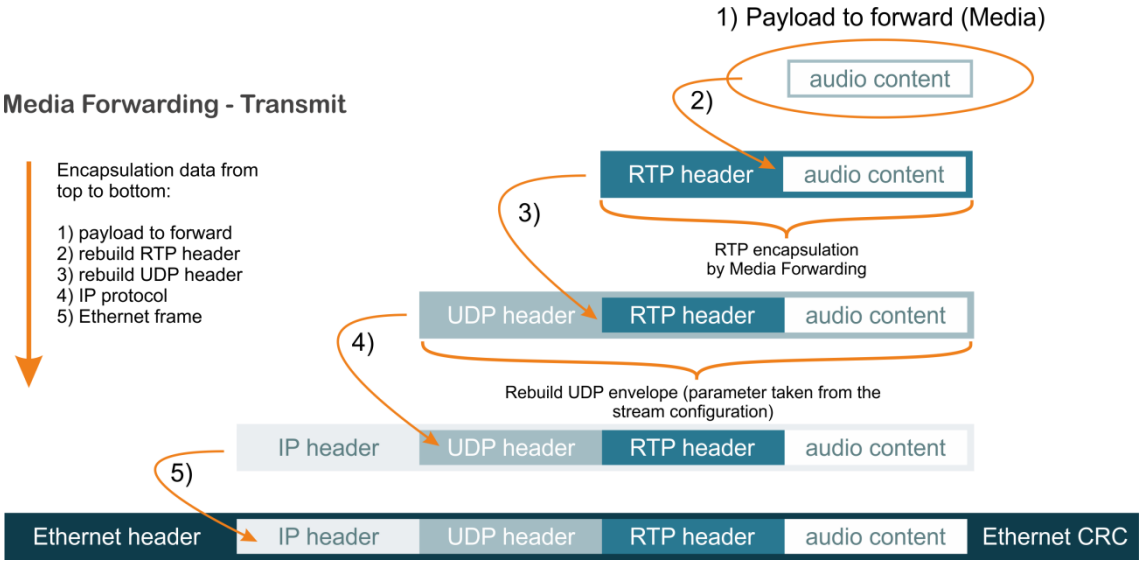


Figure 3-27: Shows how Media Forward "Transmit" encapsulates the media payload on a transmit stream from the top to the bottom of the image - this mode is payload agnostic.

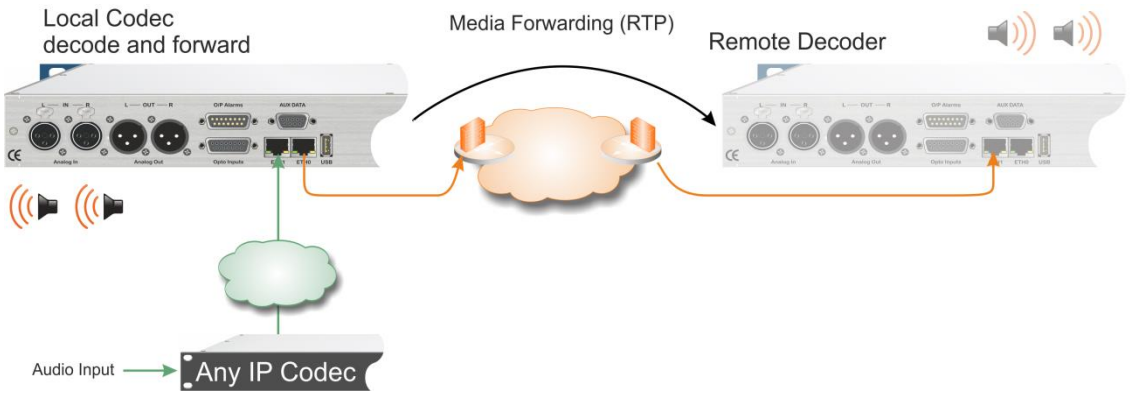


Figure 3-28: A typical Media Forward Transmit application with local content decoding (on local Codec).

3.4.9.3 UDP/RTP Re-Encapsulation

The combination of IP Forwarding and Media Forwarding allows the re-encapsulation of UDP data into the RTP protocol. In this way, the benefit of the RTP protocol can also be made available for non-audio data. These are packet sequence numbering, time stamping, and the redundant streaming as well as re-sequencing of the packet order and passing through the de-jitter buffer.

- Enc. - IP Forwarding Rx: UDP header removed
- Enc. - Media Forwarding Tx: New UDP and RTP header added
- Dec. - Media Forwarding Rx: UDP and RTP header removed
- Dec. - IP Forwarding Tx: New UDP header added

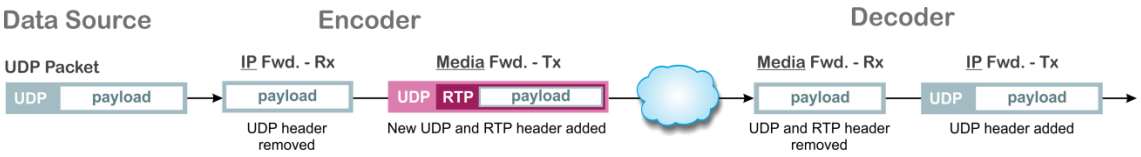


Figure 3-29: Shows the signal chain of re-encapsulated UDP data in the RTP protocol.

Notes:

3.4.10 Audio Stream Configuration

The following screen shots show all options for a bi-directional audio stream.

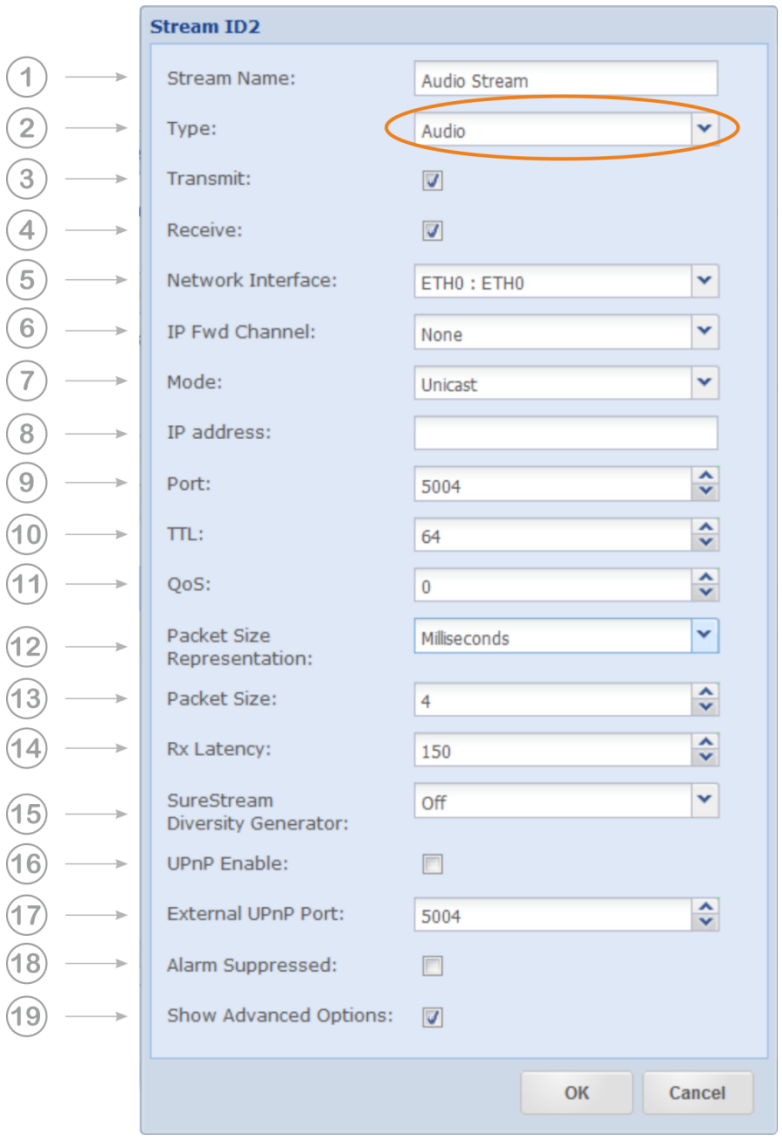


Figure 3-30: The IP Stream configuration window showing all available audio options

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

ⓘ *SureStream is a cost-option and will appear only if a license is applied to the Codec. For more details refer to the SureStream section 4.0 in this document. 4.0*

Audio Streams Configuration (*continued*)

1. **Stream Name:**
   Enter the name of this stream
2. **Type:**
   Selected Stream Type is: Audio
3. **Transmit or**
4. **Receive**
   or both for duplex. Note: Duplex mode usually allows passing an NAT gateway without any further configuration on the external gateway.
5. **Network Interface**:
   Select the network interface (ETH 0/1) or any pre-configured virtual interface for this stream. Both physical and all virtual interfaces can be used.
6. **IP 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.
7. **Casting Mode**:
   Unicast is a point-to-point connection. The stream can be received from one decoder only. The system allows the configuration of several unicast streams (multiple unicast).
   Multicast allows point-to-multi-point streaming and uses the IGMP protocol for managing multicast joins and leaves; IGMPv2 and v3 (SSM) is supported.
   SSM Multicast: (Source-specific Multicast) SSM has several advantages over "normal" Multicast architectures. An essential is the possibility to make a multicast group usable through several sources. With SSM, a receiver can receive the data from a specific source. The Multicast Source IP address must also be entered for this purpose. The Source IP Address input field appears only in the receiver mode and if SSM Multicast has been selected.
8. **IP Address**:
   Enter the destination IP address, the hostname or a keyword 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 3.5.4.4). For multicast: Enter the multicast group address.
9. **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 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.
10. **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 final destination, it will be deleted. This avoids flooding the network with "blind" packets.

Audio Stream Configuration *(continued)*

11. **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.

12. **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 1152Bytes when using digital MPX mode.

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

13. **Packet Size**:
    Packet size describes the size of the payload of 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.

14. **RX Latency**:
    This is the setting of the de-jitter buffer in Decoder Mode (Rx). 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.

15. **SureStream Diversity Generator**:
    This allows setting the diversity generator level for SureStream component streams in Encoder Mode (Tx). It should be used in situations where more than one component streams are connected to the same network via the same ETH port. This setting ensures that the diversity is maintained under this condition (refer to section: 4.1.4)

16. **UPnP Enable**:
    This check box enables the UPnP IGD "Internet Gateway Device" feature for this individual stream.

17. **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.

18. **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.

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

3.4.10.1 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.

3.4.10.2 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		
MPEG2/4 AAC LC	min. 21.3ms	variable
MPEG2/4 AAC LD	min.10.6ms	variable
MPEG2/4 AAC ELD	min.21.3	variable
MPEG2/4 HE AAC	min.42,6	variable
MPEG1 Layer II	min.24ms	variable
MPEG2 Layer II	min.48ms	variable

3.4.11 IP Address Keywords

These keywords must be used instead of a destination IP address in the streams table.

3.4.11.1 Local Loopback IP Address

With "**localhost**" the unit can resolve the local IP address of the selected interface by using this keyword as the destination address of the Tx stream. This feature allows a quick check of configurations by streaming to the local address; that equals a local IP loop.

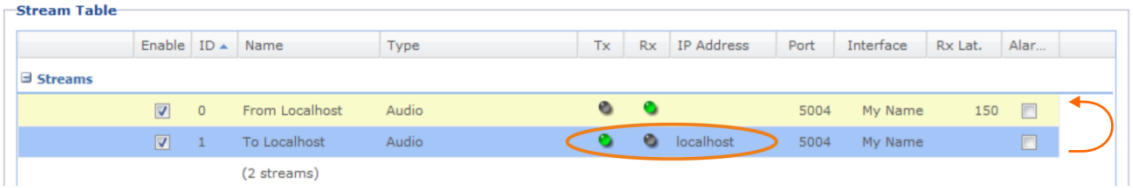


Figure 3-31: Shows an example of the Keyword "localhost" is the IP destination

ⓘ *"Localhost" keyword works on ETH0 and ETH1, but on Tx streams only (works not on bi-directional streams).*

IP Address Keywords (*continued*)

3.4.11.2 Reply to Sender

The keyword "**SENDER**" (Sender, sender) entered in the destination IP address field of a bi-directional stream configures the Tx path of the receiving codec from the originator source address. This configuration updates the destination IP address dynamically.

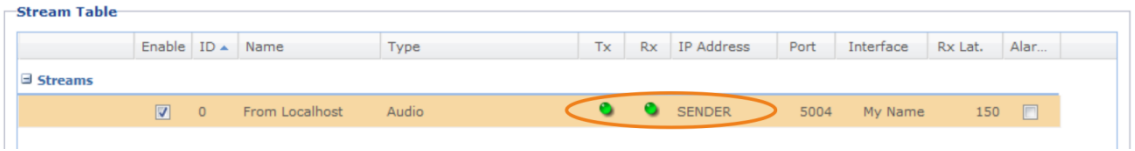


Figure 3-32: The Keyword "SENDER" is the IP destination

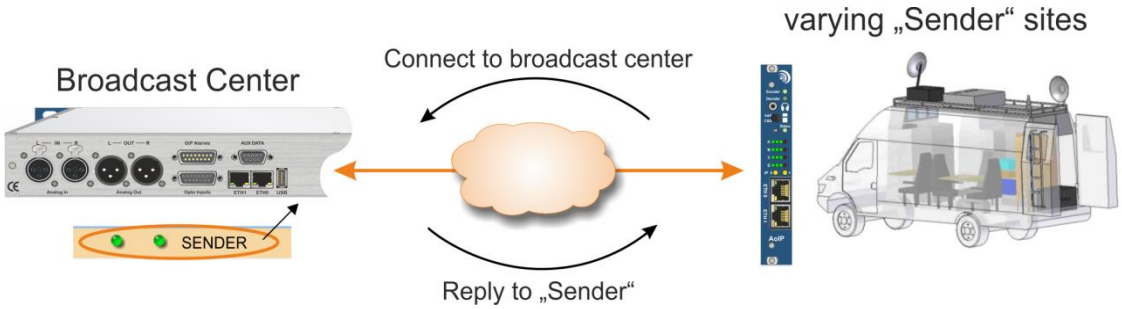


Figure 3-33: Shows a typical application with varying remote sites – "SENDER" will reply to the current sender address automatically.

Notes:

3.4.12 AUX Data and GPIO Stream Configuration (Tx/Rx)

Creating an AUX or GPIO data stream follows the same principle as described for the audio stream. An Aux data stream is a UDP stream sending or receiving the RS232 or GPIO data. A GPIO stream sends the switch commands or receives commands and triggers the corresponding relays – the options on the configuration window are the same for both data types.

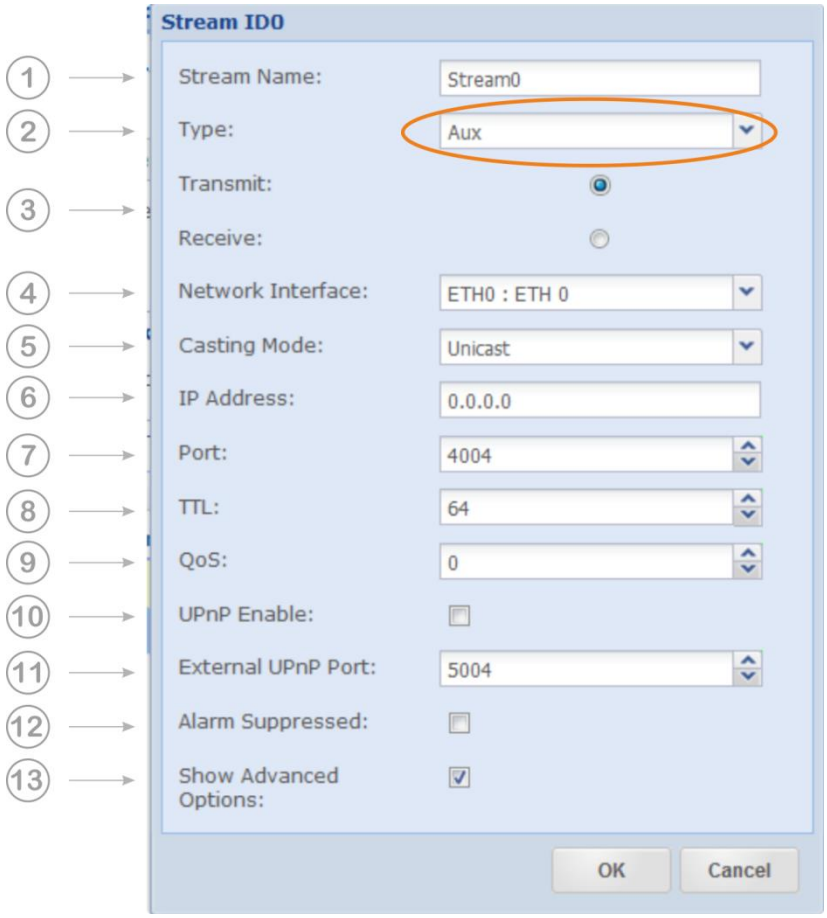


Figure 3-34: Shows the configuration options for AUX or Opto/Relay streams

AUX Data or GPIO Stream Configuration *(continued)*

1. **Stream Name**:
   Enter the name of this stream
2. **Type**:
   Select Stream Type AUX or GPIO (Opto/Relay)
3. **Mode: Transmit or Receive** (no duplex mode possible)
4. **Network Interface:**
   Select the network interface (ETH 0/1) or any pre-configured virtual interface for this particular stream. Both physical and all virtual interfaces can be used.
5. **Casting Mode:**
   Unicast is a point-to-point connection. The stream can be received from one decoder only. The system allows the configuration of multiple unicast streams.
   Multicast allows point-to-multi-point streaming and uses the IGMP protocol for managing multicast joins and leaves.
6. **IP Address:**
   Enter the destination IP address or the hostname of the remote unit (Tx). 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 3.5.4.4). For multicast: Enter the multicast group address. If Multicast is selected for the Rx stream, the multicast group address must be entered.
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 final 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 or GPIO 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 particular 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 and GPIO 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 ms.

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.

UDP packets for GPIO data are sent every 15 ms with a fixed amount of data therein. This size and packet interval is not configurable.

Notes:

3.4.13 Audio Stream Forwarding

The principles of Stream Forwarding is described and discussed in section 3.4.9.

3.4.13.1 Audio Stream Receive, decode and prepare Forwarding

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

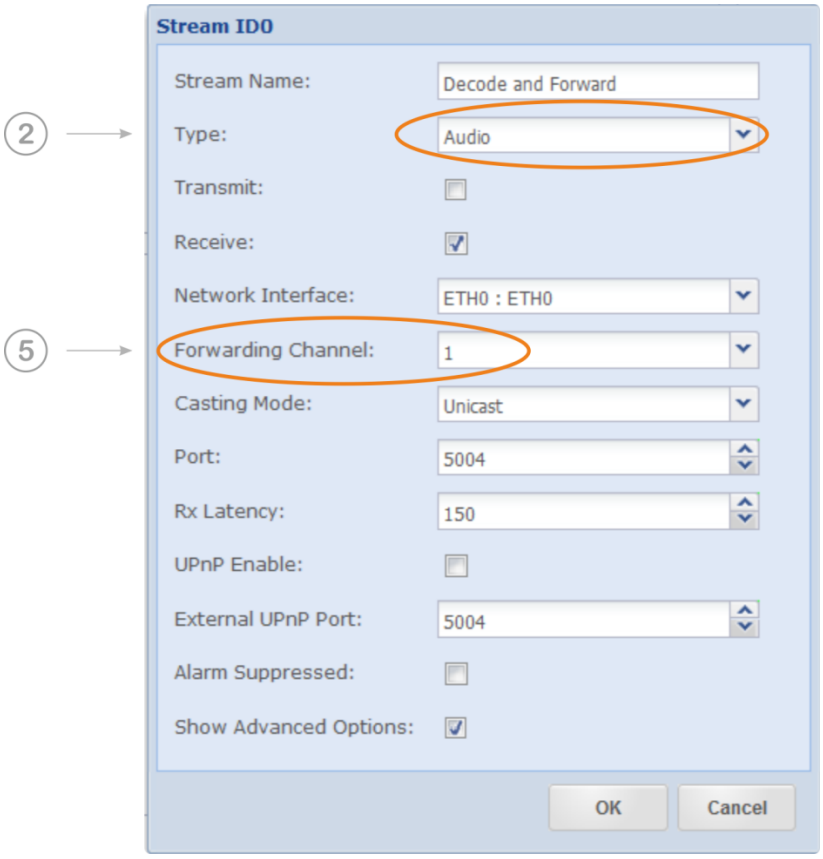


Figure 3-35 shows the configuration options for local Decode and Forward

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 3.4.10).
- (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 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 Forwarding must be chosen to forward the audio in RTP packets.

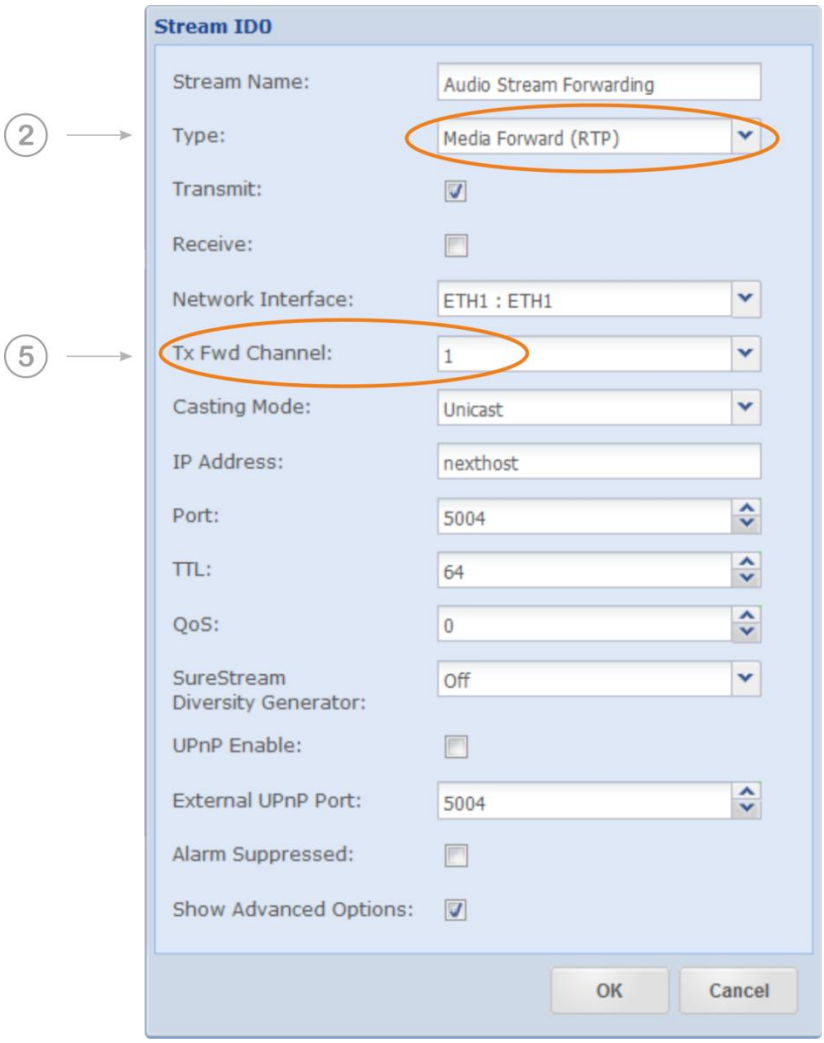


Figure 3-36 shows the configuration options for IP Forwarding

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

- (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 3.4.10).
- (5) There are six Forwarding channels available; select one channel for this stream.

For Stream Forwarding (RTP and UDP), 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, Codec A is configured as shown in Figure 3-35 (Rx) and Figure 3-36 (Tx). Codec A receives an audio stream from the network, decodes it and makes it available for Media Forwarding to any other remote site.

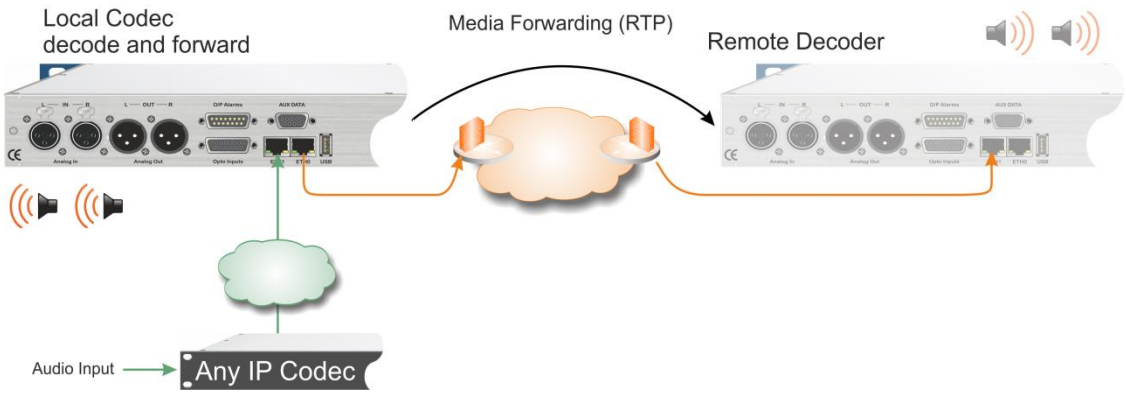


Figure 3-37: Shows the application of Media Forwarding (RTP)

3.4.14 IP Stream Forwarding (UDP)

The principles of Stream Forwarding are described and discussed in section 3.4.9.

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.

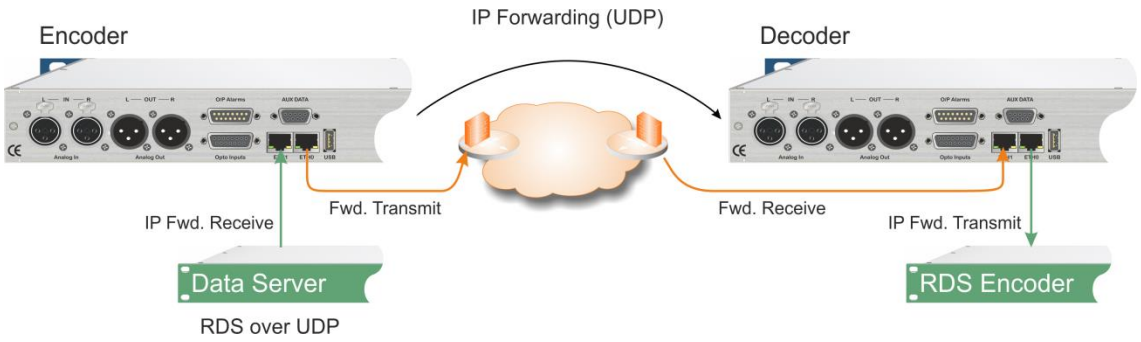


Figure 3-38: Shows a typical application for non-audio data forwarding

3.4.15 Combination of UDP/RTP Forwarding

The principle of UDP/RTP re-encapsulation is described in section 3.4.9.3.

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

The application below shows how a Digital Radio signal contribution through the IP Codec can look like (this is the same principle for DAB or HD Radio).

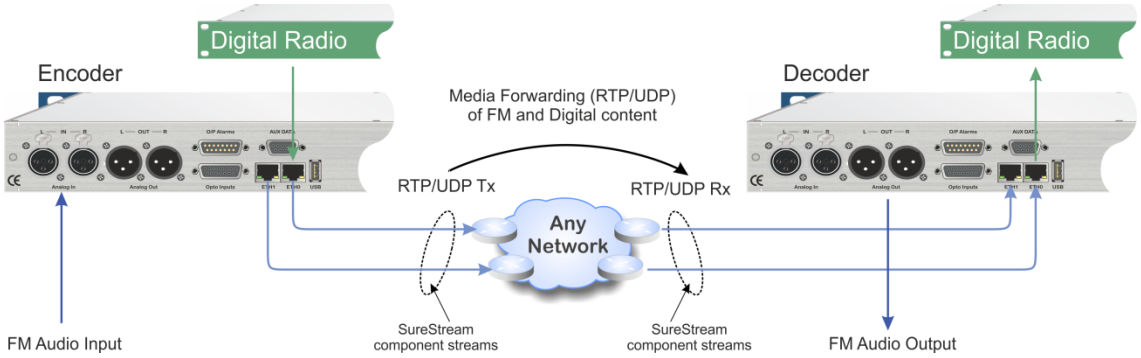


Figure 3-39: This example shows the FM Audio Input and the Digital Radio data streams protected by SureStream

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).

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.

3.4.16 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.

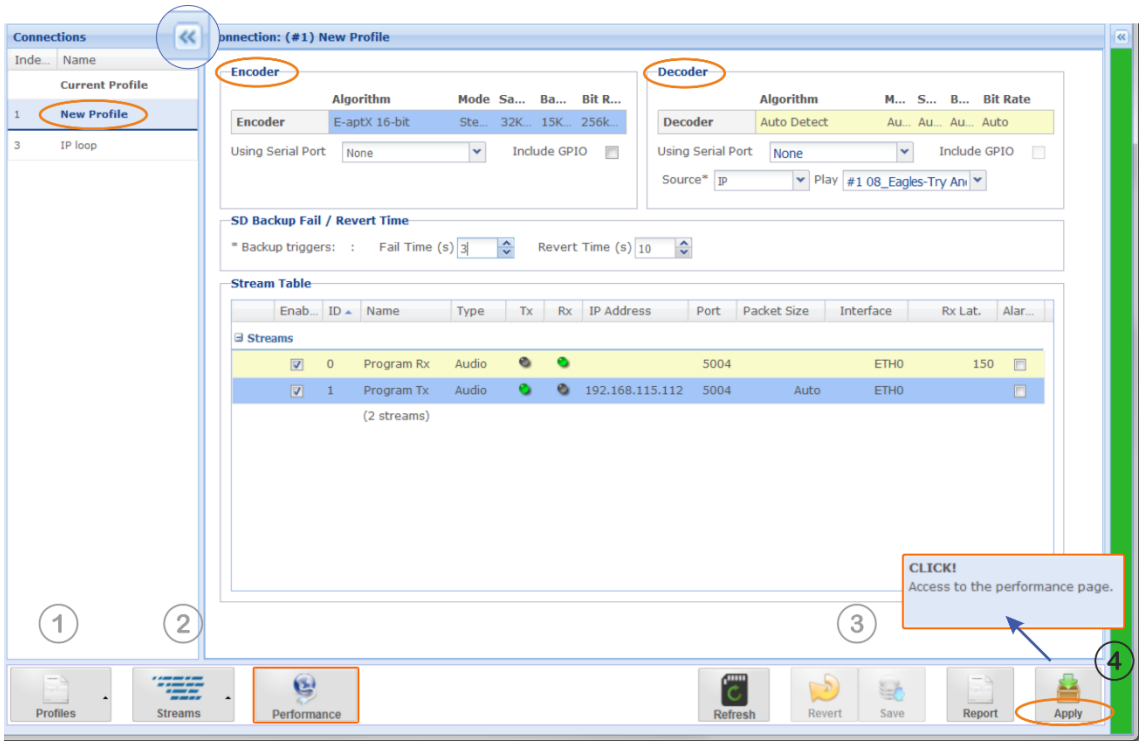


Figure 3-40: Shows the Advanced configuration window

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 on top of the list of profiles on the left-hand side (Current Profile). This list of profiles is also accessible with the "Quick Connection" tool. A click on the little arrow on top closes the profile list.

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

Current Profile

"Current Profile" shows the currently active profile name. On the example of Figure 3-40, the current profile is "New Profile". Clicking on the headline "Current Profile" shows the currently applied profile on the configuration page in read-only mode (no toolbar items provided).

Clicking on "New Profile" in the "Current 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 supported. 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 (appears if any profile was edited but not the "Current Profile"). This action does not affect the actually 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.*

3.4.16.1 SD Card – Audio Backup

This backup feature is part of a second level redundancy and provides an audio program stored on the SD card. The advanced configuration page presents the configuration of this audio file backup.

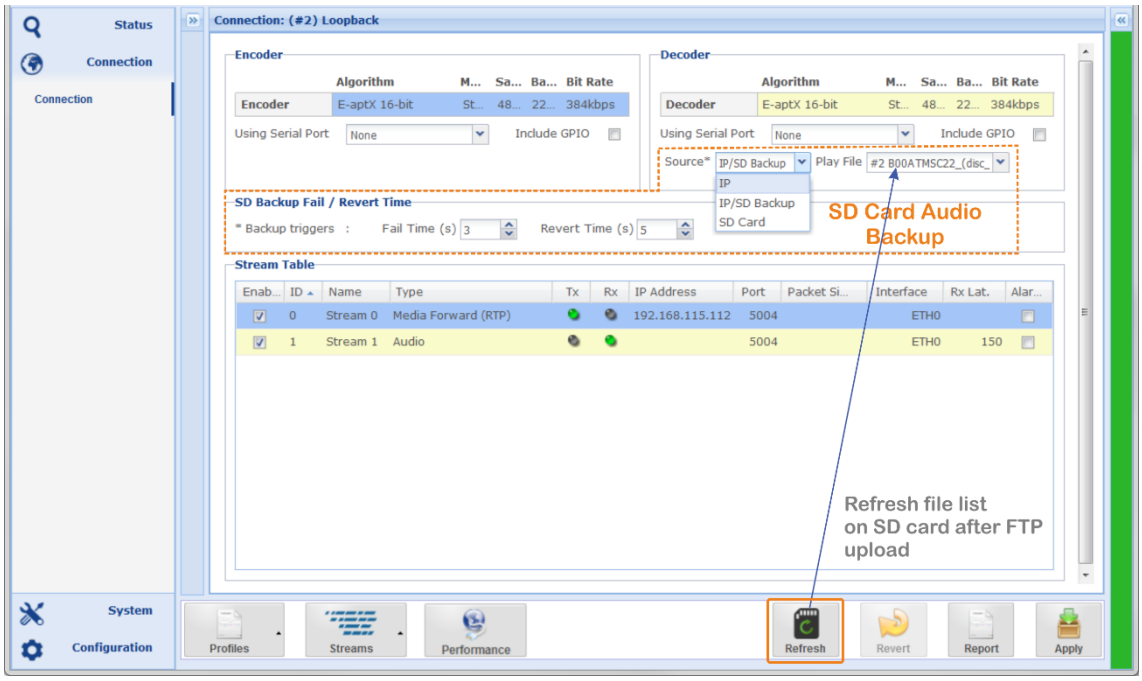


Figure 3-41 shows the configuration of the SD Card audio backup

On the Decoder configuration, the decoder source is set to "IP" by default.

Decoder sources are: IP, IP/SD Backup and SD Card.

Decoder Sources

- IP (stream)

  Decoding audio from the IP stream is the default setting and disables the backup feature.

- IP/SD Backup

  This selection decodes the audio from the IP stream if a network error occurs. The network error is "Loss of Connection" and means that the de-jitter buffer has run empty. In this event, the Decoder starts playing from the selected file on the SD card in accordance with the fail time settings (see below).

- SD Card

  Selecting this mode forces the decoder to play the selected file on the SD card; no backup switching is enabled with this mode (MP3 player).

SD Card – Audio Backup *(continued)*

The audio backup is capable of playing one audio file. You must select the file that will be used for your backup as described earlier. You can store a number of different files to the card, but only the selected file will be played.

ⓘ *The file size (program duration) is not limited by the system but by the size of the SD card.*

File Selection – Play File

The drop-down list "Play File" shows the audio files stored on the SD card. Currently, only one program file can be selected; the duration of the program file is only constrained by the SD card size.

Fail Time / Revert Time

The backup feature is triggered by the "Loss of IP Connection" event. "Fail Time" defines the period which the error must occur before the backup starts playing the file. "Revert Time" defines the period which the error must have been recovered before the Decoder reverts to decode the IP stream.

File Upload to the SD Card

- You can copy the program files on your PC and insert the pre-loaded card. Please make sure that the SD card has mounted correctly (refer to section 3.5.10.2).
- You can upload the files via an FTP connection directly to the inserted SD card. You can use your preferred FTP client to connect to the Codec FTP account (section 3.5.3.2 explains the FTP account settings).

ⓘ *The GUI does not automatically update the play file list after new files were uploaded via FTP. Clicking on the "SD Card Refresh" button in the tool bar of the page updates the file list (refer toFigure 3-41).*

SD Card Type and Format

The card type should be SDHC for audio files playback. There is no limit in size of the card.

⚠ The currently supported format is **FAT32**; please do not insert any other format!

Audio File Types

Currently, the audio backup supports linear audio and MP3 files with these suffixes:

- .wav for standard WAV-files
- .mp2 for MPEG 2 Layer II files
- .mp3 for MP3 files VBR (variable bitrate) and CBR (constant bitrate)
- .aac for AAC files with ADTS header (only)

Decoder Algorithm Setting

When the audio file backup is active, the Decoder automatically identifies the file type of the SD card, because of that the algorithm for decoding the IP stream can be different from the backup file.

SD Card – Audio Backup *(continued)*

General Considerations

Audio File – Audio Level

Playing a backup file, the Decoder uses the same audio settings as when decoding an IP stream. It is important to create the audio file with the same digital level so that no jump in level is caused when playing the audio backup file.

Audio File – File Format

The Decoder supports a variety of different file formats. Nevertheless, we recommend verifying that the decoder detects the file format correctly and plays the file without artefacts.

Audio Backup – Timing

You may perform some test to identify the best timing of Fail Time and Revert Time. The Codec needs a few seconds to identify a stable condition. To avoid a ping-pong effect, make sure that the detection periods are not set too short.

Notes:

3.4.16.2 Configuration Validation

The Validation Engine (Valex) 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 and example about how the Valex Engine intervenes and how it presents information about mistakes on the GUI.

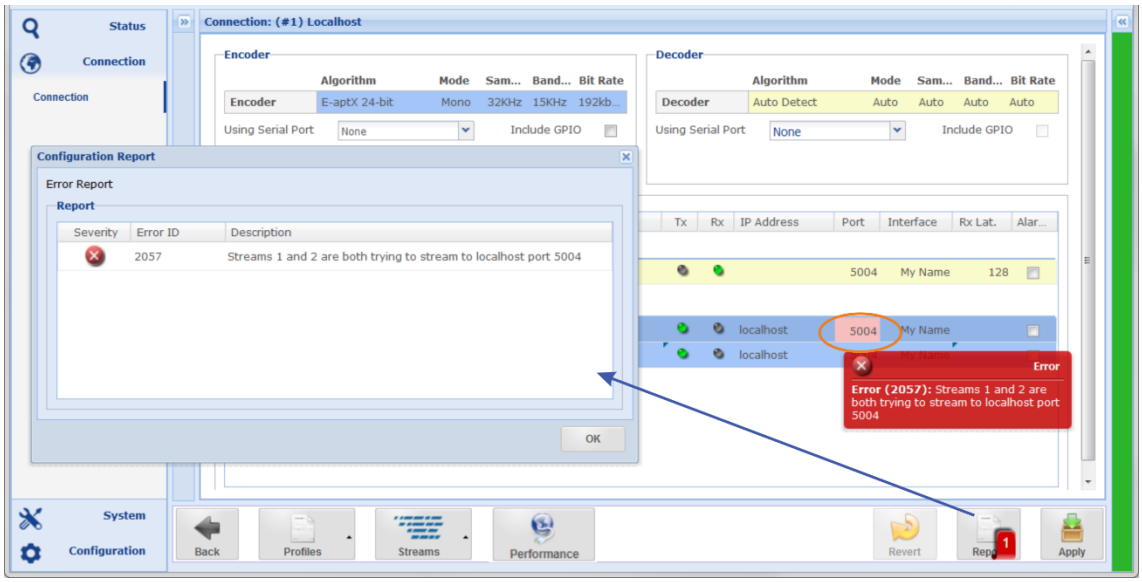


Figure 3-42: Demonstrates how the Validation Engine presents error conditions and warnings

The invalid configuration in this example is the assignment of IP port 5004 to two Tx streams. The Validation Engine highlights this misconfiguration as an error on all affected instances; i.e., on the port configuration of the 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.

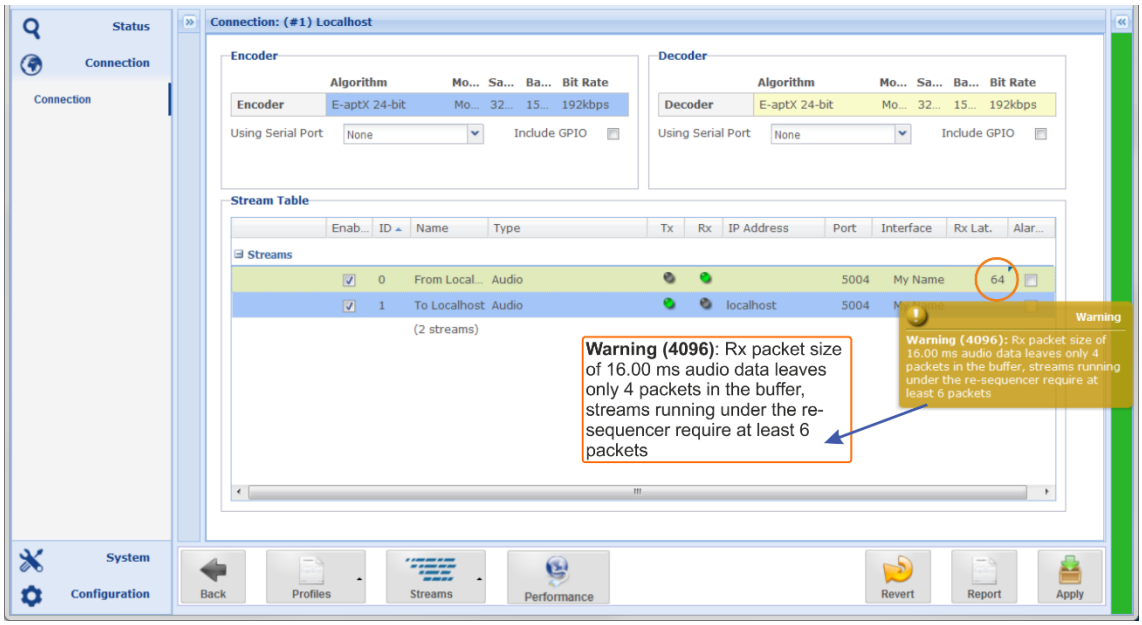


Figure 3-43 shows a yellow warning from the Validation Engine

The Validation Engine has identified a problem within this profile. In this example, the de-jitter buffer is set to 64 milliseconds. The Valex Engine has calculated 16 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 96 ms (6x 16 ms = 96 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.

ⓘ *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:

3.4.17 Digital MPX over IP – AES 128 or 192 kHz FS

The digital MPX transmission modes accept sample rates of 128 kHz or 192 kHz FS providing either a data path of 64 kHz (audio & RDS) or 88 kHz (full MPX). The algorithm list provides the MPX transmission mode of 16 Bit or 24 Bit.

The audio format and stream configuration follow the standard procedure as described in section 3.4 and **Fehler! Verweisquelle konnte nicht gefunden werden.**. For digital MPX, only linear PCM 16 or 24 Bit must be used.

ⓘ *The digital MPX transmission mode is an option and is available only if the license has been applied to the unit. How to implement a license is described in "Main Menu – System".*

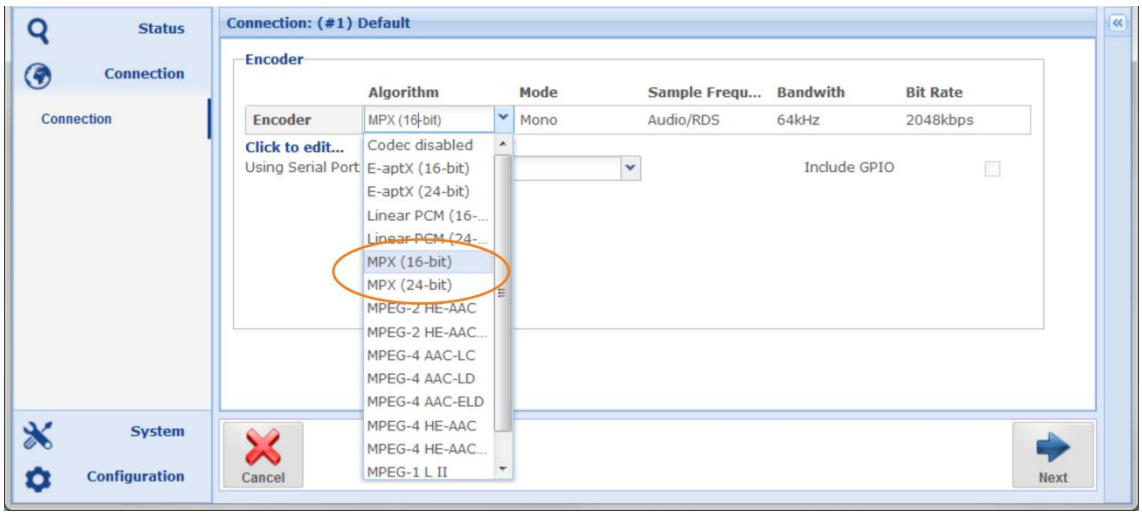
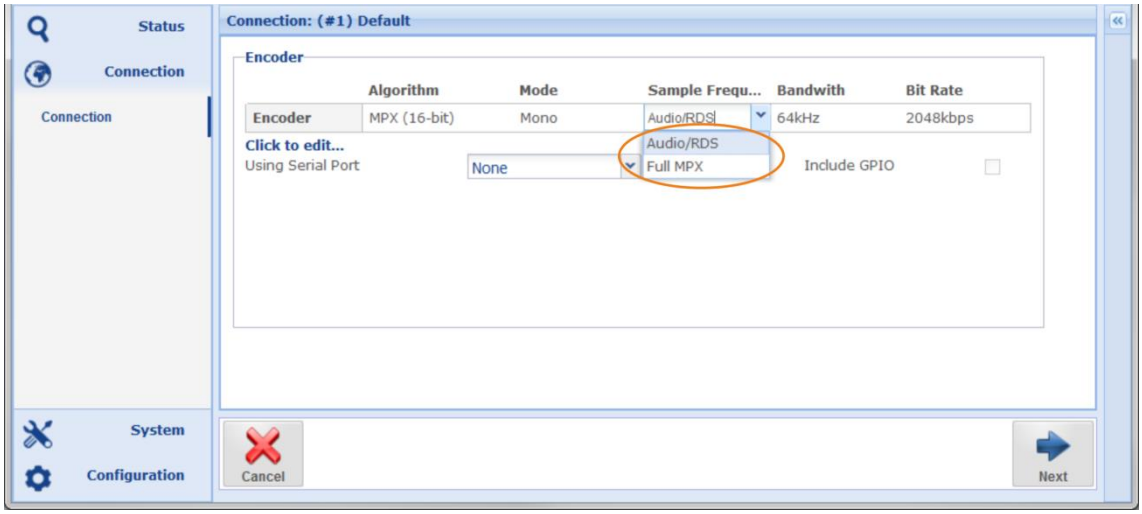


Figure 3-44 shows the audio algorithm selection with the MPX options



ⓘ *Figure 3-45 shows the sample frequency selection field providing the two MPX modes*

3.4.17.1 Digital MPX – Stream Configuration

The stream configuration for digital MPX follows the same procedure of generating an IP audio stream. Due to the high bit rate selecting 192 kHz sample frequency, the packet time cannot exceed 3 ms for a 16 Bit transmission and 2 ms for a 24 Bit transmission. The maximum payload of a packet is 1350 Byte.

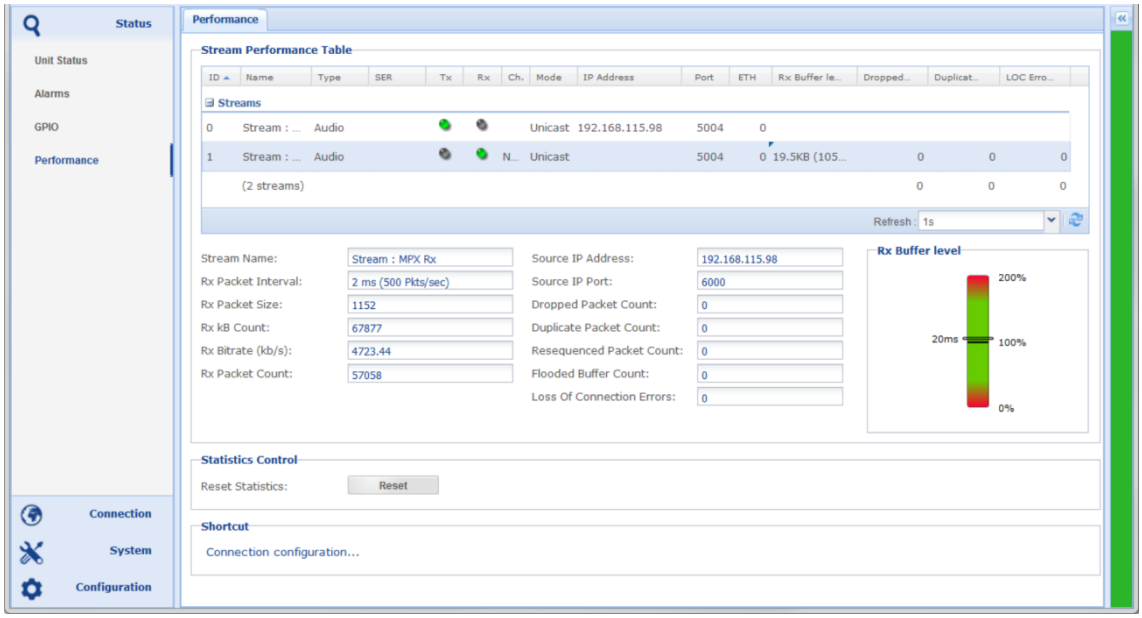


Figure 3-46 Performance monitor of the received stream @FS 192 kHz (~4.750 kbps, 500 packets/s)

3.4.17.2 Digital MPX – Technical Specifications

- Digital MPX input, AES-3 format (mono, left channel only)
- 128/192 kHz FS – Bandwidths input/output: 64/88 kHz
- Linear transmission with 16 Bit and 24 Bit resolution
- Bit rates (payload):
  @ FS 192 kHz, 16 Bit: 3.072 kbps, 24 Bit: 4.608 kbps
  @ FS 128 kHz, 16 Bit: 2.048 kbps, 24 Bit: 3.072 kbps
- IP Packet time
  @ FS 192 kHz max: 3 ms for 16 bit, 2 ms for 24 Bit
  @ FS 128 kHz max: 5 ms for 16 bit, 3 ms for 24 Bit
  (payload must not exceed 1280 Bytes)
- Overmodulation Cancellation Algorithm (OMC), minimizing adverse effects of packet losses on the FM deviation – implemented as standard
- Fully compatible with existing reliability enhancements like SureStream and IP packet forwarding
- Sample rate converter on Input and Output
- Headphone monitoring of L+R/2 (mono mix)

3.4.17.3 Digital MPX Link – Typical Application

Central signal processing and digital MPX generation

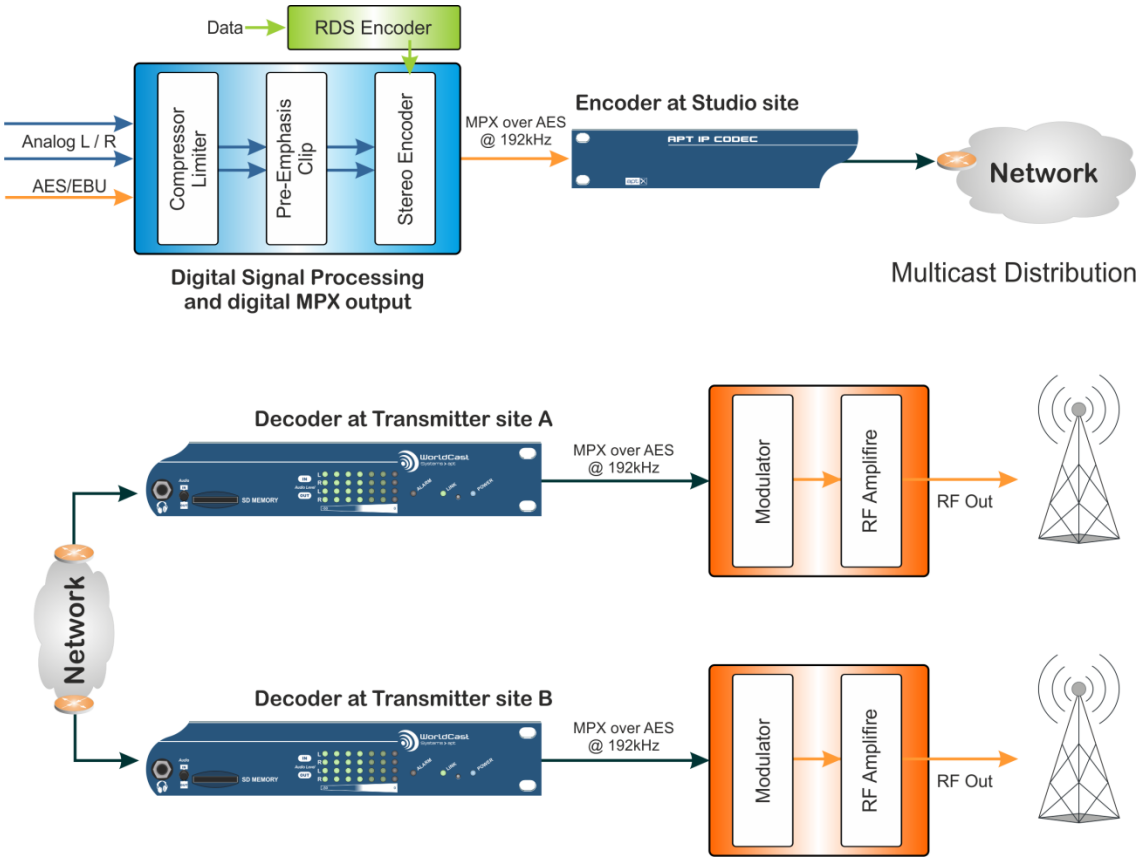


Figure 3-47: Shows a typical MPX distribution application

3.5 Main Menu - System

3.5.1 Date and Time

The IP Codec 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.

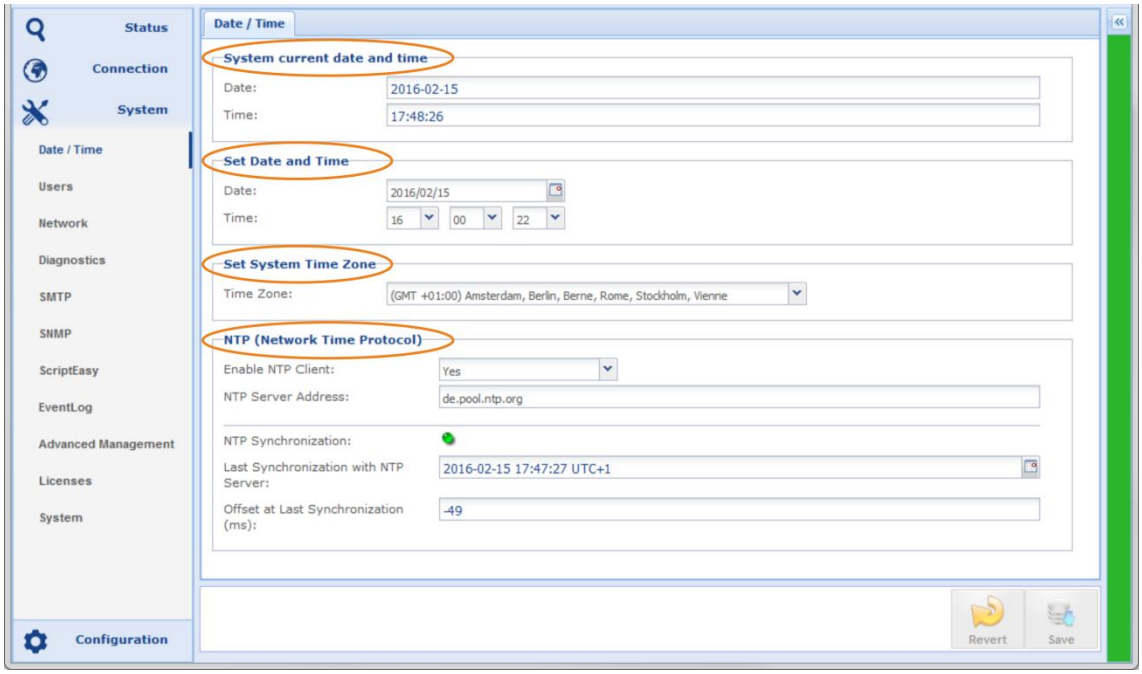


Figure 3-48: Shows the system page for date and time configurations

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.

3.5.2 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 big 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).

3.5.2.1 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 no gateway address is entered on ETH0, the NTP client attempts to connect via ETH1, 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.*

3.5.2.2 NTP Server general Considerations

- The NTP Server should always be referenced to an external source (GPS or another IP).
- Stratum values should be as low as possible (less than 10).
- 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.*

3.5.3 User Management

3.5.3.1 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.

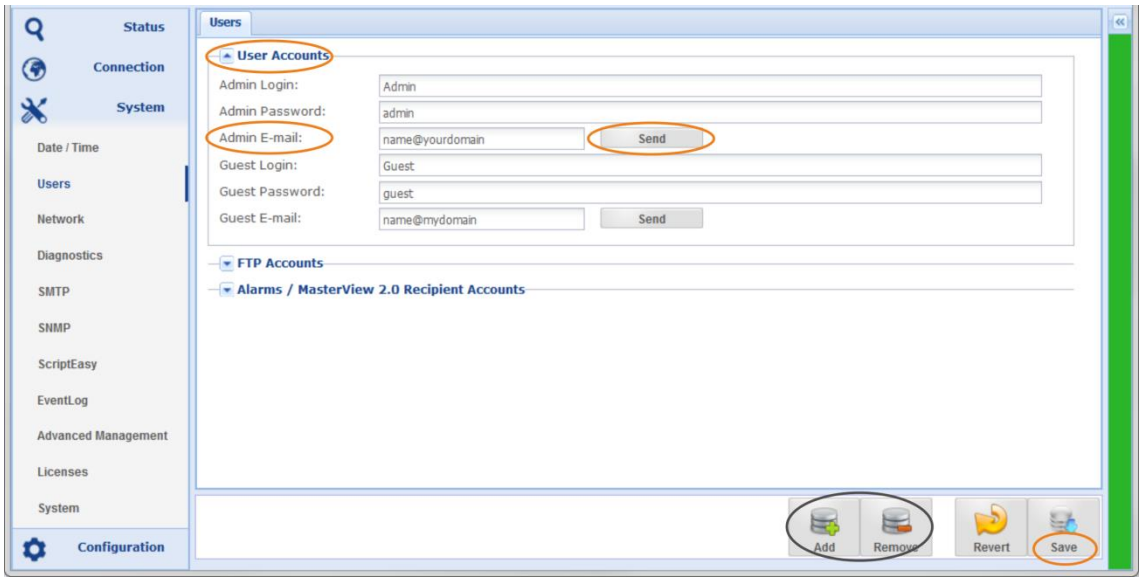


Figure 3-49: Shows the user page with account managers

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.

ⓘ *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 3.5.6).

ⓘ *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!

3.5.3.2 FTP Accounts

These FTP accounts are used for the communication with external applications.

All FTP accounts work on both ETH ports. The firewall allows filtering the FTP service on each ETH port; it is recommended to filter the FTP service if not used (section 3.5.4.8).

The FTP service allows uploading or downloading files to the Codec while streaming audio. There is no bandwidth throttling or speed limit for the file transfer. Care must be taken not to compromise the audio streams by overloading the link capacity. You must configure your external FTP client to manage the maximal up- and download speed accordingly.

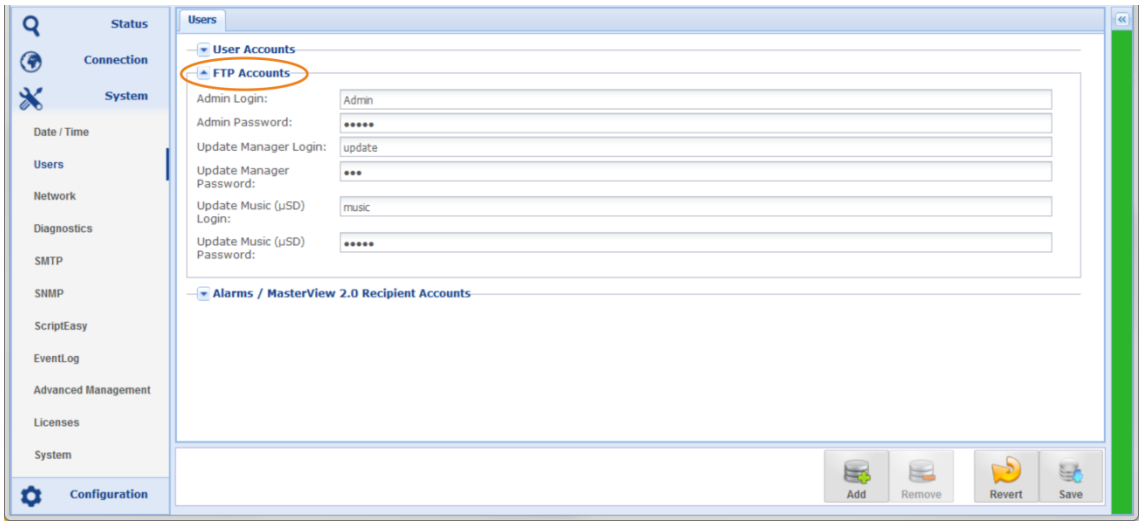


Figure 3-50 shows the user page with the FTP account manager

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

ScriptEasy Applications

ScriptEasy requires access via FTP for uploading a new script initially. Once the script is uploaded the FTP account is no longer used. ScriptEasy uses a dedicated and hidden FTP account, 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 (SD Card)

You must use this account to access the file system of the SD card inserted in the Codec. This account allows you to upload and manage audio files for the Audio Backup Feature.

⚠ The optional APT Network Management Software (NMS) utilizes FTP for centralized firmware uploads. If the NMS is used, make sure that the FTP account is enabled on the firewall (see firewall settings in the network configuration section 3.5.4.8).

3.5.3.3 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.

Notes:

_____

_____

_____

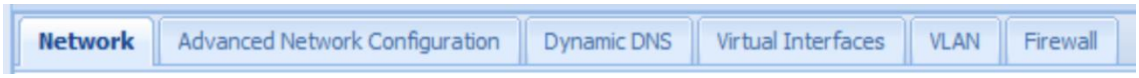
_____

_____

_____

3.5.4 Network Configurations

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



3.5.4.1 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.

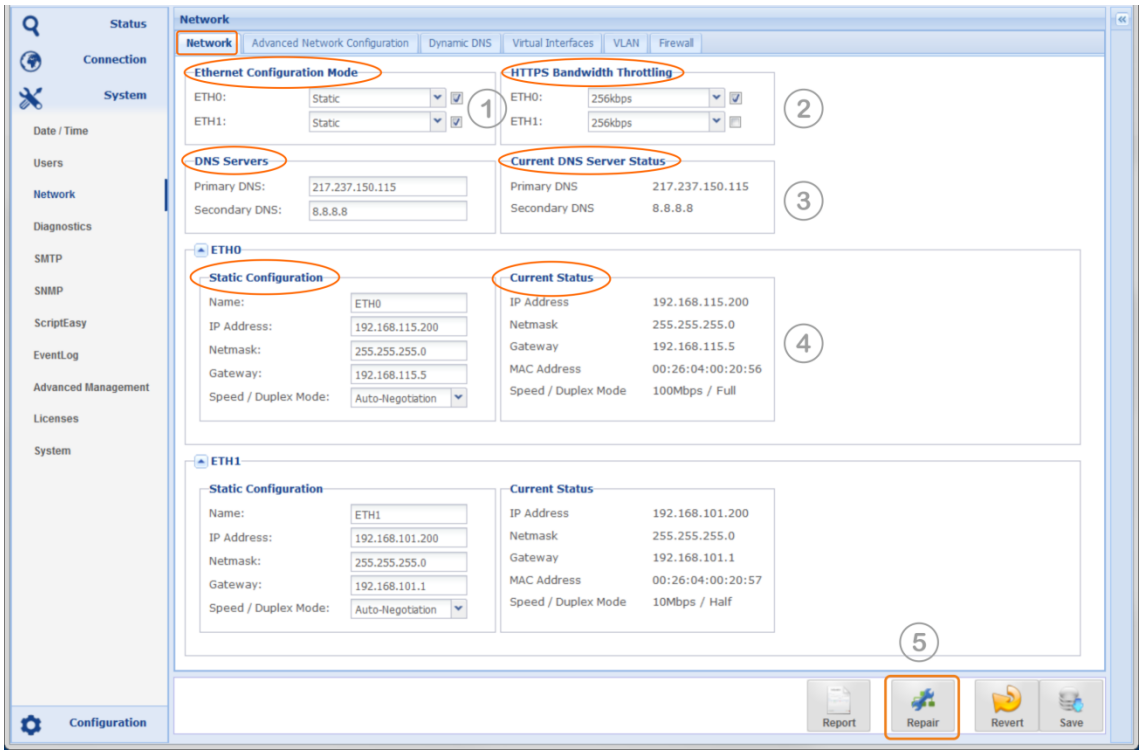


Figure 3-51 shows the options on the Network configuration page

(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.

- Check boxes for enabling or disabling an ETH interfaces

Network - Network *(continued)*

(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.

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. In the manual (static) mode, the DNS addresses can be from ETH0 or ETH1. The DHCP server configures both DNS entries (primary and secondary) from the same network interface (ETH).

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 and ETH1

Section 4 shows the "Current Status" of both interfaces 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)

Each ETH interface MUST be configured on a **separate** sub-network. It is not possible to assign more than one ETH interface to the same subnet!

(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).

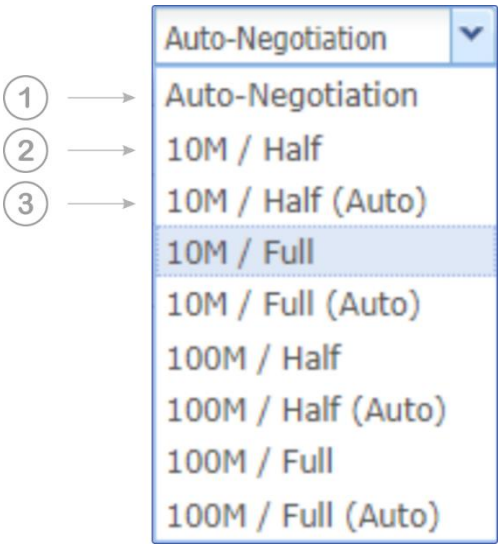
Network - Network *(continued)*

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.

*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:

3.5.4.2 Advanced Network Configuration

Advanced Configuration provides UPnP settings for the management ports.

3.5.4.3 UPnP - NAT Traversal Mode

The NAT traversal mode enables the IP Codec 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 Codec 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.

ⓘ *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.

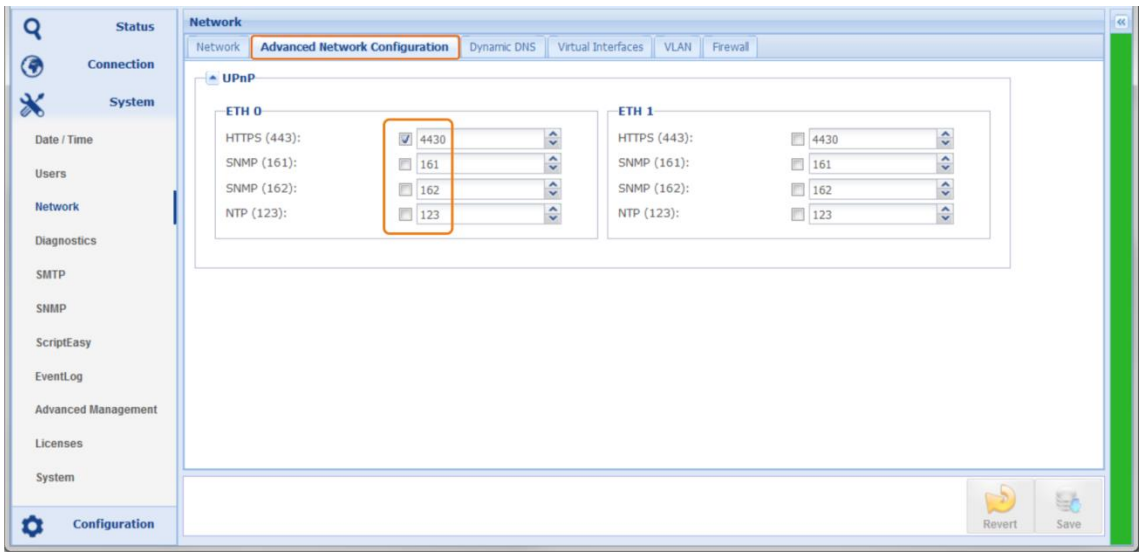


Figure 3-52: Shows the UPnP settings for management port 443

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). Port mapping or port forwarding is possible on both ETH interfaces independently.

3.5.4.4 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 Codec provides an integrated Dynamic DNS client allowing communication with the most popular Dynamic DNS service providers. With this service enabled, each network interface of the IP Codec 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, at least, one hostname must have been registered on one of the DDNS services provided on the drop-down list (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.

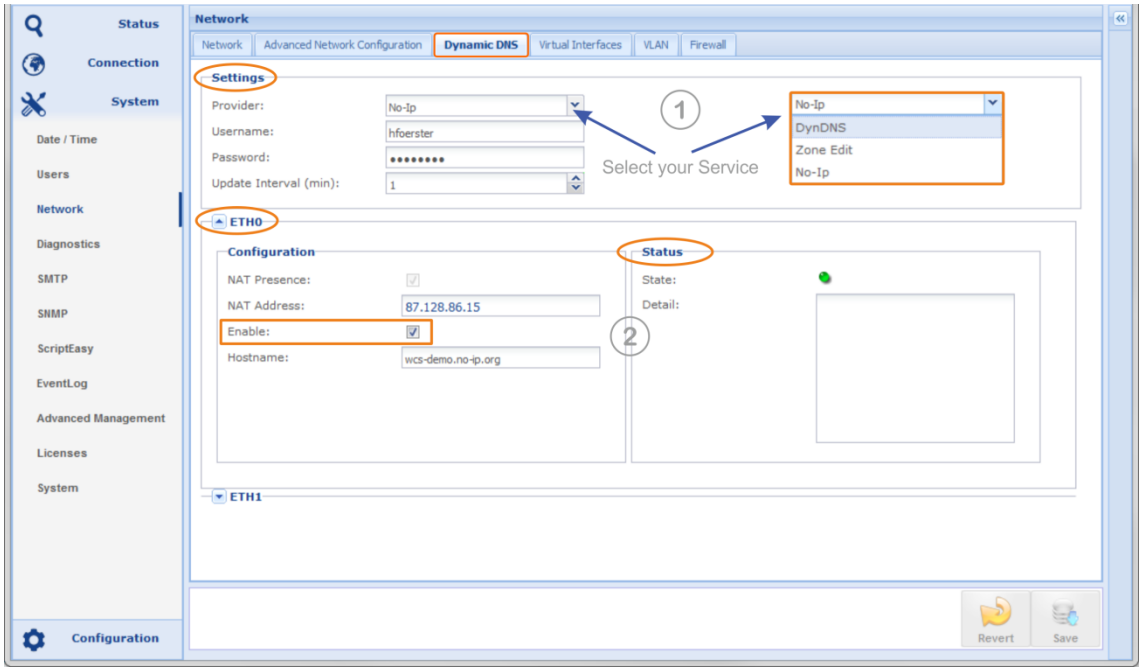


Figure 3-53: Shows the Dynamic DNS client settings and status information

Dynamic DNS *(continued)*

The example above uses the No-IP service (www.noip.com). With the username and the password, the client connects to this DDNS service provider if the "Enable" checkbox is ticked on one or both ETH ports 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:

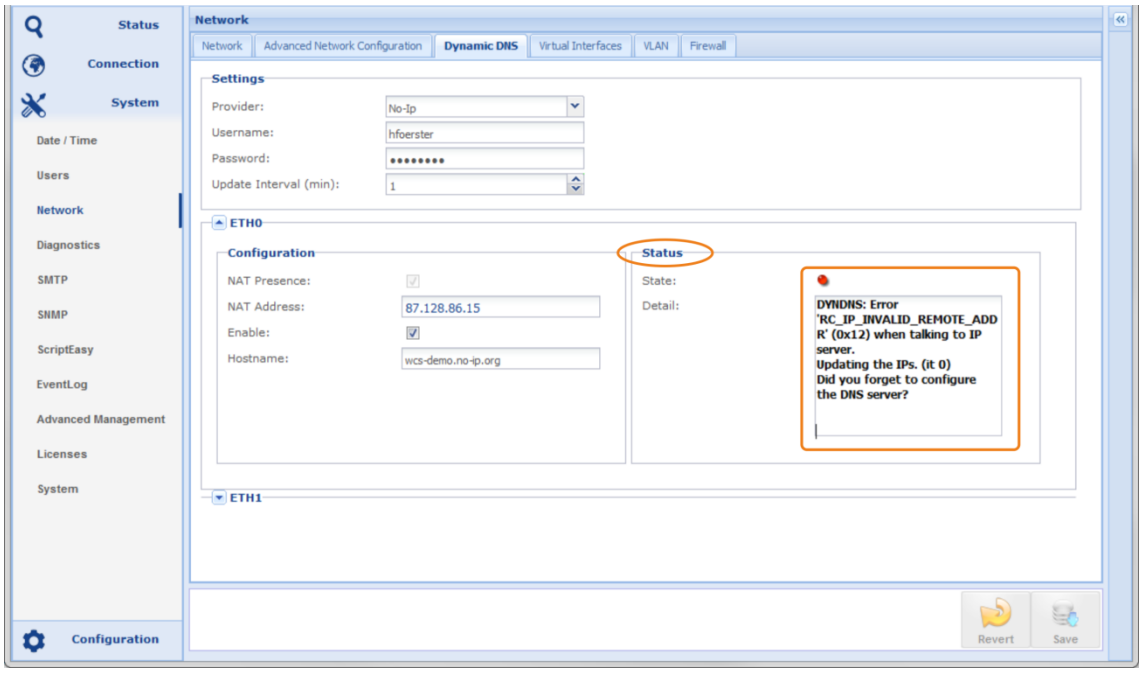


Figure 3-54: Shows an error message of the DDNS status

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.

3.5.4.5 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 in order 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.

ⓘ *For using mDNS your management PC must be connected to the same sub-network as your unit; mDNS Look Up is enabled on ETH0 only!*

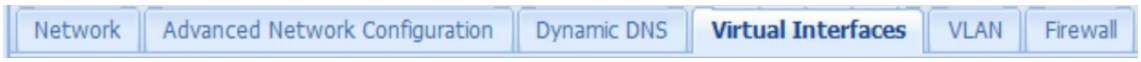
For the IP Codec the mDNS name is:

wcs-SerialNumber.local – e.g. for an IP Codec with serial number H000872:

https://wcs-H000872.local *(for system release 1.2.x and higher only)*

ⓘ *The serial number is available on a label on the side of the IP Codec. The "Local" domain is the common domain of your PC.*

3.5.4.6 Virtual IP Interfaces



With virtual IP interfaces applied to the physical ETH ports (ETH0/ETH1), the single physical interface can have multiple static IP addresses and multiple gateways, but without virtual LAN tagging.

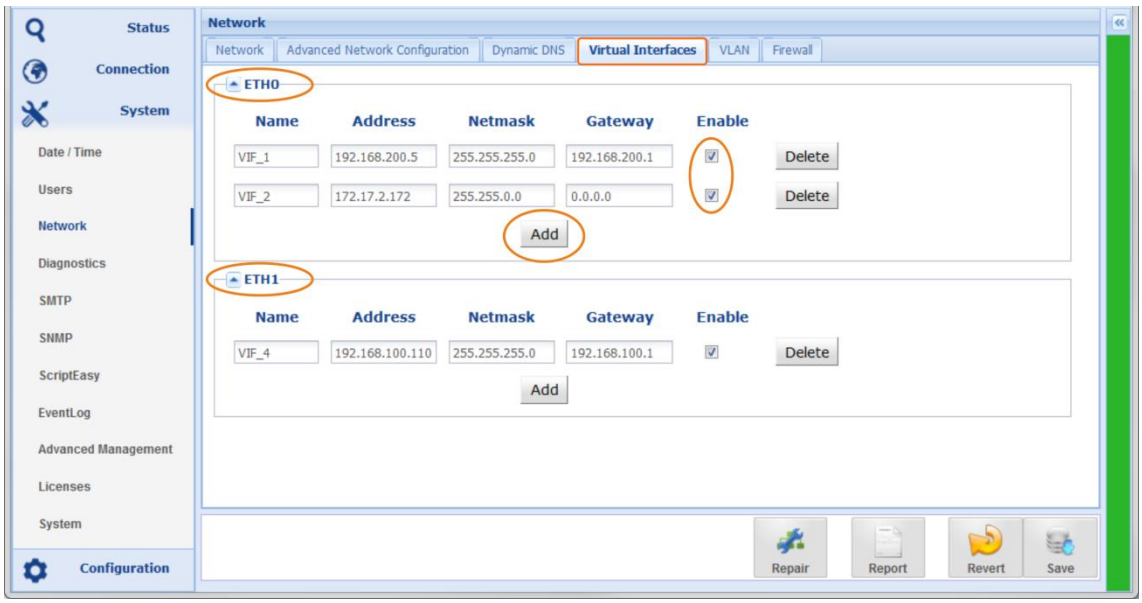


Figure 3-55: Shows the management page of virtual interfaces

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 3.4.10 pos. 5), the new interface is available in the drop-down list.

3.5.4.7 VLAN Tagging – Virtual LAN

Applying VLAN IDs (VID) to the virtual interface allows integrating the IP Codec 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 limitation of physical interfaces.

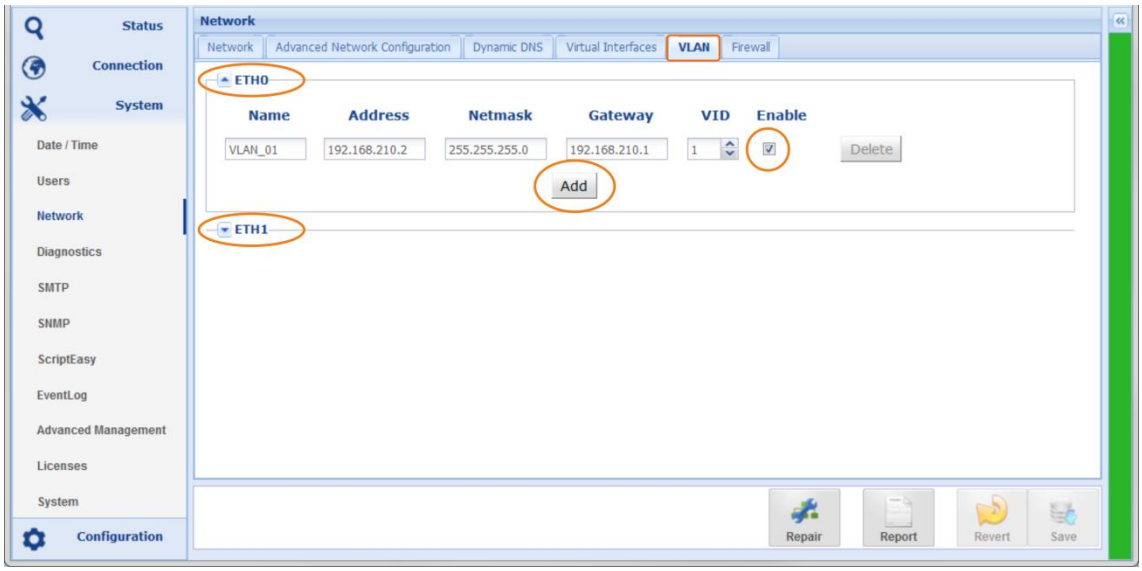


Figure 3-56: Shows the management page of virtual LANs (VLAN)

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 3.4.10 pos. 5), the new VLAN interface is available in the drop-down list.

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:

3.5.4.8 Firewall

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

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

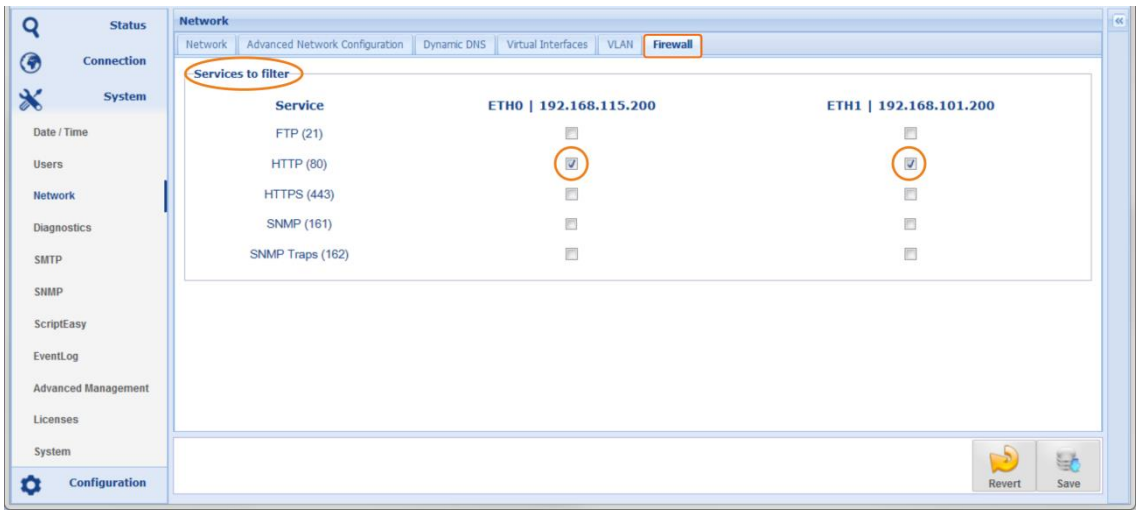


Figure 3-57: Shows the filter options on the firewall page - HTTP service (port 80) is disabled on both interfaces

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

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

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

3.5.5 Diagnostic Page

Restart

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

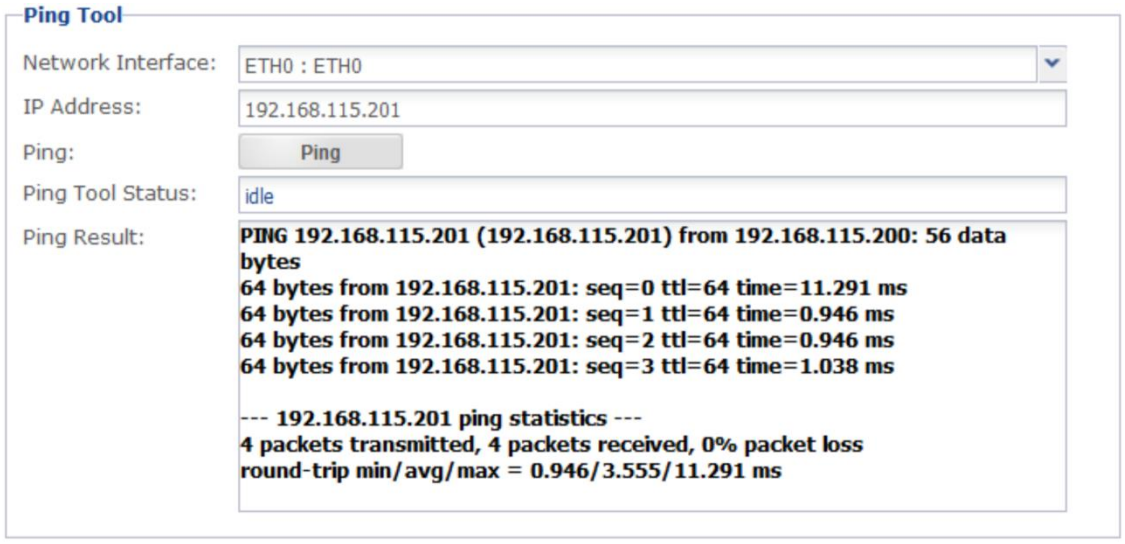
Default Configuration

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

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 ETH interface. This diagnostic tool facilitates the identification of possible connection problems.



3.5.6 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 3.5.3).

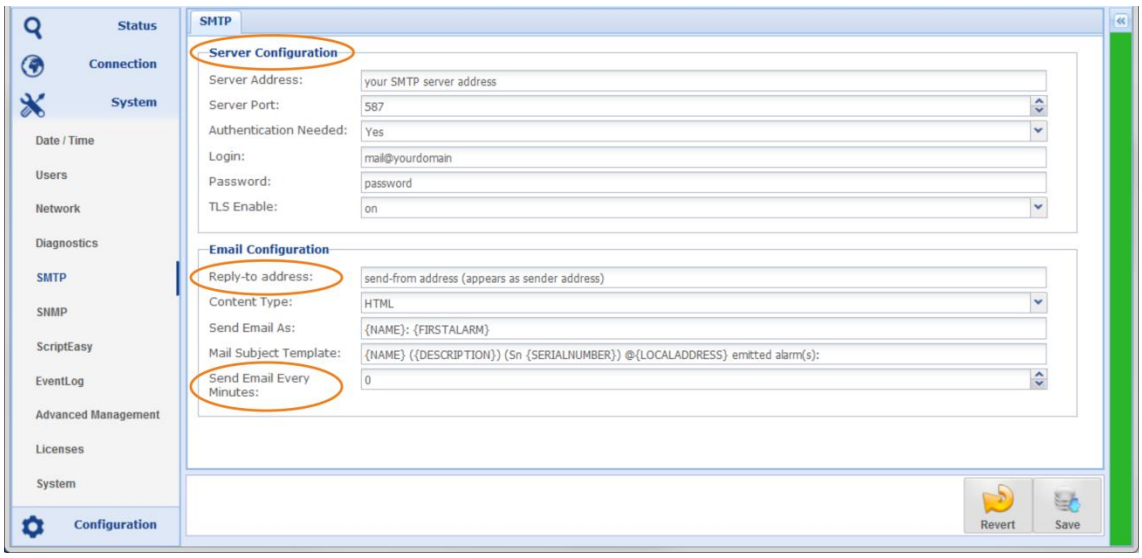


Figure 3-58: Shows the SMTP (email) configuration page

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 3.5.3).

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 Codec
- {SERIALNUMBER}: Serial number of alarming unit
- {LOCALADDRESS}: IP address of port ETH0 of alarming unit

3.5.6.1 SMTP Client - Network Connection

Connecting to an email server in a network (or internet) requires a valid gateway IP address entered in the interface settings. The email client first tries to connect via ETH0 (default gateway). If a connection to the email server cannot be established via ETH0, the SMTP client attempts to establish the connection via the ETH1 interface.

Notes:

_____

_____

_____

_____

_____

_____

3.5.7 SNMP

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

3.5.7.1 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).

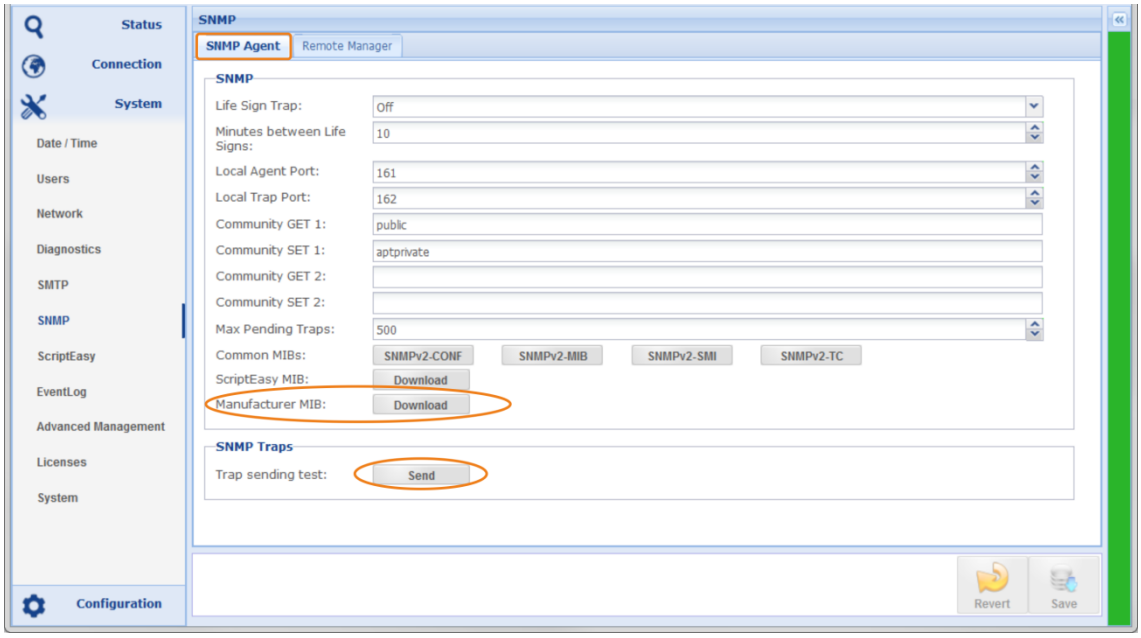


Figure 3-59: Shows the SNMP-Agent configuration page

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

3.5.7.2 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.

3.5.7.3 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.

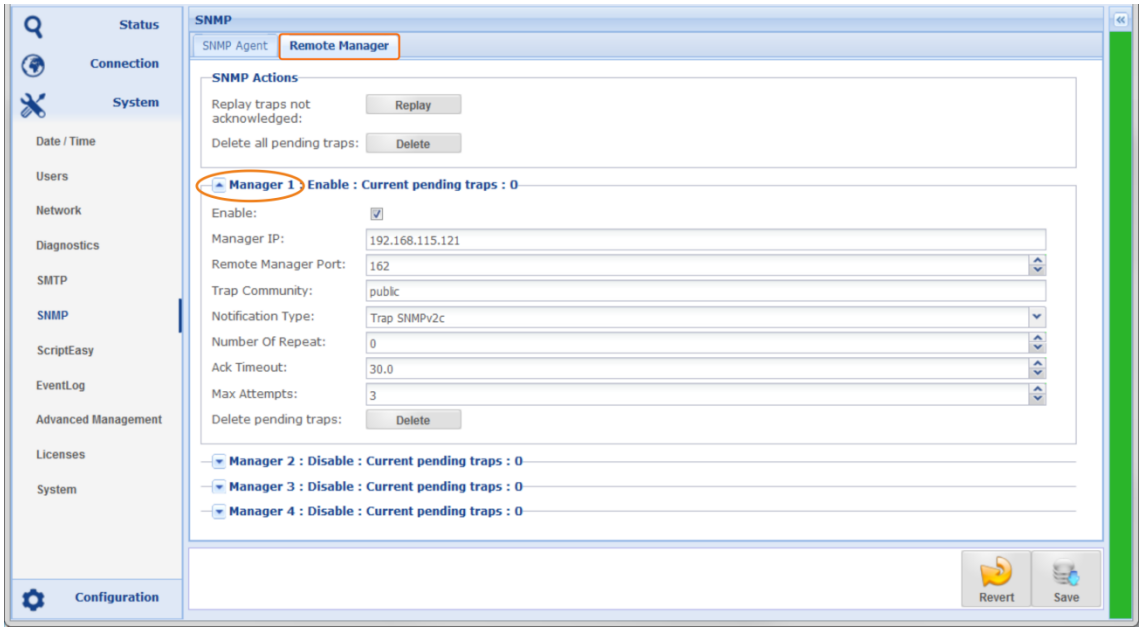


Figure 3-60: Shows the configuration page for the SNMP Remote Managers

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

3.5.8 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 IP 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 website (user account required).

3.5.8.1 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.

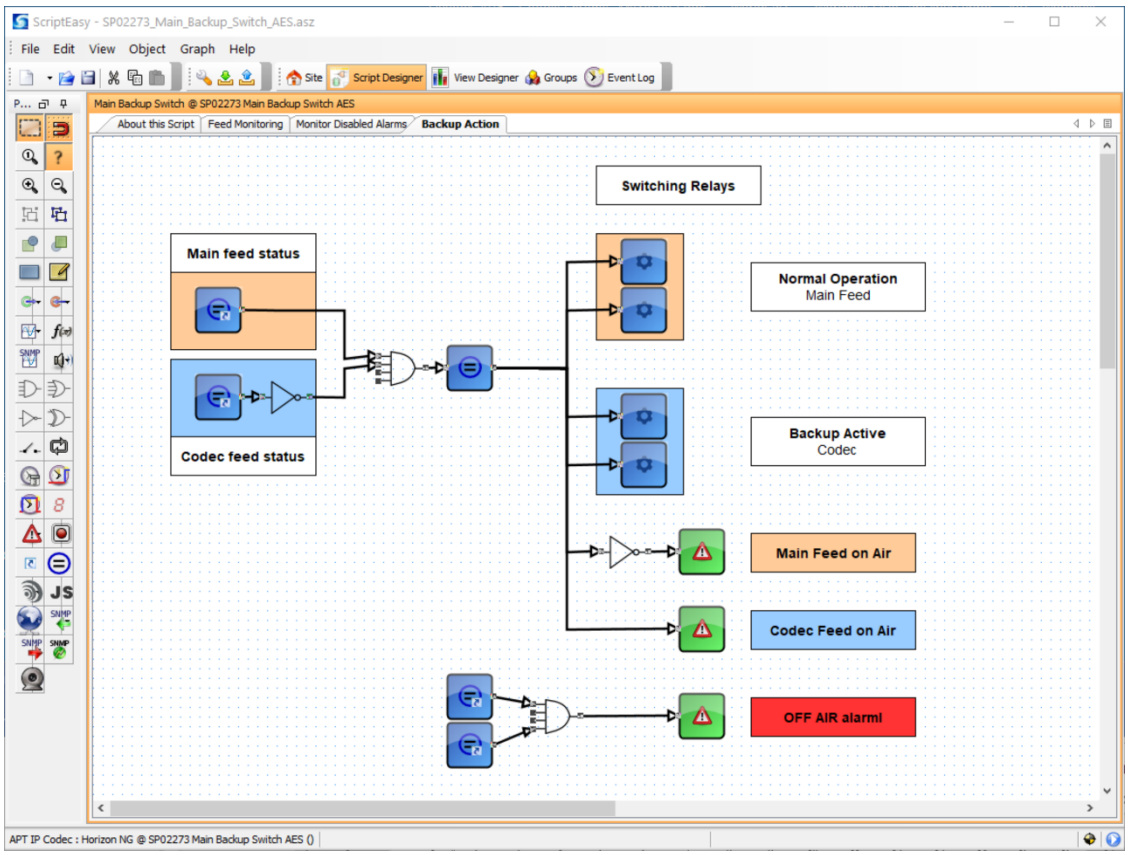


Figure 3-61: Shows the Script Application Designer IDE

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

3.5.8.2 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.

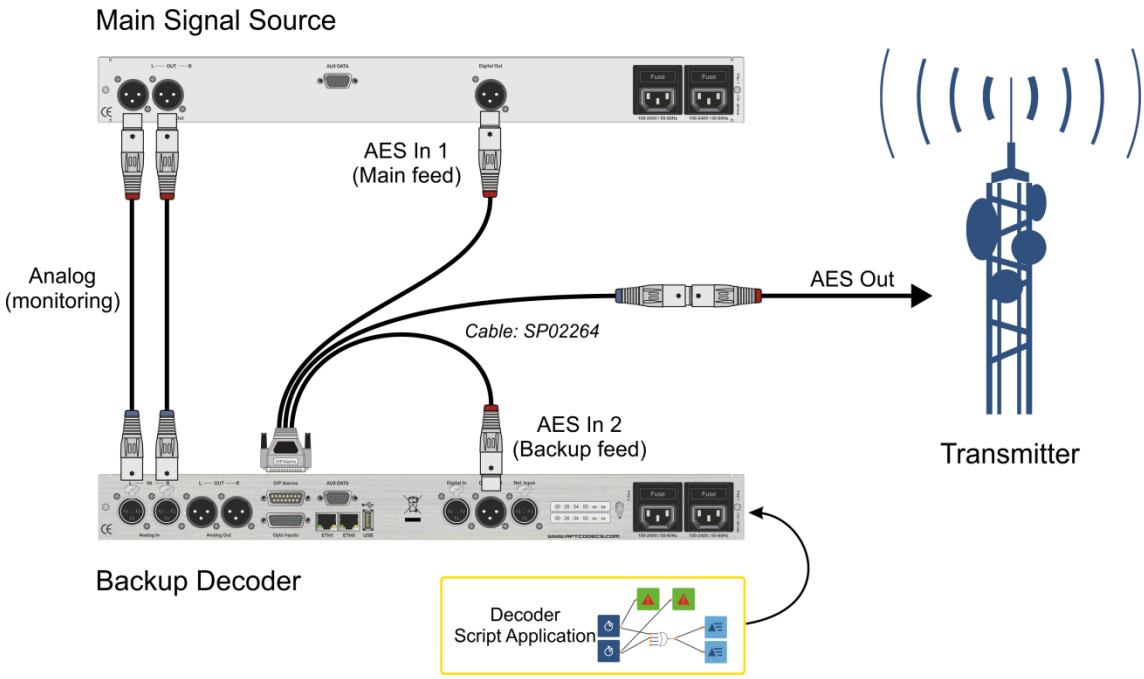


Figure 3-62: Shows the main-backup switching application controlled by the script application

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.

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

3.5.8.3 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.

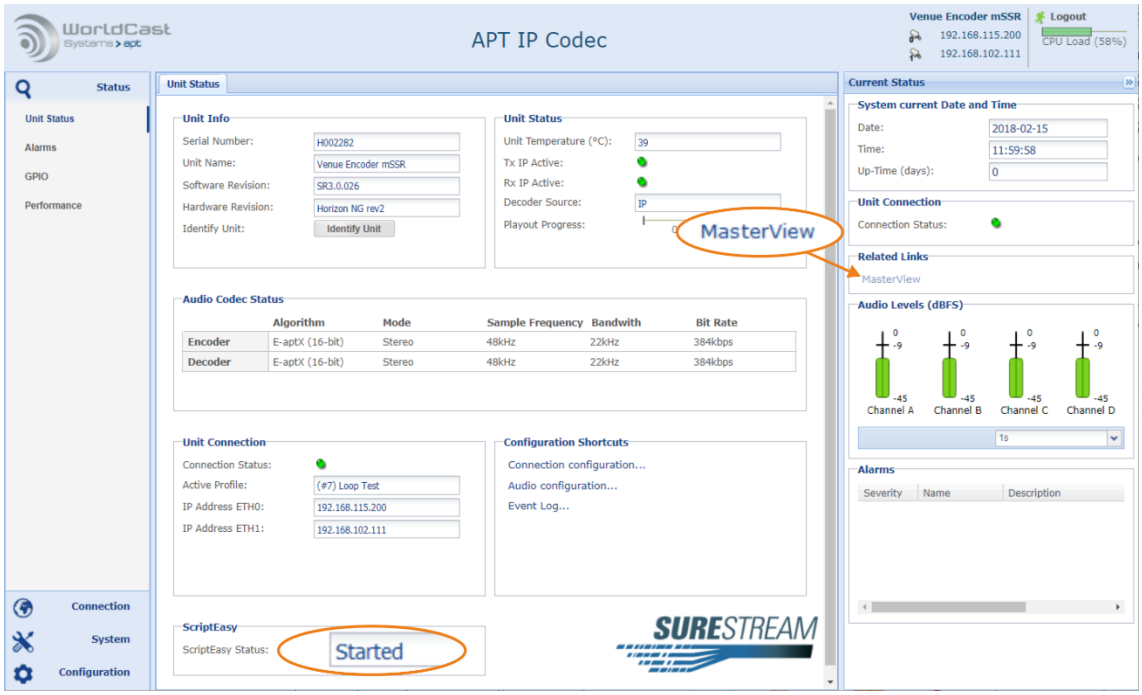


Figure 3-63: Status page showing the link to MasterView

With a script application running on the Codec device (script started), the link to the Master-View 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.

3.5.8.4 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.

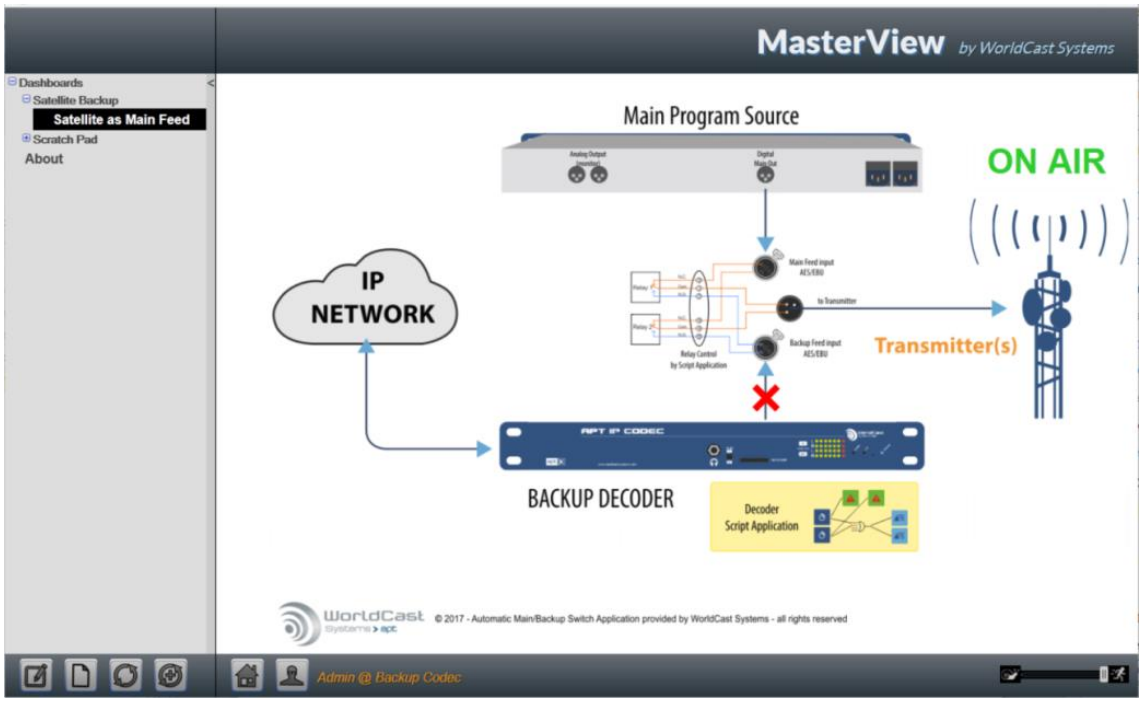


Figure 3-64: Shows the application status on the dashboard – On Air condition

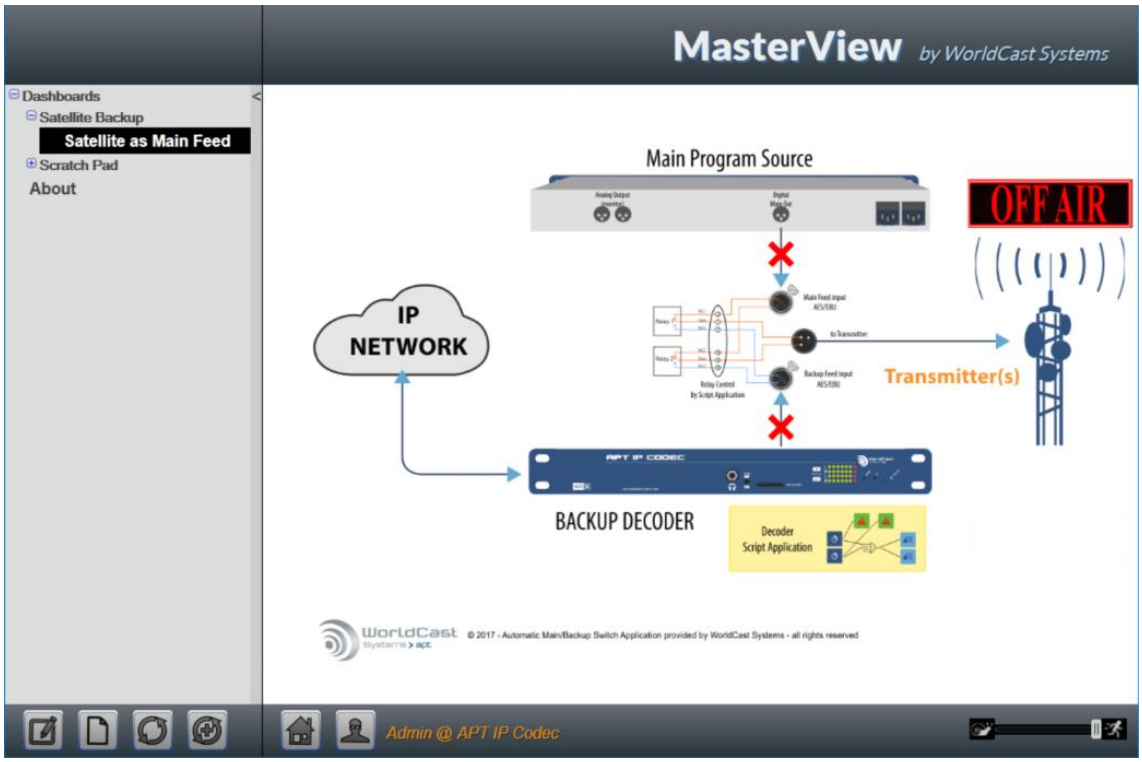


Figure 3-65: Shows the application status on the dashboard – Off Air condition

3.5.8.5 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 3.5.8.6.*

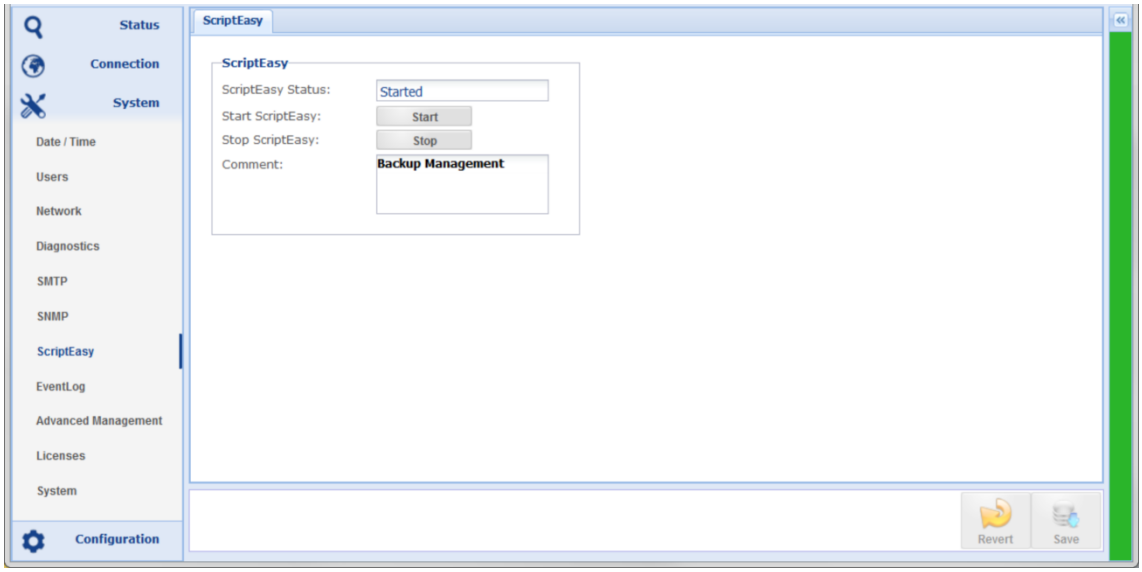


Figure 3-66: The ScriptEasy page in the system menu shows the script controls

ⓘ *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 3.5.4.8).

3.5.8.6 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).

3.5.9 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 in order to limit the number of shown log entries.

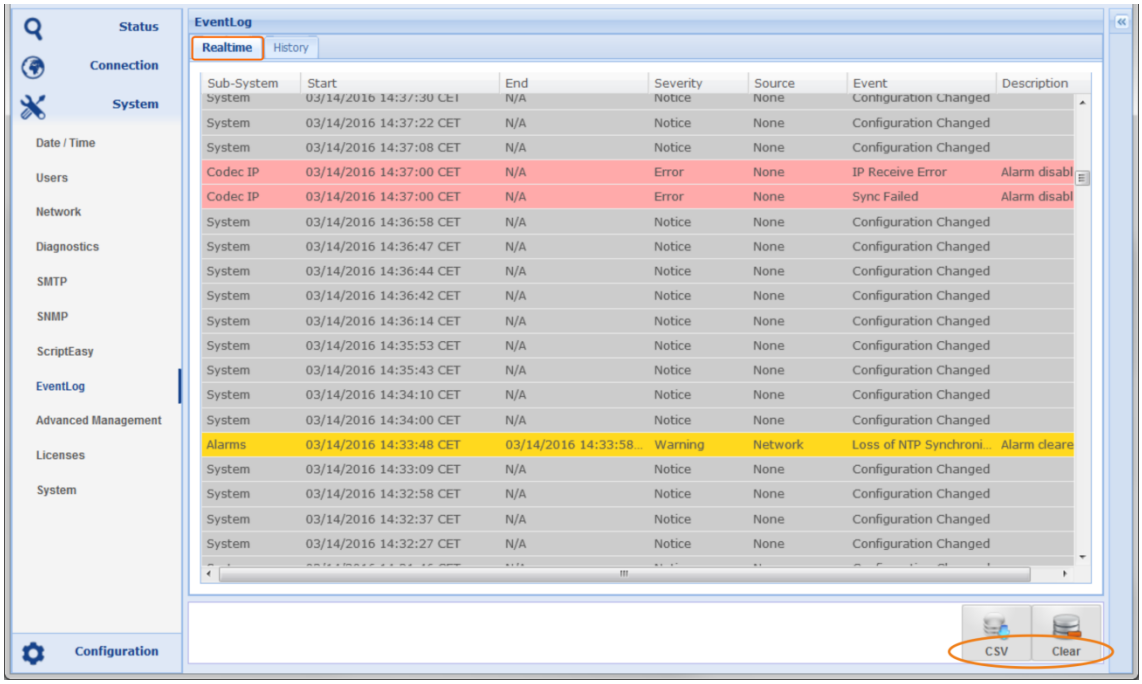


Figure 3-67: Shows Event Logs in the real time

3.5.9.1 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.

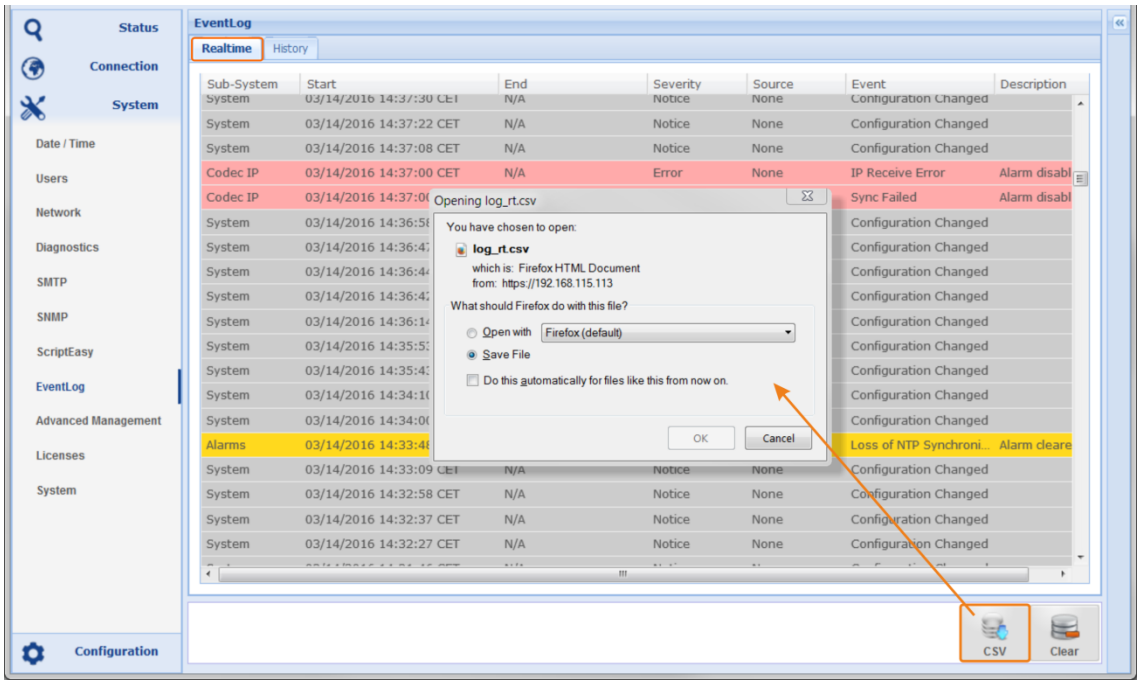


Figure 3-68: Shows the CSV formatted log file entries

3.5.9.2 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.

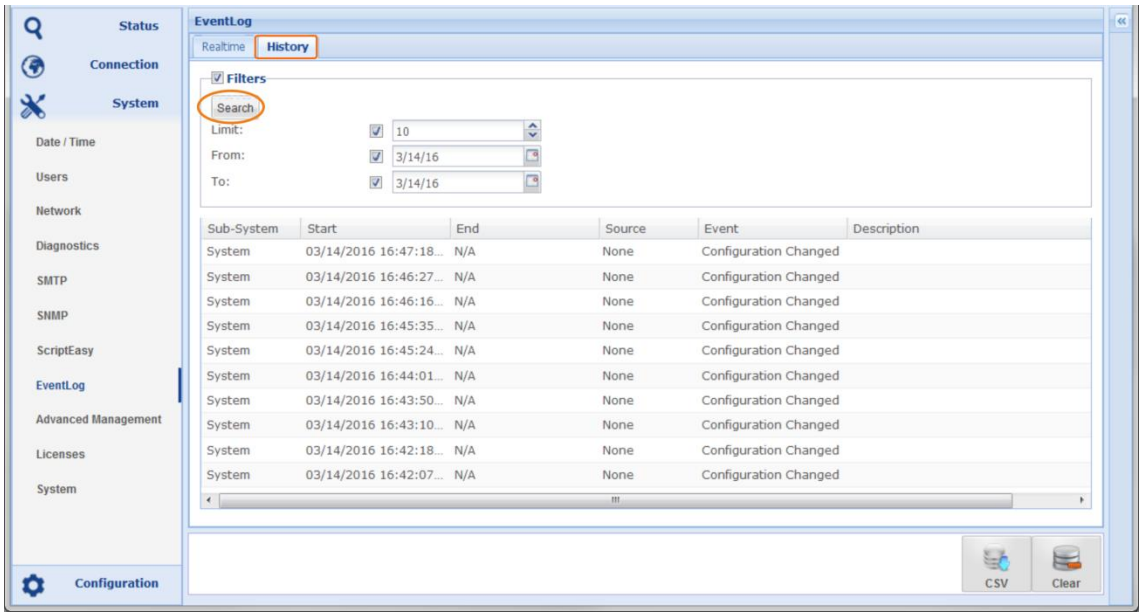


Figure 3-69: Shows the history retrieval options

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.

Notes:

3.5.10 Advanced Management

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

3.5.10.1 Inserting an SD Card

- Remove the power lead(s) from the IP Codec
- Insert the SD card as shown below
- Re-connect the mains lead to the IP Codec

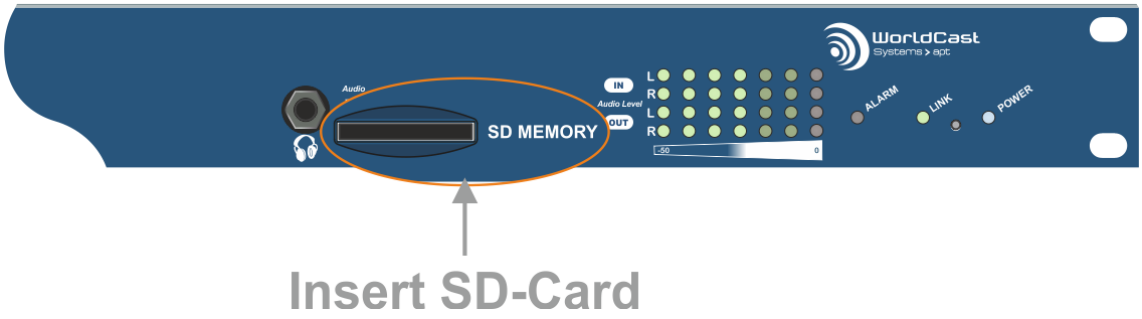


Figure 3-70: Shows how to insert an SD card

3.5.10.2 SD Card Management

Once an SD card has been inserted, the system will mount the card on boot up (only FAT format is supported – no FAT 32 and no NTFS). The SD Card status shows "Mounted". Clicking on the Eject button unmounts the card.

ⓘ *An SD Card is mounted during bootup – there is no manual mounting possible.*

Two system applications support and require the SD card properly mounted.

- SD Card System Backup
- Audio Backup on SD card

⚠ Don't insert an SD card while running a firmware prior SR 2.0! The inserted SD card is not supported by earlier releases and inhibits the unit to boot.

3.5.10.3 SD Card System Backup

With the system backup, you can store and recall the entire system configuration to and from the SD Card. The backup file consists of all system configuration including network settings and all user settings.

If you restore this backup file to a new device, the new unit appears as an exact clone of the origin IP Codec (including all network settings – but not the MAC addresses!).

⚠ You should use the SD Card System Backup if a device has been replaced or a fatal error has destroyed the configuration.

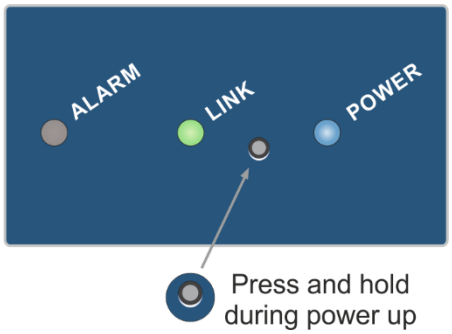
ⓘ *For reloading only the unit configuration, the "Backup/Restore Configuration" option should be used (refer to next section).*

SD Card Backup File Creation

Clicking on the "Backup" button creates a restore point and copies the configuration to the SD card. The "Restore Point Available" field displays the status and the creation date of the backup file. Clicking again on the button overwrites the current file and sets a new time stamp.

Restore a System Backup

- Follow the procedure for inserting the SD Card into the unit (Figure 3-70).
- Remove the power lead(s) from the unit
- On the IP Codec's front panel, there is a small hole where behind this hole sits a little Switch. Press this button and connect the power supply to the unit. Hold the button pressed during power-up until the status LED starts to flash (about 10-15 seconds). The unit boots and loads the configuration from the SD card.



⚠ It is important to press the little button reliably while the power supply is connected to the unit (press and hold, then connect the mains lead).

Notes:

_____

_____

_____

3.5.10.4 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 Codec #H000872: backup-H000872-20160408-181525.dat.

⚠ You can edit the file name only behind the Serial number part e.g., "backup-H000872-**My-Codec**.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).

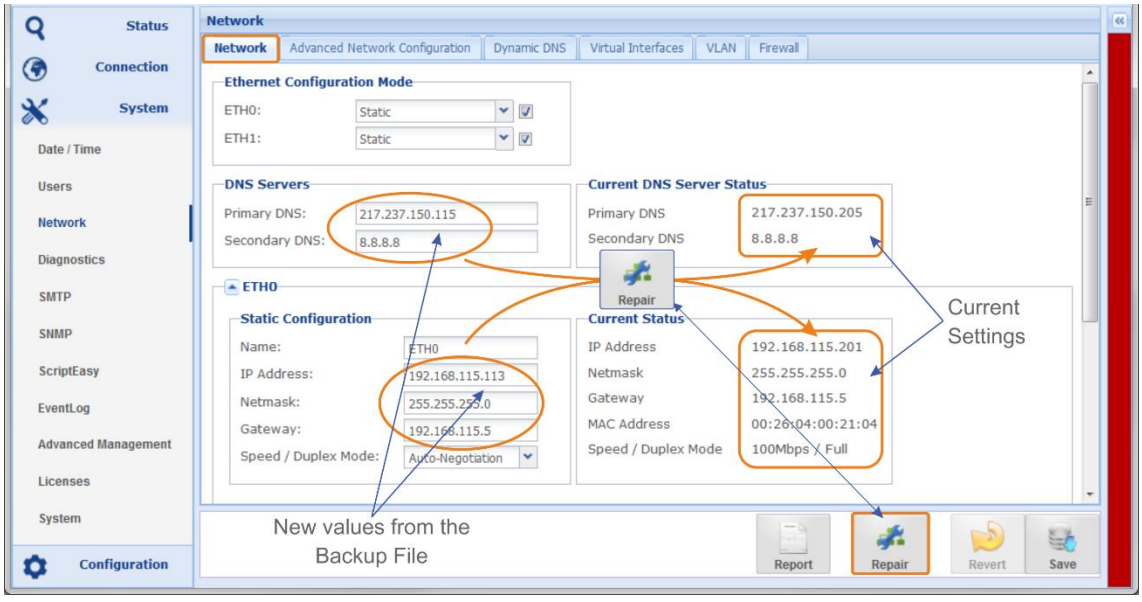


Figure 3-71 shows the network page after a backup file was loaded; network parameters are different from the current status. Clicking on "Repair" applies the network setting from the backup file.

3.5.10.5 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.

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

About – System Firmware

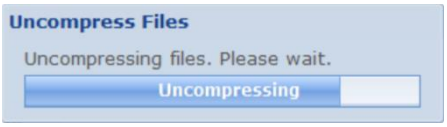
A Firmware release consists of a set of inter-compatible firmware files. These are system files for the DSP, the system operational system, and the WEB GUI. A system release will always be delivered as a Zip-Archive.

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

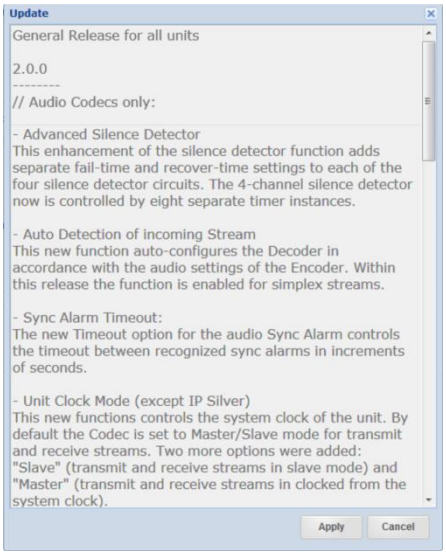
Clicking on the "Update" button opens the PC file browser. Navigate to the folder where the firmware file is stored and select the zip-archive (HZNG_IP_CODEC_SR_x_x_x.zip). Confirm your selection and proceed with the firmware update.

The progress bar indicated the current status during the file upload.

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

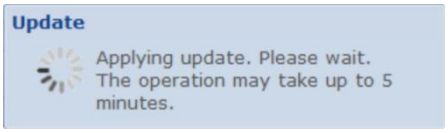


Once the firmware archive is successfully uncompressed and verified, the window with the release note appears. The release note contains the most important information about new features, bug-fixes and other changes in the new firmware.



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.*

3.5.11 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: This license is a cost option. Please contact your APT sales office for more information.
- Digital MPX: This license is a cost option. Please contact your APT sales office for details.

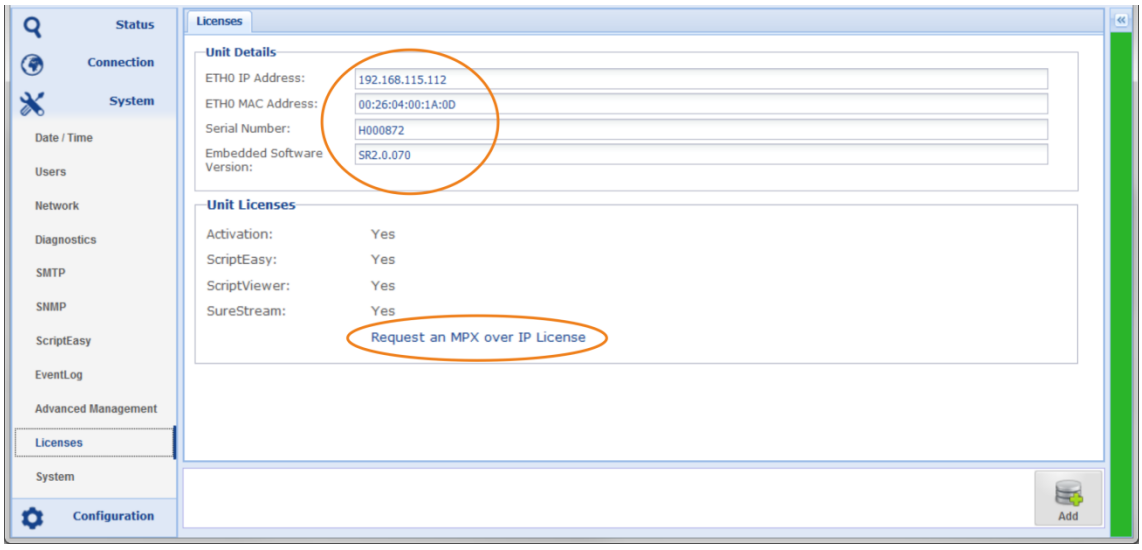


Figure 3-72: Shows the unit parameter for getting an options license

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.

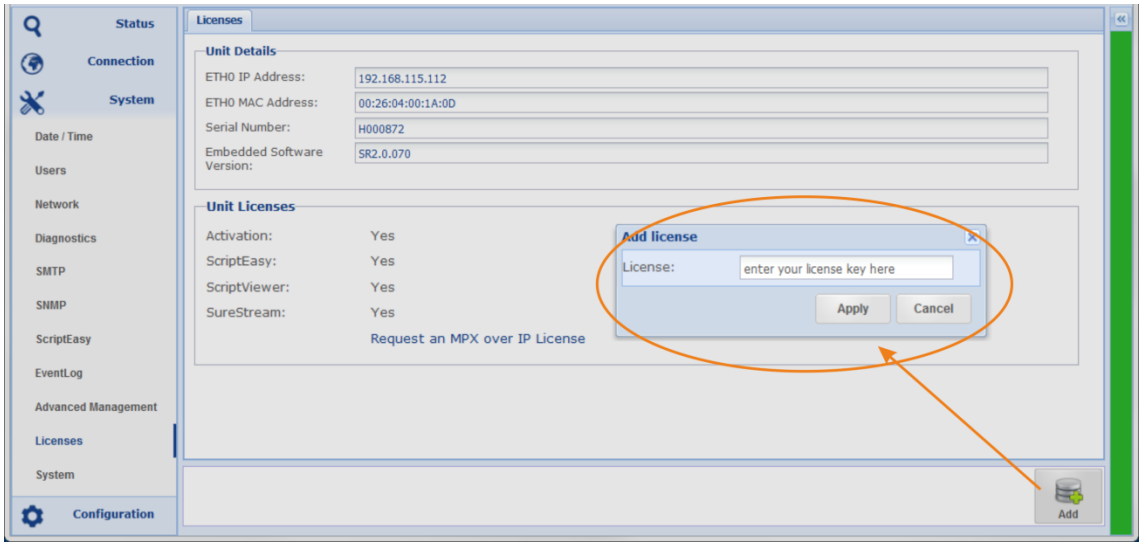


Figure 3-73: Shows how to apply a new license key to the system

Notes:

3.5.12 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 particular 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.

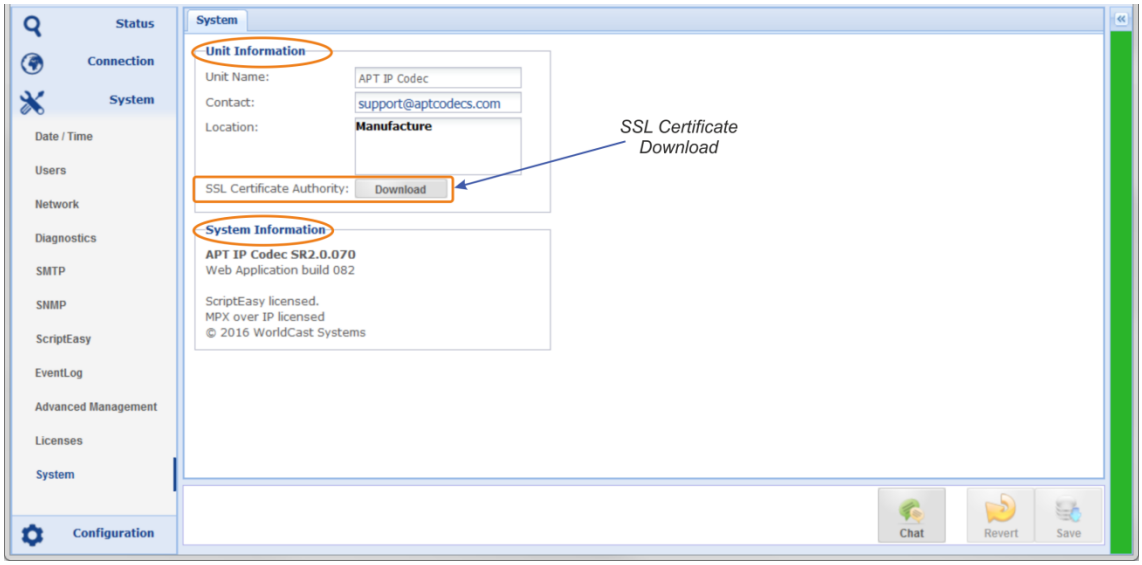


Figure 3-74: Shows the "System" page of the System menu

3.5.12.1 SSL Certificate Authority

Download the SSL certificate as shown in Figure 3-74: Shows the "System" page of the System menu 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.

3.5.12.2 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.

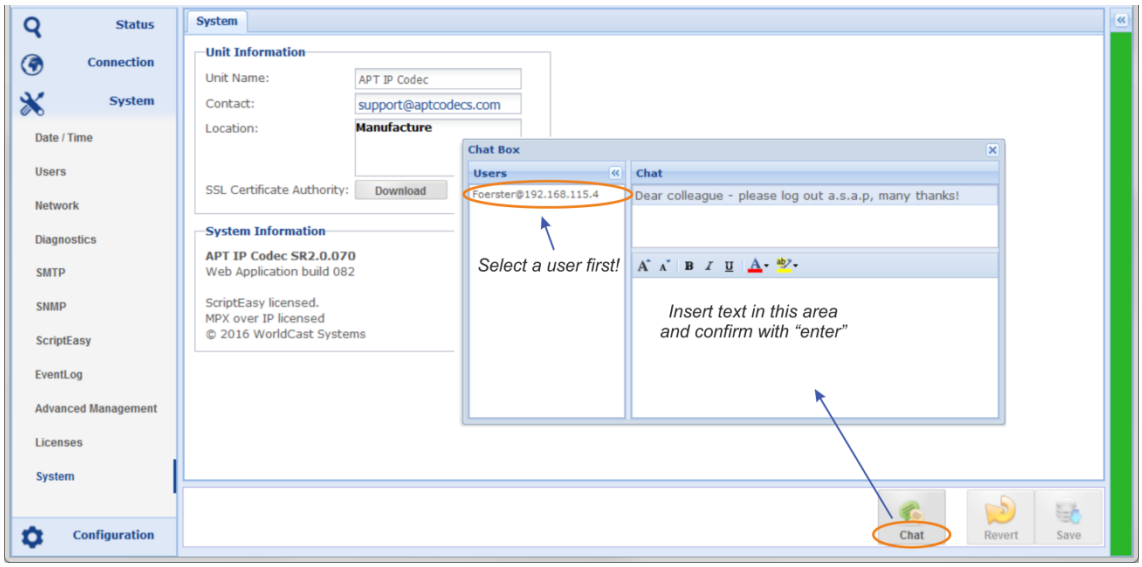


Figure 3-75: Shows the "System" page of the System menu with Chat Box open

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.

ⓘ *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.

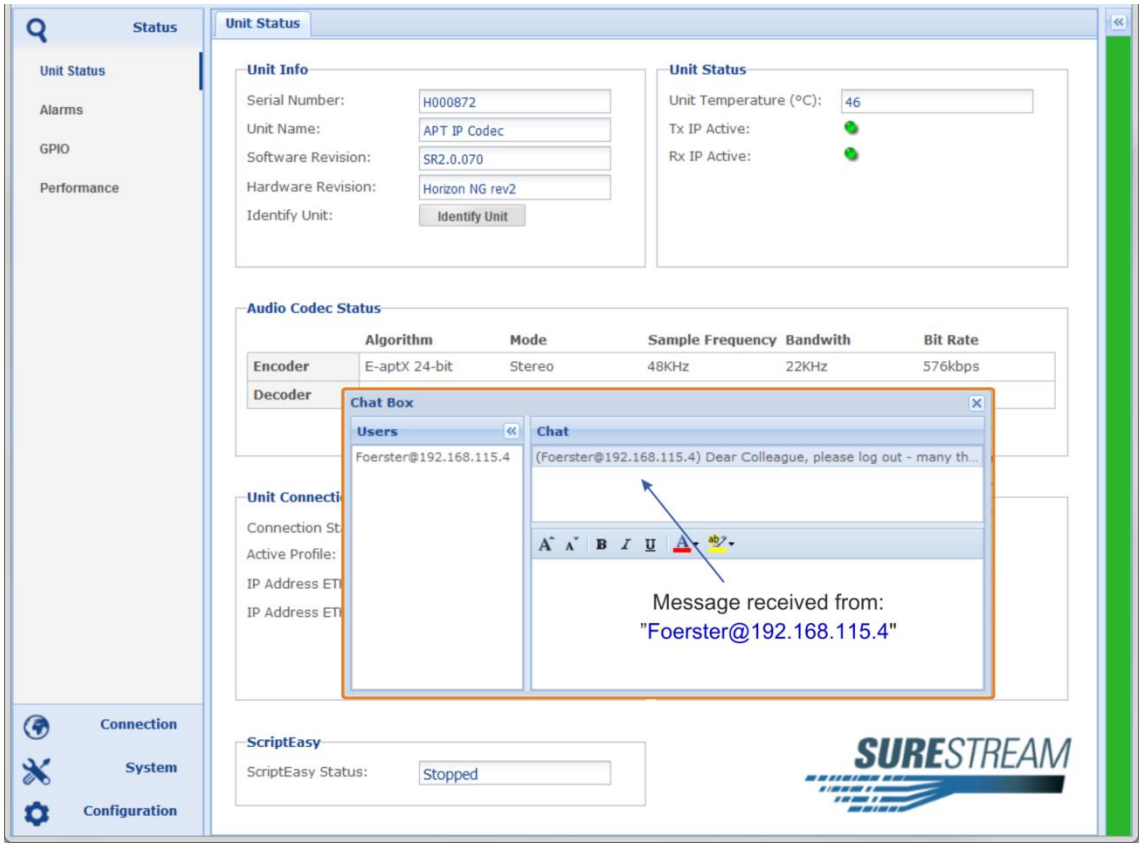


Figure 3-76: The chat box pops up when a message is received

3.6 Main Menu – Configuration

The configuration menu provides four submenu items, the Audio Configuration page, Network Alarms, the AUX Data/GPIO page and the alarm configuration page. These are basic configurations controlling operational modes and system behaviors.

3.6.1 Audio Configuration

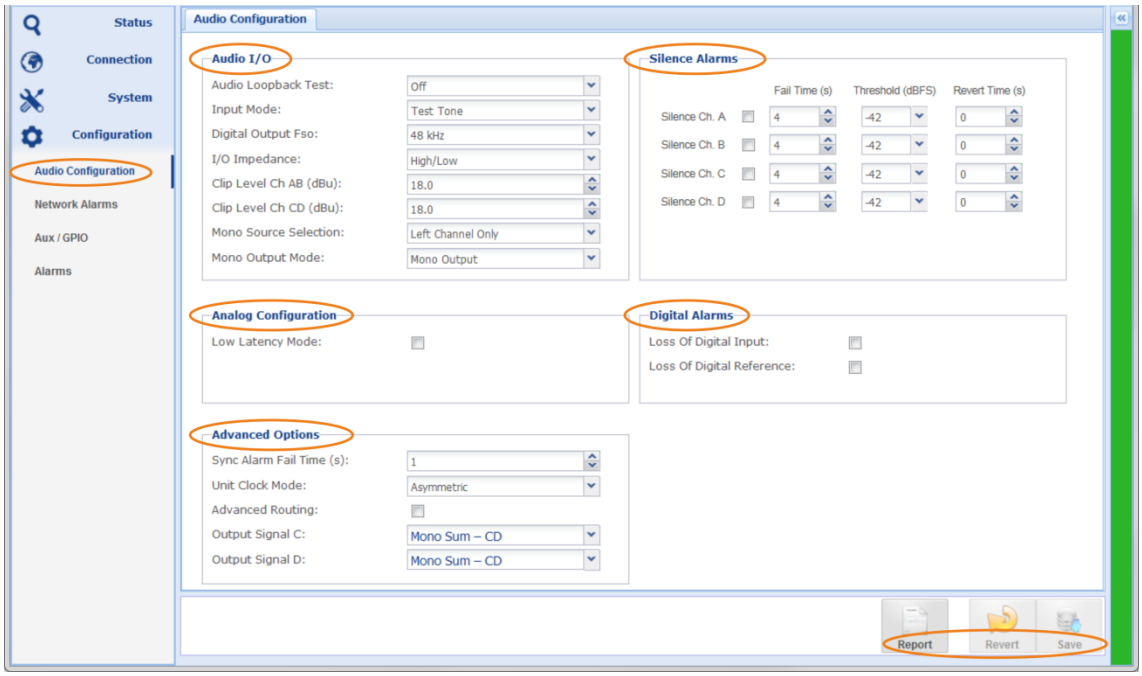


Figure 3-77: Shows the Audio Configuration page

All setting can be reverted or saved by clicking on either of the buttons as shown above. All configuration options are described on the following pages.

Notes:

3.6.1.1 Audio Configuration

This section provides the following configuration options (listed for Duplex operation):

Configuration	Options	Description
Audio Loopback Test	Off Local Loopback	This is the normal operational mode Enables a local audio loop between Input and Output
Input Mode[1]	Analog Digital Test Tone	Selects the Analog Inputs to be active Selects the Digital Inputs to be active An internal generator applies a 1 kHz tone for test purposes to the audio inputs
Digital Output FSO	32, 44.1, 48, 96, 192 kHz[2] Ref.	Sets the Digital Output sample frequencies Allows synchronizing the Digital Outputs to an external clock such as AES-11
I/O Impedance	High/Low 600 Ω/600 Ω	Analog I/O impedance: In: >10 kΩ, Out: <50 Ω The I/O impedance is set to 600/600Ω
Input Clip Level (dBu)	Values 6-24 dBu	Adjusts the analog Input level in reference to the digital dBFS in increments of 0.1 dB
Output Clip Level (dBu)[2]	Values 6-24 dBu	Adjusts the analog Output level in reference to the digital dBFS in increments of 0.1 dB
Mono Source Selection	Left Channel only Mono Sum ((L+R)/2)	This describes the signal source (input) for a mono mode of a mono audio algorithm. This selection takes both input signals (left & right) and divides it by 2 (-3 dB)
Mono Output Mode[3]	Mono Output MonoFill	Mono Output on left channel only MonoFill copies the signal also to the idle channel; mono output on L & R connectors

[1] The analog and the digital outputs are always active simultaneously
[2] Analog Outputs are non-functional when 96 or 192 kHz is selected.
[3] MonoFill cannot be used together with the advanced routing option as the two features stay in a conflict

3.6.1.2 Analog I/O Clip Levels

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

All level readings are referenced to the digital domain where 0 dBFS=+24 dBu.

For example, if the analog level of +6 dBu shall equal -9 dBFS then the **analog clip** level (shall equal 0 dBFS) must be set to +15 dBu (0 dBFS=15 dBu, -9 dBFS=+6 dBu).

Audio Configurations *(continued)*

3.6.1.3 Analog Configuration – Low Latency Mode

This "Low Latency Mode" affects 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 for modes with FS = 48 kHz, e.g.:

- Linear PCM at Fs = 48 kHz
- AptX® Enhanced at Fs = 48 kHz
- and other algorithms supporting Fs = 48 kHz

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 Fs = 32 kHz) then this mode is automatically deactivated regardless of the enable/disable status on this configuration page. As long as this mode is enabled, it automatically takes place if an audio mode at 48 kHz is selected.

3.6.1.4 Sync. Alarm Fail Time

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.

3.6.1.5 Unit Clock Mode

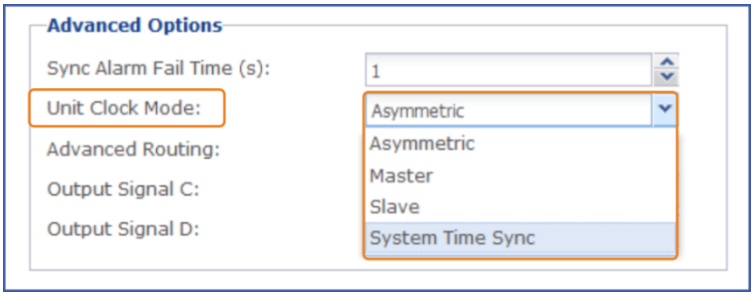


Figure 3-78 shows the Unit Clock Mode selection

- **Asymmetric**:
  By default, the Codec is clocked asymmetrical if it is set to duplex mode. Asymmetrical clocking guarantees a flawless anywhere-to-anywhere streaming. In this mode, the Tx stream is clocked from an internal or external source in the Encoder while the receiving Decoder derives the system clock from the packet interval utilizing its VCXO. Asymmetrical clocking avoids buffer underrun and overflow events.
- **Master**:
  This mode uses the internal crystal for sending a stream (Tx) and for receiving a stream (Rx). This mode is only useful in a LAN environment or in a network with no or very low delay jitter.
- **Slave**:
  This clock option uses the internal VCXO for sending (Tx) and for receiving (Rx) streams. If a stream is received, the VCXO adapts to the buffer condition. In this case, the Tx clock follows the VCXO.
- **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 3.6.2.*

Notes:

Advanced Options *(continued)*

Advanced Routing & Decoder Mono Mode

The technical description is available in section 3.6.1.6.

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 co-dec. 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.

Digital Alarms

Digital Alarms are used to monitor the presence of the digital audio signal and the digital reference input.

Configuration	Options	Description
Loss of Digital Input	Enable/Disable	Enabling this checkbox will flag this alarm if the digital source at the digital input is lost
Loss of digital Reference	Enable/Disable	Enabling this checkbox will flag this alarm if the digital reference signal at the reference input is lost

Silence Alarm Configurations

These alarms are Silence Detector alarms. These settings allow enabling the alarm for each Input and Output channel (A/B/C/D). You can set the Fail Time, the threshold level and the Revert Time each of the channels separately.

- Fail Time: Defines the duration the alarm condition must exist before the alarm is flagged
- Threshold: Defines the level in dBFS the signal must not fall below for the duration defined as Fail Time.
- Revert Time: Defines the duration the level must be higher than the threshold level before the alarm is reverted.

3.6.1.6 Advanced Routing & Decoder Mono Mode

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

1. Creation of Mono signals from incoming stereo IP streams
2. Advanced Routing of the output signal

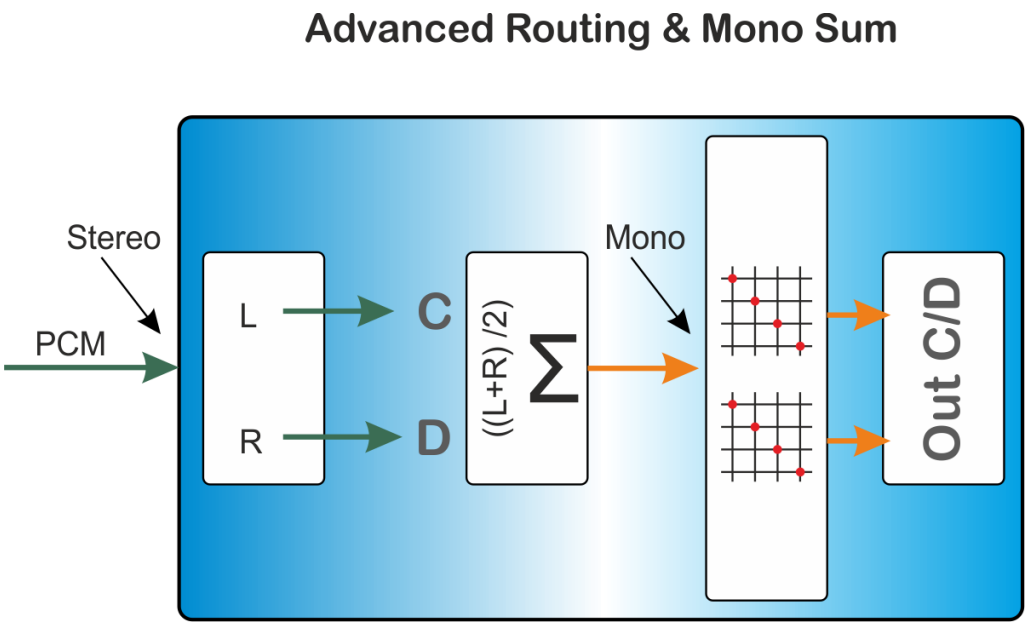


Figure 3-79: Shows the principle of this feature of the Decoder

Decoder Mono Mode

This feature allows creating 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.

3.6.2 Program Time Alignment

If you set your system time to NTP time (section 3.5.2) and select the "System Time Sync" clock mode (section 3.6.1.5), you can correct 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 10-15 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.

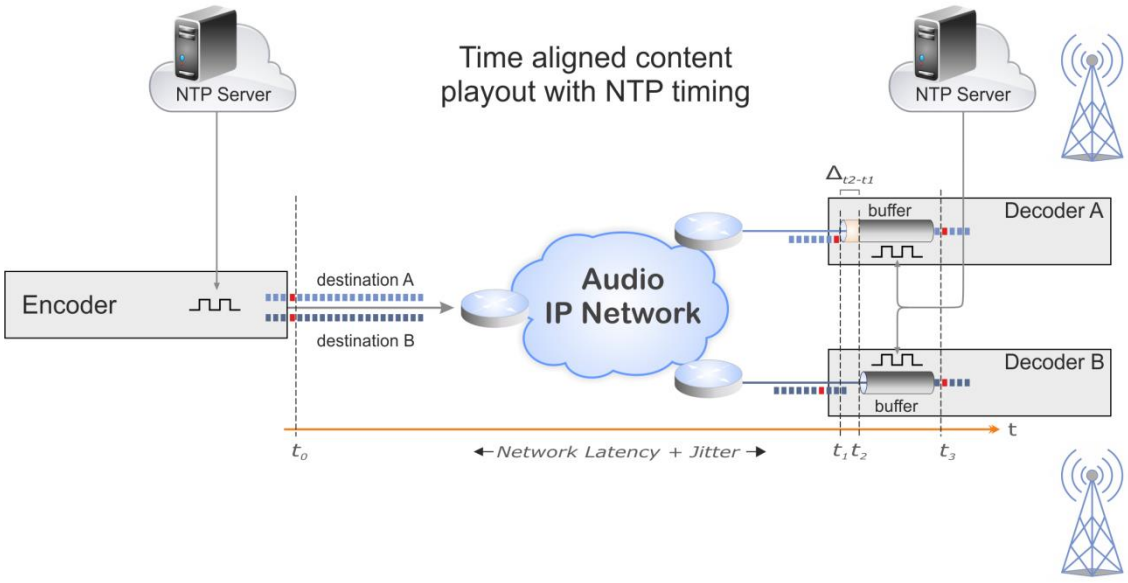


Figure 3-80 shows the principle of time aligned content playout

3.6.3 Network Alarms

This page provides the alarm options of the Ethernet interfaces and Dynamic DNS.

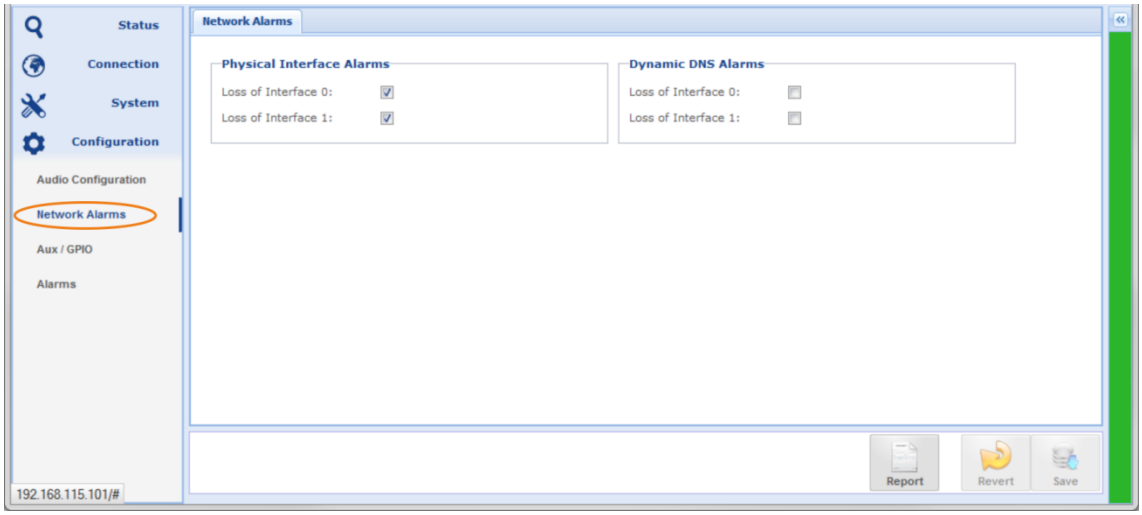


Figure 3-81: Alarm configuration options of Ethernet ports

Enable/Disable alarms for physical loss of connections.

If this alarm disabled, a physical loss of connection would not be recognized as alarm

Enable/Disable alarms of Dynamic DNS connection

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

Notes:

3.6.4 AUX/GPIO Configuration

This page manages the Switch Inputs (GPI), the relay behavior (GPO) and the Aux data rate settings.

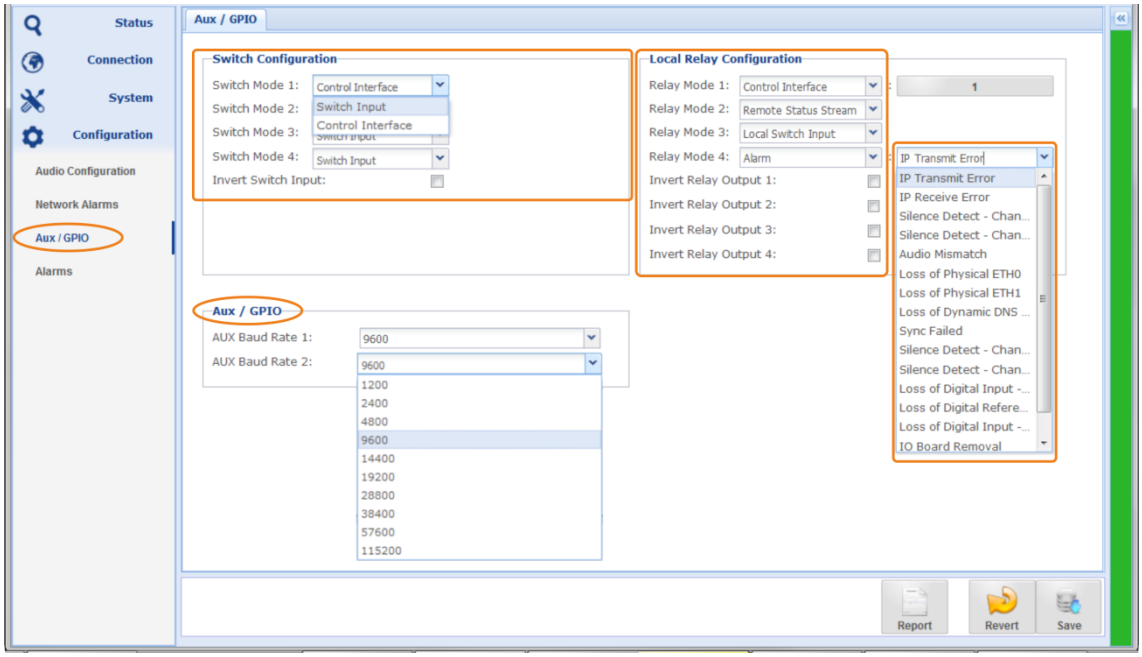


Figure 3-82: Shows the AUX Data and GPIO configuration page with all options

3.6.4.1 Local Relay Configuration

You can control the relay contact closures in four ways:

1. From a control button on this page (control Interface)
2. By GPI commands from the remote site via IP connection
3. By the LOCAL switch input of this unit
4. For an individual alarm per relay or a group of alarms (custom alarms)

A set of checkboxes allows you to invert one or more individual relay outputs.

ⓘ *The AUX data interface allows sending and receiving RS232 data with baud rates selectable from 1.200Baud to 115.200Baud. Note: For embedded mode, the data rate is max. 9.600Baud.*

ⓘ *GPI inputs are combined into a single data stream or embedded with aptX® Enhanced. Only aptX® Enhanced allows embedding both the AUX data and GPI signals.*

AUX / GPIO Configuration Options

Configuration	Options	Description
Switch Configuration	Switch Input	Controlling the relays on the remote and/or local unit by driving the switch input on the rear of the local Codec.
	Control Interface	The control interface is the WEB GUI. Selecting this mode allows controlling the remote and/or the local relays from this configuration page.
Invert Switch Input	Enable/Disable	Non-inversion: Local switch active, remote/local relay active Inverted Mode: Local switch inactive, remote/local relay active This inversion is valid for all four switches
Local Relay Configuration	Alarm	The selected alarm condition activates this relay
	Control Interface	Allows activating a relay by a control button on this page
	Remote Status Stream	Follows the switch command received from the remote end
	Local Switch Input	Follows the local Switch Input commands
Invert Relay Output	Enable/Disable	checkboxes allow you to invert one or more individual relay outputs
AUX Data Baud Rate	Value	The drop down list provides baud rate setting from 1.200 to 115.200 baud

Note: For embedded mode, the data rate is max. 9.600 baud.

Notes:

3.6.5 Alarms Configuration

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

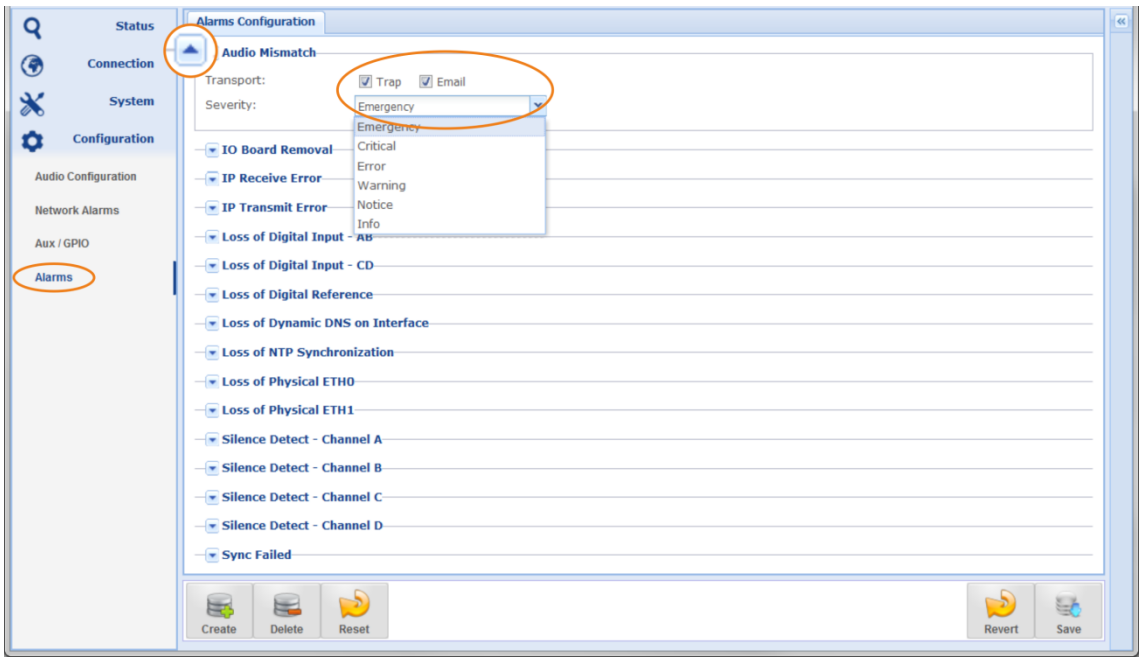


Figure 3-83: Shows the Alarms Configuration page

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 can be found on the SNMP page.

- **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 3.5.6.

- **Severity**

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

3.6.5.1 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.

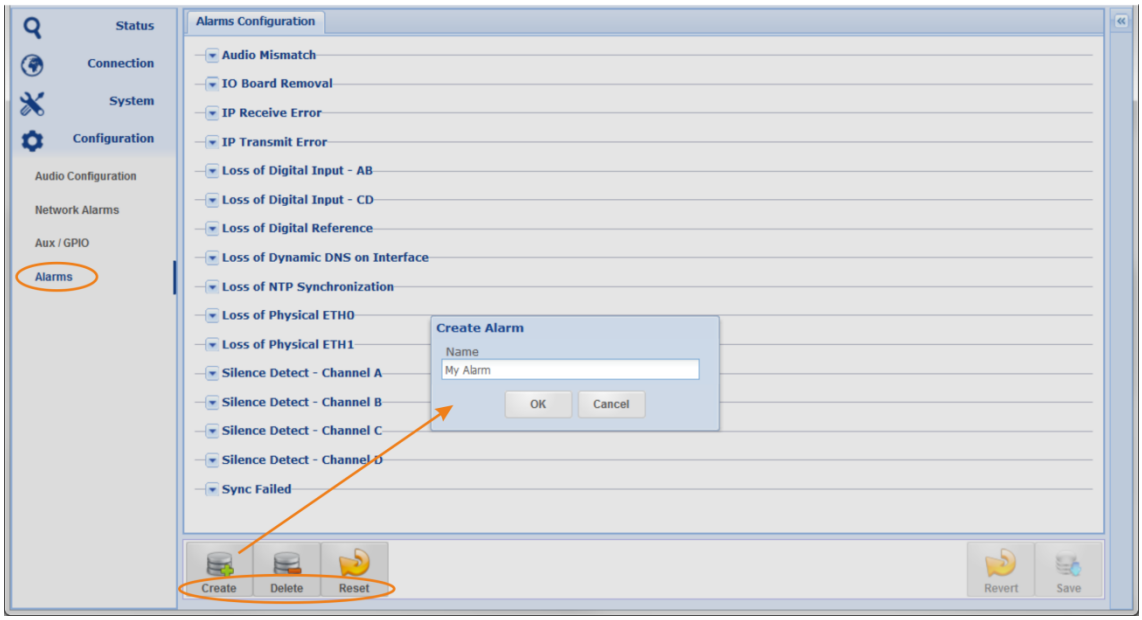


Figure 3-84 How to create a group of Alarms - apply a name to the new group and save it

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.

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.

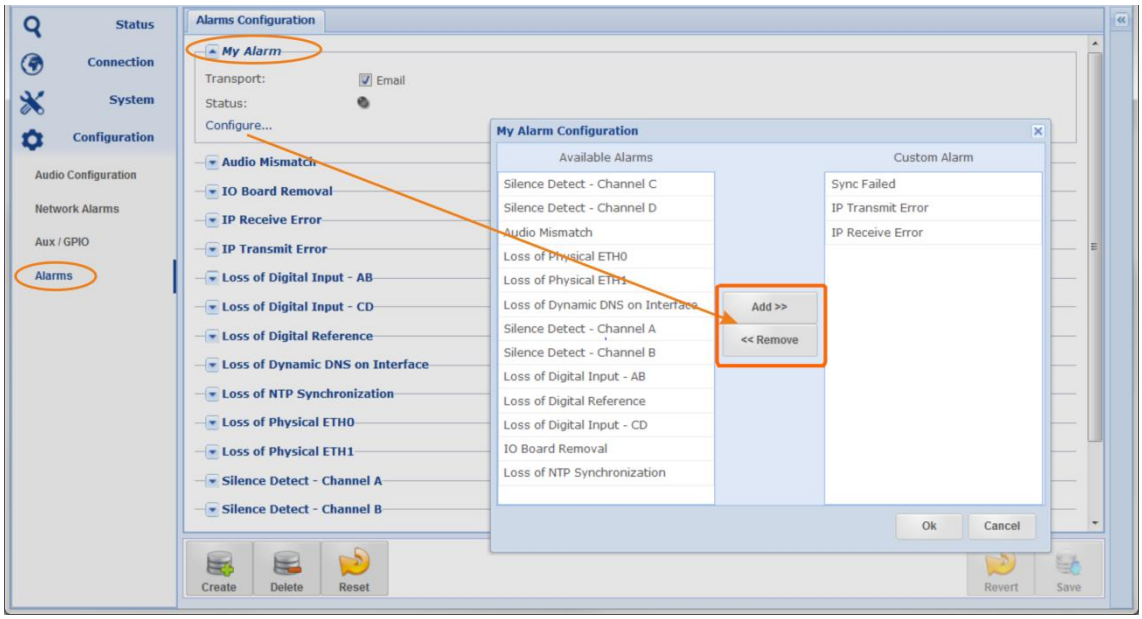


Figure 3-85: Shows how to create an alarm group

- Once this alarm group is created, the email alert can be enabled. This new alarm group is available on the relay configuration page and treated as a single alarm.

Notes:

4.0 SureStream Option

The SureStream option is not a standard feature and must be applied to the unit by entering a license key.

Once a SureStream license was applied to the unit, the Status Page will indicate the availability of SureStream by presenting the SureStream Logo. For requesting a SureStream License, please refer to section 3.5.11 (System Licenses).

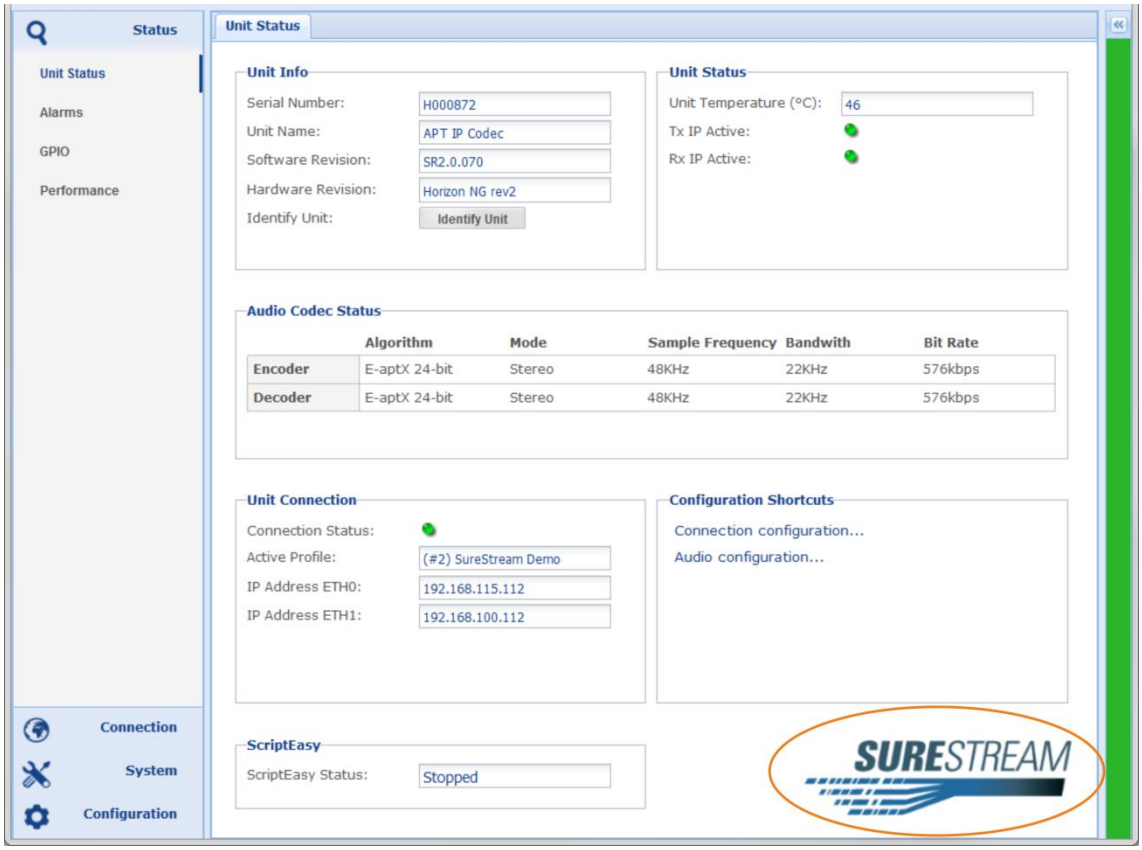


Figure 4-1: Shows the Status Page with SureStream license applied

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)*

SureStream is highly efficient on potentially lossy networks like the public Internet. It can also be used for permanent redundant streaming on managed networks.

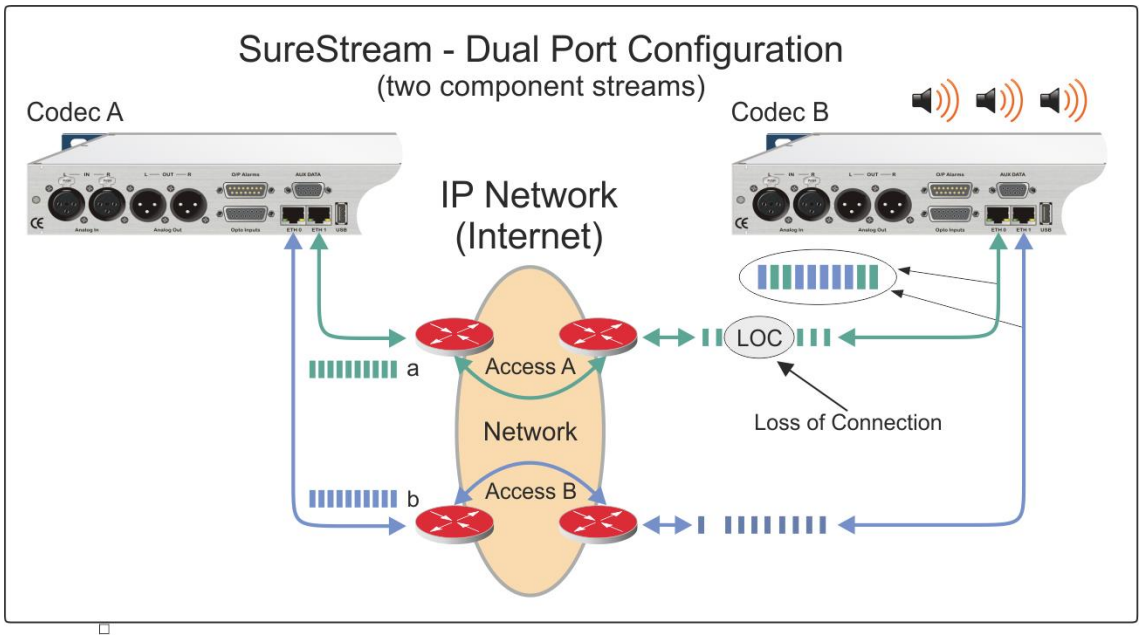


Figure 4-2: Shows a typical Dual Port Configuration running SureStream

The configuration example above shows a SureStream configuration using both streaming ports utilizing two component streams; as many as required redundant streams could be generated. This example uses the internet with standard xDSL access services. Diverse streaming on the internet has the effect that the access routers treat each component stream individually by passing it randomly on different paths to the destination IP address.

On the receiving end, the Enhanced Re-Sequencer generates the single packet stream from all component streams on a first-in-first-out packet basis. All duplicated and redundant packets are dropped.

4.1.1 SureStream Encoder

On the Encoder side, the heart of SureStream is the Statistical Diversity Generator. This generator ensures that the redundant streams appear on the network as diverse as possible. This generator runs an algorithm that can be optionally set up with three additional sets of parameters (called "levels"). These levels allow the use of more than one redundant stream on the same network interface while keeping each stream divers from each other. On a dual interface configuration as shown in Figure 4-2, the network as such maintains the stream diversity without adding diversity levels.

4.1.2 SureStream Decoder

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

4.1.3 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/GPIO, forwarding).

The screen shot below shows a SureStream group from the Encoder site with bi-directional streams. 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.

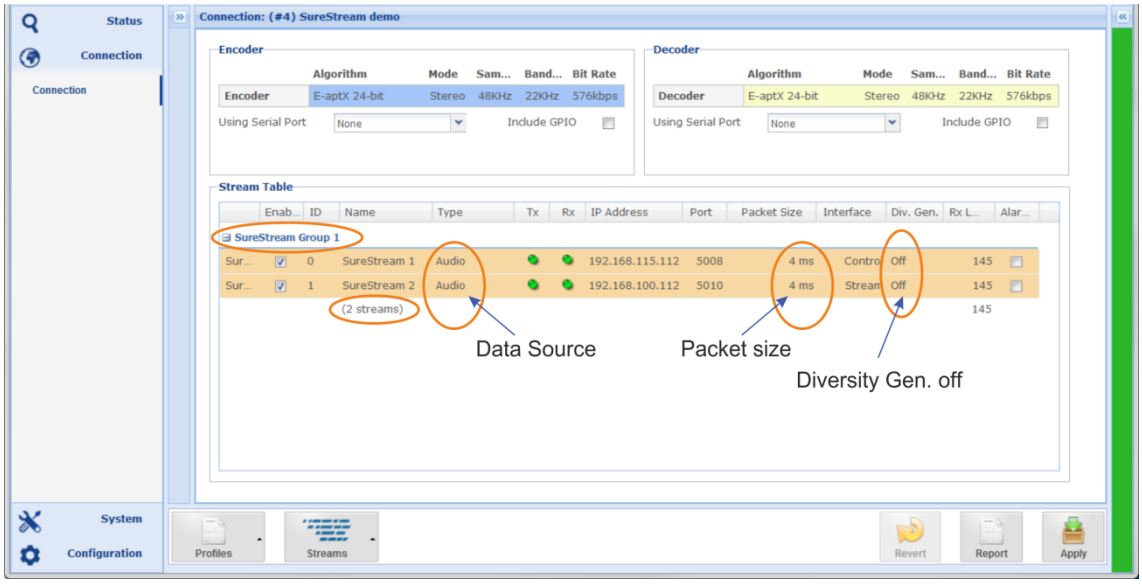


Figure 4-3: Shows a SureStream configuration on the Encoder

The figure above shows the Encoder settings. Both streams are assigned to the same remote unit but to different destination IP addresses. Hence, the streams are received on two ports at the Decoder. This implies that the streams are sent through different paths from the Encoder into different networks. – This is the ideal configuration and utilizes the full potential of the SureStream technology.

It is not required to enable the Diversity Generator in these settings; usually, the two different networks ensure a sufficient diversity.

For streaming through the internet on two separate xDSL lines, it is preferable to use two different providers. By doing this, the chance getting the streams routed differently is much higher. Hence, the reliability of the link increases significantly.

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

SureStream – Encoder Configuration *(continued)*

Once the SureStream license was applied to the unit, the Diversity Generator option appears on the stream configuration window. Again, creating a group of component streams follows the standard procedure.

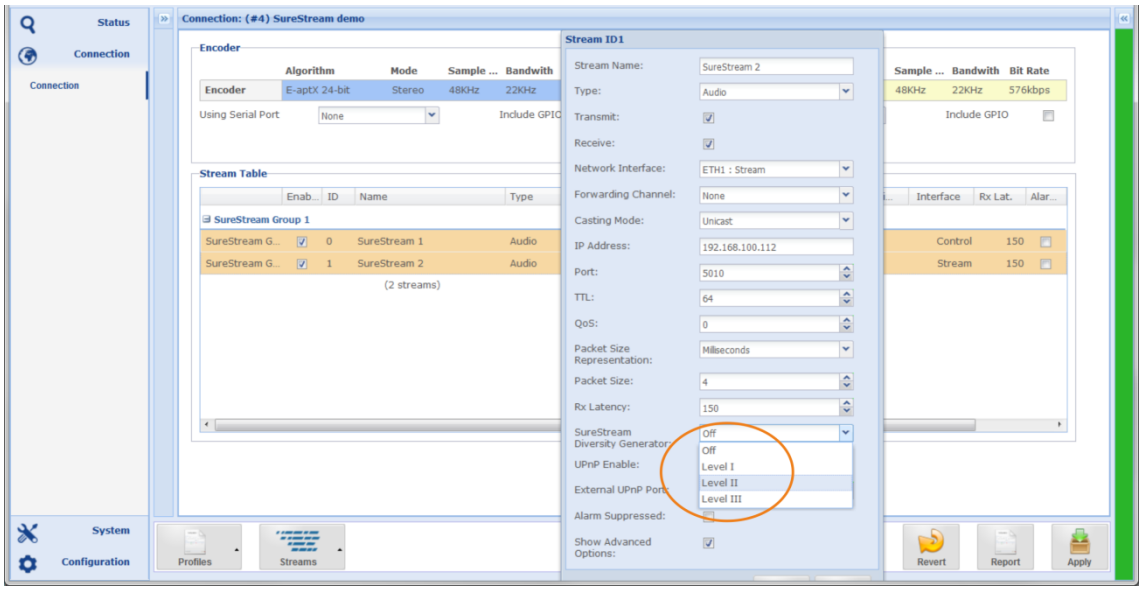


Figure 4-4: Shows the Diversity Generator options on the stream configuration window

4.1.4 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.

In situations where both ETH ports are connected to different networks, the diversity generator might become obsolete because the networks already ensure sufficient diversity.

ⓘ *In a configuration where both ETH ports are used for only one component stream on each port (two streams in total), the Diversity Generator Level settings should be switched OFF on both streams.*

ⓘ *Using both ETH ports implies that two different networks are used. With this condition, the different networks create already the desired diversity of the component streams.*

4.1.5 Creating a Set of redundant 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 works 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 (or default)– there are no constraints for applying a name
Stream Type	SureStream supports "Audio" and "Media Forward (RTP)" streams only
Transmit Mode	SureStream supports "Transmit" mode
Receive Mode	SureStream supports "Receive" mode
Transmit/Receive	SureStream supports "Duplex" mode
Mode	SureStream supports "Unicast and Multicast."
Dest. IP Address	This can be the same for all streams, but SureStream works more efficient if both ETH ports are used, hence the destination IP address should be different (receiver uses two ETH ports – on different networks). In a single ETH port configuration, the target IP address is mostly the same on all component streams.
Port	For each stream - the IP port **must be different**
TTL	For all streams - the TTL value **must be equal**
QoS	For all streams - the QoS setting **must be equal**
Packet Size	For all streams - the Packet Size must be equal (linked)
Physical Port	Streams can/should use both ports: ETH0 and ETH1
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 Levels	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.

ⓘ *Note: SureStream, in general, can be used in a stream table for simplex streams (individual Receive or Transmit streams).*
SureStream can also be used on a stream table for bi-directional streams (duplex streams).
BUT component streams CANNOT be configured as simplex AND bi-directional streams in the same stream table or the same profile.

4.1.6 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 is always decoded while the data of the stream type "Media Forward receive" is never decoded but 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 re-combiner, and the re-sequencer are the complementary parts of the stream diversity. The re-sequencer is always enabled and expects a minimum of six IP packets in the buffer to unfold his full performance. If the buffer size is smaller than the size of six packets, the validation engine flags a yellow warning, but the re-sequencer continues to work.

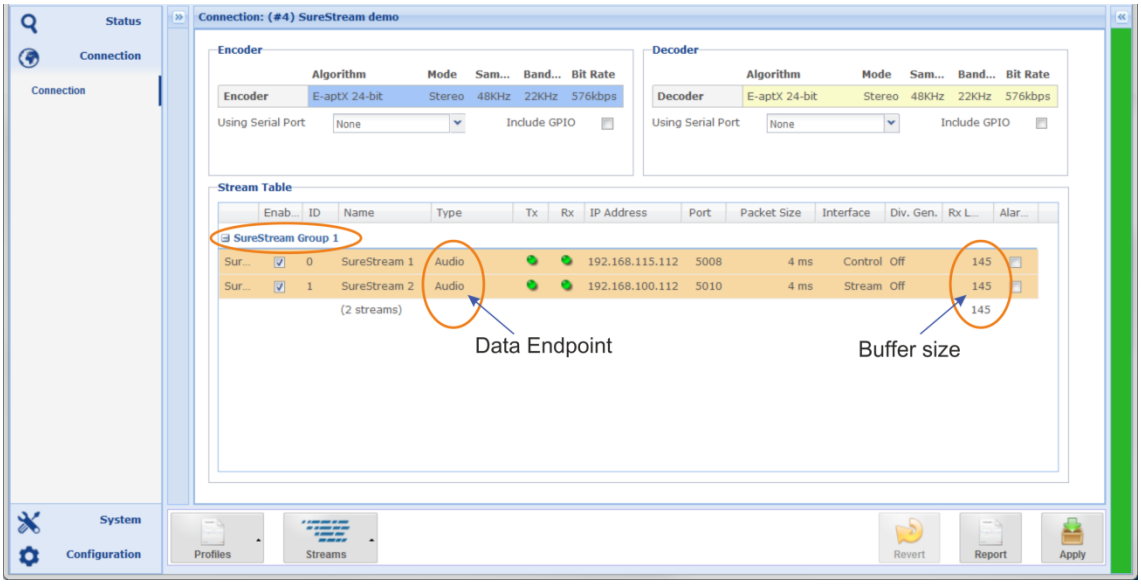


Figure 4-5: Shows a SureStream configuration on the Decoder with two streams received

The figure above shows a Decoder configuration with bi-directional streams. The two component streams are received on different ETH interfaces ("Control" and "Stream"). Hence they are transmitted through different network paths at the Encoder (as shown in the Encoder section).

4.1.7 SureStream – Performance Monitoring

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 re-combiner, it is not directly visible on the performance monitor. There are two ways of monitoring the SureStream performance:

- Deriving performance information from the component streams
- Creating a monitor stream, making the recombined stream visible (section 4.1.7.2).

4.1.7.1 Deriving Performance Information from the Component Streams

Without a monitor stream, the performance of the recombined stream is included in the highest stream ID. The screen shot below shows the principle.

Stream ID 2 includes the packets of ID 2 AND the recombined stream. The number of duplicated packets is 50% of the total packet rate (displayed as "Duplicated Packets"). The statistics of stream ID 1 shows the packet count of a single stream.

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:

- 2 Component Streams
- 0 Dropped Packets of decoded content
- 10832 Duplicated Packets
- 0 LOC Events of decoded content

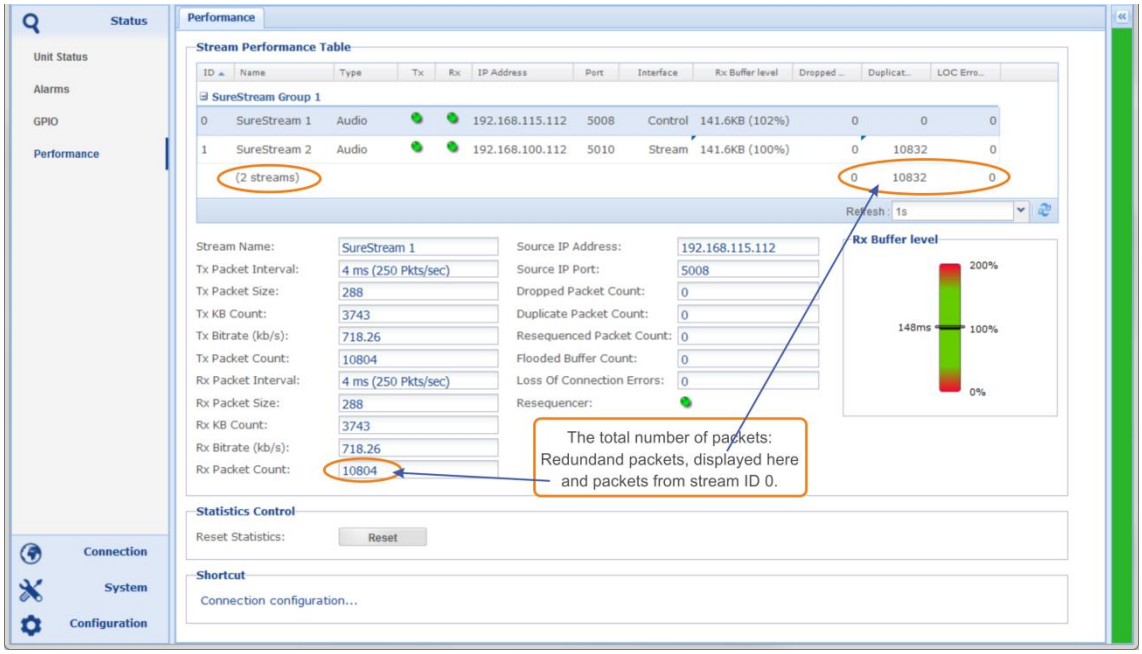


Figure 4-6: Shows the stream performance without a monitor stream

4.1.7.2 Creating a Monitor Stream

A monitor stream is one additional stream in a SureStream group on the RECEIVE site. 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 a bi-directional 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.

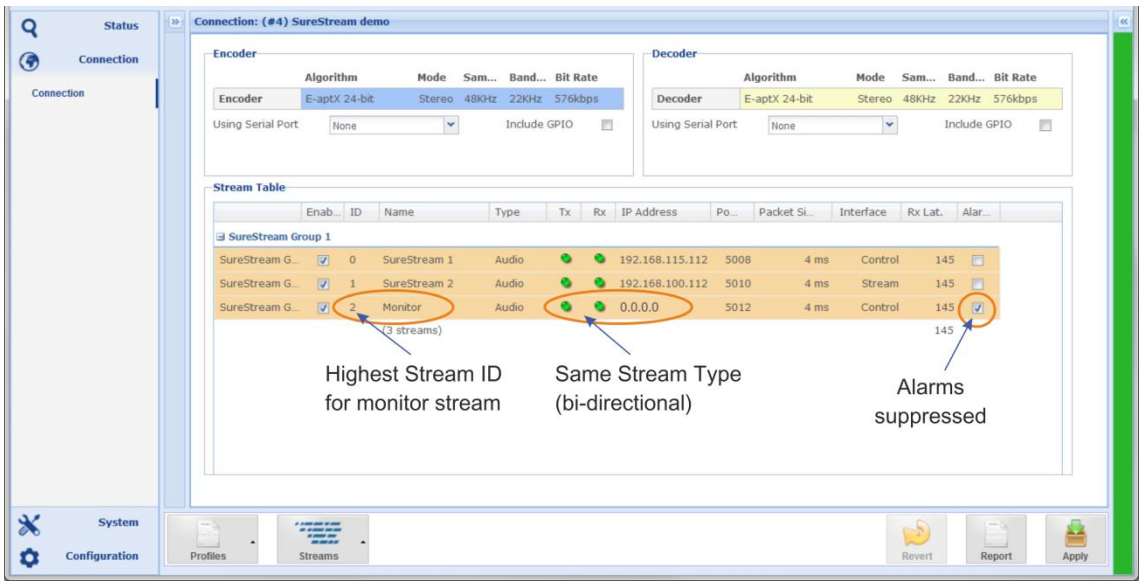


Figure 4-7: Shows a SureStream group with two component streams with a monitor stream

The stream table of the screen shot above is the same configuration as on Figure 4-5 but with the Monitor Stream. The monitor stream must be a duplex 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).

Notes:

4.1.7.3 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.

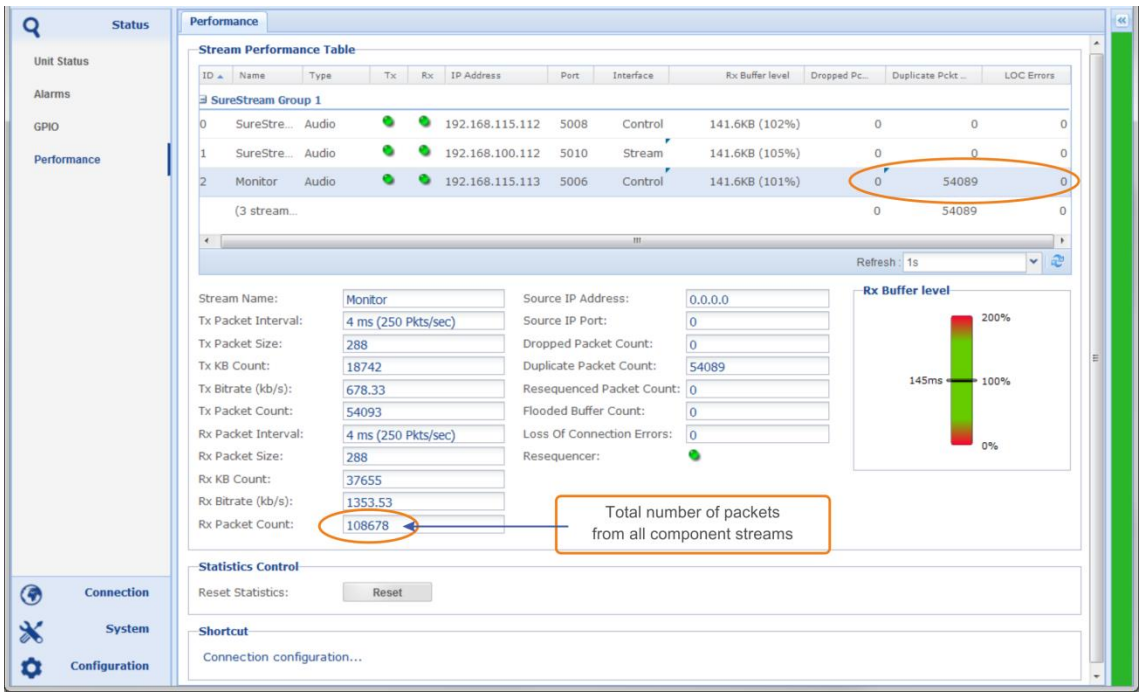


Figure 4-8: Shows the performance of the SureStream monitor stream

The performance figures of the monitor stream present the same IP statistics as described in section 3.3.4.

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 LOC should be 0. The number of duplicated packets is the sum of packets from all component streams minus the packet rate of one component stream. In the example above, the number of duplicated packets is about 50% of the total number (2 component streams).

Notes:

5.0 The WorldCast Management System (NMS)

The WorldCast Network Management System (NMS) allows monitoring multiple Codecs and modules 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 IP Codec module when accessed from the NMS family tree view. The presentation of the GUI of the IP Codec is the same when opened in the family tree view (NMS) or directly from a WEB browser.

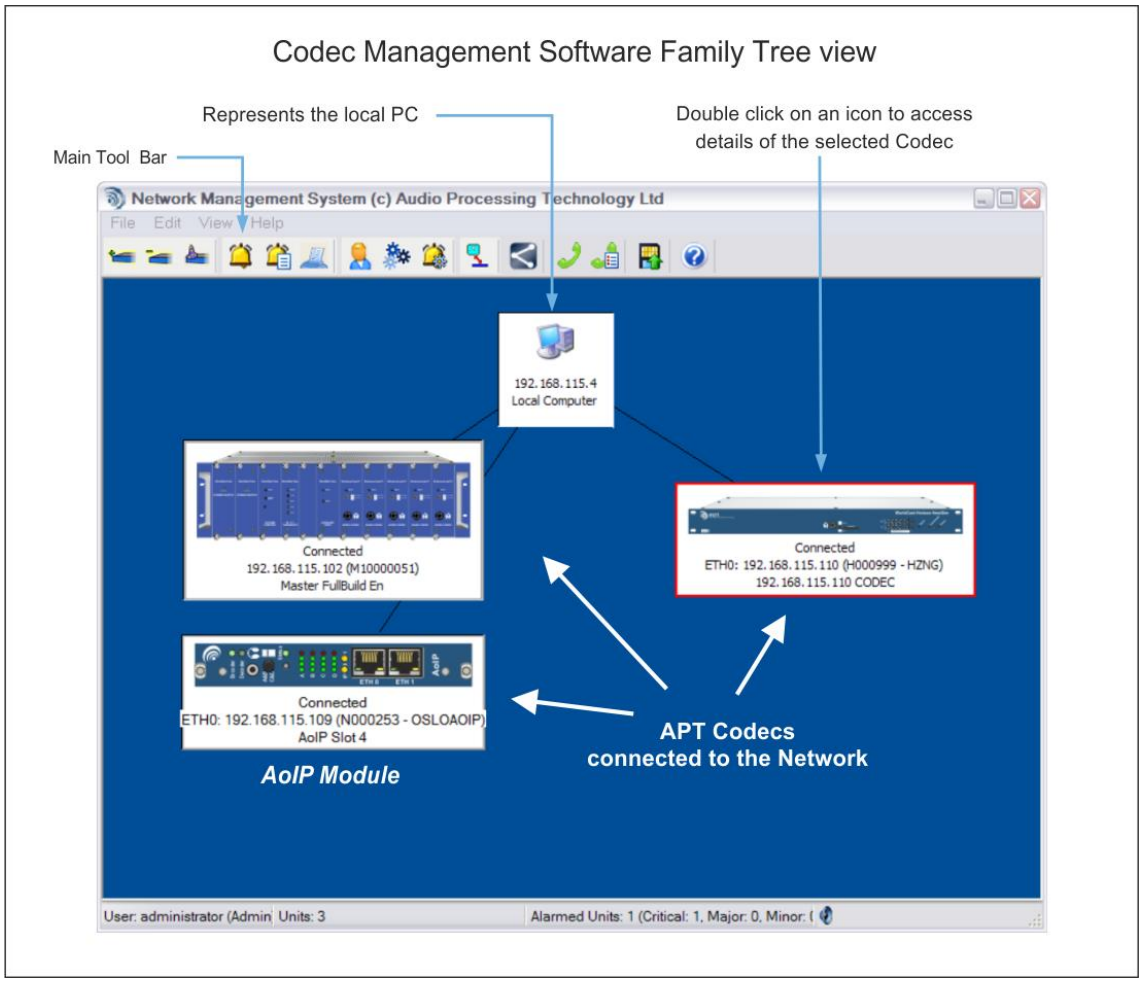


Figure 5-1 Family Tree of the Network Management System (NMS)

The presentation of the IP Codec *configuration pages is the same whether it is opened from the family tree view (NMS) or directly from a WEB browser.*

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.

The Codec Management System – *(continued)*

The Codec Management System is designed to operate as a program under Windows as a single task. This means that only one instance of the NMS software can be installed on the same PC.

Nevertheless, it is possible and allowed to have more than one installation of the **NMS** in the network. The NMS software design does not allow simultaneous access to the same Codec device from different seats with the same permissions. If one seat has opened a Codec device on the family tree, the software inhibits any attempt of accessing the same unit from another seat in read/write mode. The first user gets the read-write control of this particular device, and any other user will be restricted to read-only permissions. This feature avoids configuration conflicts caused by several seats.

Whenever a user opens a device on the family tree, the NMS sends out a broadcast request/announcement to the network looking for any other user actually configuring this particular unit.

ⓘ *If the network does not allow broadcasting, i.e. in public domain networks like the internet, this protection becomes ineffective.*

Notes:

5.1.1 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)

ⓘ *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).*

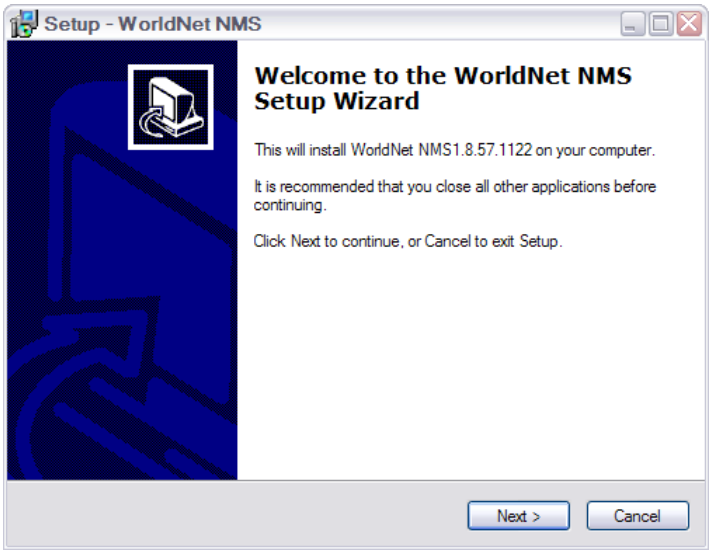
ⓘ ***The NMS requires IP port 7777 and 7778 to be opened on your network!***

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

First Screen

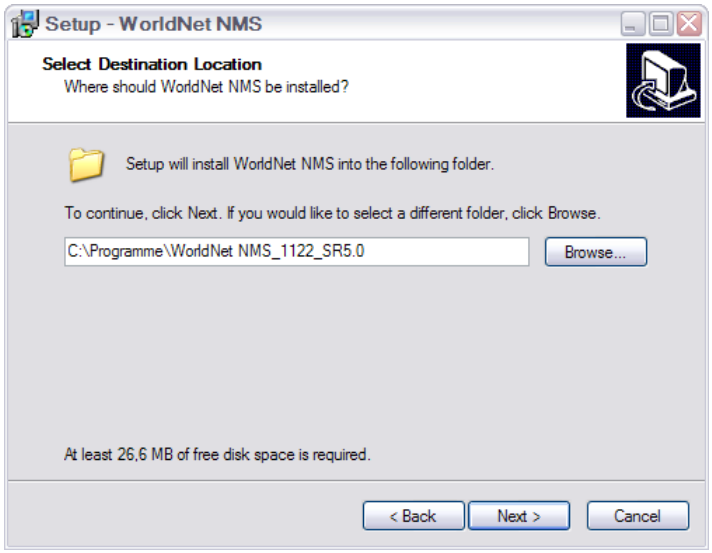
It shows the NMS build version; please make sure that you're installing the correct version, here build #1122.

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



Next Screen

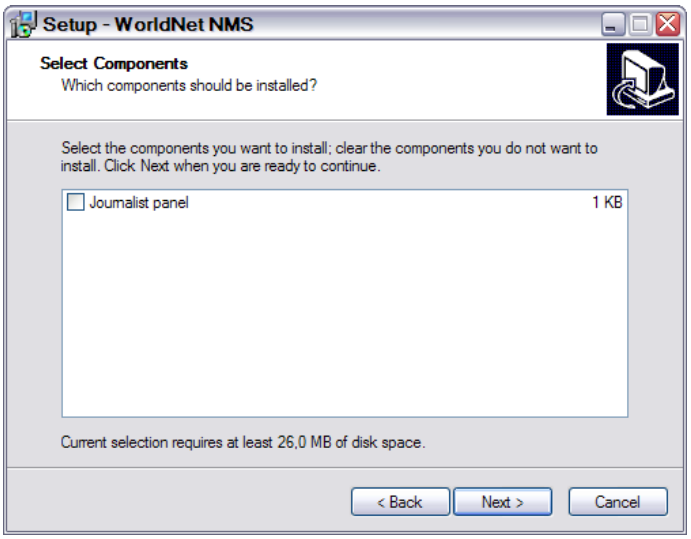
Please choose the folder where you like to install the NMS application.



Installing the Codec Management System *(continued)*

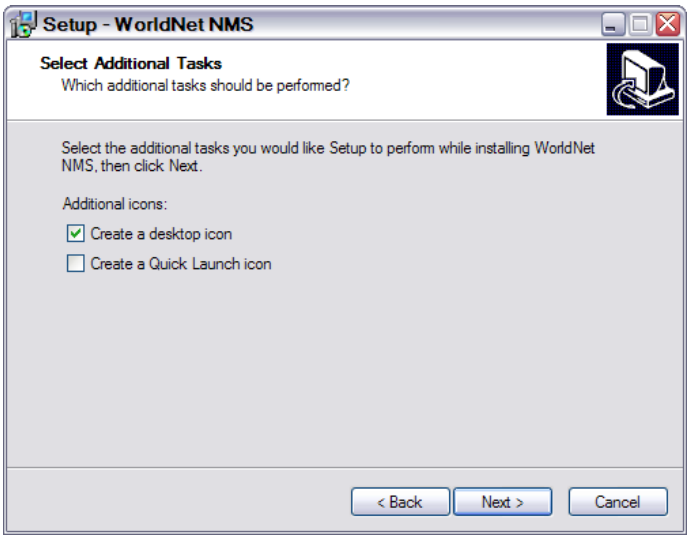
Next Screen

Journalist Panel is available for Eclipse/Meridian type Codecs only – do not select it unless you are also running Eclipse or Meridian units in your network.



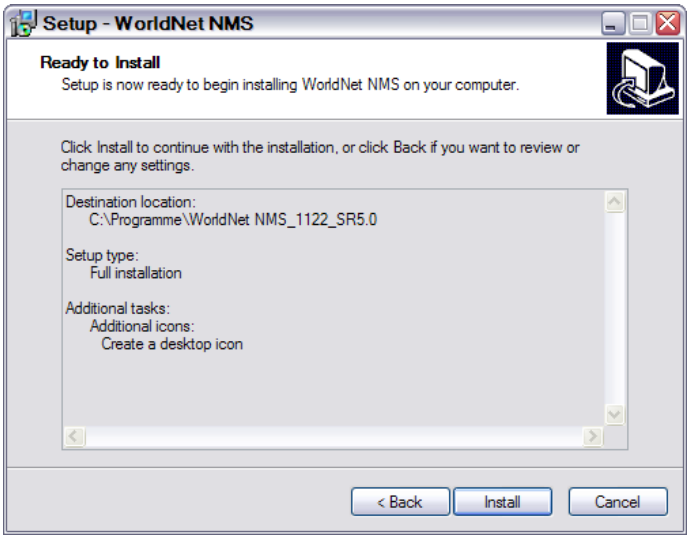
Next Screen

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".



5.1.2 Getting Started

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

ⓘ *To you open the NMS application, ensure that the cabling is properly connected from the Codec to the PC and that your service PC's Ethernet card has an IP address within the range of 192.168.100.0 to 192.168.100.255. All Codec IP interfaces are set to an IP address within this range as a factory default – usually 192.168.100.110.*

ⓘ *The NMS application remains 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 changing the Administrator login as soon as possible.

ⓘ *Default Username:* ***administrator***

ⓘ *Default Password:* ***password***

The manual of the WorldCast NMS system is provided with the software. You can find the full documentation as help file: Click on the menu "Help" and then again "Help."

6.0 Specifications

6.1 Specification APT IP Codec & IP Decoder

Physical	
Dimension	1U x 19” rack mount 44mm x 480mm x 160mm - 1.73” x 19” x 6.3”
Weight	<1.5kg / <3.355lbs
Environmental	0°C to +55°C, 95% humidity (non-condensing)
AC Power Supply	
AC Input Voltage	85-264VAC auto sensing, 47~440Hz
Input Inrush Current	Cold Start 65A max. (230VAC)
Input Current	0,4A/230VAC
Efficiency	81% typical
Total Output Power	21,6W
Output Voltage	12VDC
Hold Up Time	115V-16ms, 230V-50ms at full load
Over-Load-Protection / Short-Circuit-Protection	Above 105% rated output power (Hiccup mode, recovers auto-matically after fault condition is removed)
DC Power Supply	
DC Input Voltage	36-75VDC
Input Current	0.6A max
Efficiency	87.5% typical
Isolation	2250VDC
Total Output Power	25.2W
Output Voltages	12VDC
Short Circuit Protection	On all Outputs with auto Recovery

Analog Interfaces	
Interface Type	electronically balanced, capacitive isolated physical: on XLR3 connector
Audio channels	Duplex Mode: Stereo Input **and** Output (analog & digital outputs simultaneously active) IP Decoder: Stereo Output
I/O impedance Software selectable	High >10 kΩ Low <50 Ω or 600 Ω/600 Ω IP Decoder: Low <50 Ω or 600 Ω
Modes of operation	Stereo, Mono
Audio characteristics	Input to output: clip level: +24 dBu Analog Input/Output: adjustable by 0.1 dB increments in reference to the digital domain
Digital Interfaces (AES/EBU)	
Interface Type	AES3 transformer balanced or AES unbalanced (compatible with 75 Ω interfaces) physical: on XLR3 connector
I/O impedance	AES3: 110 Ω
Audio channels	Duplex Mode: 1x AES Input **and** 1x AES Output IP Decoder: 1x AES Output
Modes of operation	Stereo, Mono
Output sampling rates	32/44.1/48/96/192kHz & ext. ref. – software configurable
AES Reference	AES-11 reference input on XLR3 connector
SRC	Sample Rate Converter at Inputs and Outputs
General	
Diagnostics	Local loop back Integrated Test tone generator (encoder only) Ping Tool for each ETH interface
SD Card Audio Backup Supported File formats	SDHC – no size limitation FAT32 format .wav linear PCM .mp2 for MPEG 2 Layer II .mp3 for MPP3 files (VBR & CBR) .aac for AAC files with ADTS header (only)
Audio Modes	Mono L&R/2 on encoder and decoder (generates a mono signal from a stereo stream) , MonoFill mode on decoder which copies a mono channel to both outputs; Stereo
Audio Bandwidth	10 Hz – 22.5 kHz and 88/64 kHz for digital MPX (optional)
Dynamic Range	Up to >110 dB @ 24 Bit
Signal Processing	24 Bit Audio processing

Audio Formats and Coding Algorithms	
Linear PCM Digital MPX optional:	Fs = 32 kHz, 1024/1536 kbps (16/24 Bit stereo) Fs = 48 kHz, 1536/2304 kbps (16/24 Bit stereo) Fs = 192 kHz, 3072 /4608 kbps, 16/24 Bit mono, full digital MPX bandwidth 88 kHz Fs = 128 kHz, 2048 /3072 kbps, 16/24 Bit mono, digital MPX bandwidth 64 kHz
apt-X® Enhanced	Sampling rates: 8/16/24/32/48 kHz Bit-Resolution: 16/24 Bit Bit-Rates: 64 - 576 kbps
MPEG 1 Layer II	Bit Rates: 64 - 384 kbps Fs 32/48 kHz Mono, Dual-Mono, Stereo, Joint-Stereo
MPEG 1 Layer III (decode only)	Bit Rates: 64 - 320 kbps Fs 32/48 kHz Mono, Dual Mono, Stereo, Joined Stereo
MPEG 2 Layer II	Bit Rates: 64 & 128 kbps Mono, Dual-Mono, Stereo, Joint-Stereo
MPEG 2 HE-AAC	Bit Rates: 16 - 128 kbps Mono, Stereo, Fs 16/22.05/24/32/44.1/48 kHz
MPEG 2 HE-AACv2	Bit Rates: 16 - 64 kbps Stereo, Fs 16/22.05/24/32/44.1/48 kHz
MPEG 2/4 AAC: AAC-LC AAC-LD AAC-ELD HE-AAC (compatible with VLC player) HE-AACv2 (compatible with VLC player)	Advanced Audio Coding AAC (low complexity): 8 - 384 kbps Mono, Stereo, Fs 8/11.05/12/16/22.05/24/32/44.1/48 kHz AAC (low delay): 24 - 256 kbps Mono/Stereo, Fs 22.05/24/32/44.1/48 kHz AAC (enhanced low delay): 64 - 256 kbps Mono/Stereo, Fs 44.1/48 kHz HE-AAC (high efficiency): 8 - 128 kbps Mono/Stereo, Fs 16/22.05/24/32/44.1/48 kHz HE-AACv2 (HE + PS): 8 kbps - 64 kbps Stereo, Fs 16/22.05/24/32/44.1/48 kHz

Framed Algorithms – Packet Sizes		
MPEG2/4 AAC LC	min. 21.3 ms	variable
MPEG2/4 AAC LD	min. 10.6 ms	variable
MPEG2/4 AAC ELD	min. 21.3 ms	variable
MPEG2/4 HE AAC	min. 42.6 ms	variable
MPEG1 Layer II	min. 24 ms	variable
MPEG2 Layer II	min. 48 ms	variable

IP – Interface and Protocols	
IP Interface Physical	Dual IP ports, 2x RJ45 for streaming and/or management
IP Interface electrically	Separate PHY per interface 2x MAC addresses 2x network address settings Port speeds: Full Auto, 10/100BaseT/Tx restricted auto or hard coded, Auto MDI-X
Virtual IP Interfaces	VIF on both physical ports assigns multiple IP addresses to a physical port (ETH0 / ETH1).
VLAN Tagging IEEE 802.1q	Both ports provide VLAN-tagging. As a VLAN-tag-aware end device, it can add and remove VLAN tags to the interfaces (VIDs).
Ethernet	IEEE 802.3x
IP Protocol	IPv4
DHCP	on all physical ports
Bridged Modem Support	Supports 3G/4G modems running in Bridged Mode
ICMP	PING responds on both ports
IGMP	Version v2 and v3 (with SSM support)
TCP/IP	for WEB GUI control
UDP	for audio/aux streaming
RTP/RCTP	for audio
FTP	for firmware update via NMS
HTTP/HTTPS	for web application and firmware update via WEB GUI, HTTPS is the standard protocol
SMTP	E-Mail notifications
SNMP	SNMPv2c, trap v1, v2, and v2c – SET, GET, Inform, TRAP - trap send behavior configurable per individual trap (enable, disable, send and forget, send until acknowledged, etc.) SNMP agent supports two sets of community strings
NTP	NTP client integrated
mDNS	DNS look up and hostname streaming
Dynamic DNS	Client supports dynamic DNS services on ETH0 and ETH1
NAT traversal Mode	UPnP (IGD protocol) is used for NAT traversal mode. It allows configuring a UPnP-enabled NAT router (typical: xDSL services)
Management	WEB GUI, APT NMS, SNMP, API support
User Management	2-Level user management on WEB GUI access (Admin/Guest)
Configuration Backup	Backup storage of full unit configuration with or without IP interface configurations (System-Backup on SD card or Configuration-Backup on off-line storage). Auto-Restore at boot time (supports cloning of a unit)

IP – Audio Streaming – IP Forwarding	
Casting Modes	Unicast, multiple unicast multicast, multi-multicast, source-specific multicast (SSM)
Stream Types	Audio (RTP): Rx, Tx, duplex AUX (UDP): Rx, Tx GPIO (UDP): Rx, Tx IP Forwarding Transmit and Receive: UDP (for any data) Media Forwarding Transmit and Receive: RTP (media) UDP payload re-encapsulation into RTP/UDP (any data)
Non-Audio Streaming	Forwarding of any data, like EDI for DAB transmitter along audio streams with or without SureStream protection
Clock	2 clock domains selectable (Tx/Rx)
Content Time Alignment	NTP provides metronome clocking for Encoder and Decoder De-jitter buffer uses as adjustable delay line for content alignment
De-Jitter Buffer Size	from 1 ms to 5000 ms
Streaming	Tx: 1x Stereo audio, n IP-streams Rx: 1x Stereo audio
Asymmetrical audio	Encoder/Decoder on separate audio modes/clocks/networks
Auto-Detection, Auto-Configuration	Auto-detection of the incoming stream on receive-streams. Auto-Configuration of decoder settings
QoS, RFC 2474 SURESTREAM	DiffServ with distinct DSCP values per stream; Differentiated Services Code Point for packet classification purposes SureStream Technology, based on redundant packet streaming (Statistical Stream Diversity) – license option
Network Security	
Firewall Features	Service filter on each ETH interface (enable/disable): - FTP (port 21) - HTTP (port 80) - HTTPS (port 443) - SNMP (port 161) - SNMP Traps (port 162) - SSH (port 22)
Secure HTTP	WEB GUI access via HTTPS as standard
DATA	
AUX Data	RS232
Aux data Mode	Embedded & Non-embedded
Data Rates	embedded & non-embedded:1200/2400/4800/9600 non-emb.: 14400/19200/28800/38400/57600/115200Baud
GPI, Switch Inputs	Non-embedded: 4x opto-isolated switch inputs embedded: on Eapt-X only IP Decoder: none
GPO, Relay contacts	4x relay contacts carried out as 3-pin switches

End of Document