WORLDCAST SYSTEMS

POWERFUL PERFORMANCE CONTROL SAVINGS SERVICES

User Manual

AoIP Codec Module & analog composite/MPX version

System Release 4.0.4 | Document Version 3.1 | release/update: November 2022

Our brands : apt > ecreso > audemat

WorldCast Systems S.A.S (previously Audemat S.A.S)
20 avenue Neil Armstrong - 33700 Mérignac (Bordeaux Métropole) - France
Tel +33 (0)5 57 928 928 – Fax +33 (0)5 57 928 929 - contact@worldcastsystems.com - www.worldcastsystems.com
Capital: 2 269 800 € - Siret 428 787 550 00014 - TVA FR72 428 787 550 – APE : 2630Z

afaq ISO 9001 Qualité AFNOR CERTIFICATION

DECLARATION OF CONFORMANCE

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

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

Disposing Information

According to local laws and regulations, this product should not be disposed of as 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 AoIP Codec Module and analog MPX interface card

System Release 4.0.4 - November 2022

Warranty

All information is believed to be accurate and correct at the 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 regard 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 this material's furnishing, performance, or use.

Trademarks

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

How to contact us:

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

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

How to get support

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

http://www.worldcastsystems.com or

apt-cust-support@worldcastsystems.com

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 hazards or risk of fire, the following must be observed:

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

Queste apparecchiature sono state costruite 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.

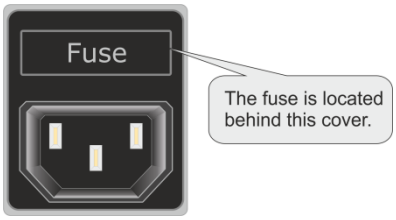
Het apparaat mag niet gebruikt worden in een vochtige omgeving, en dient ook niet gebruikt te worden als onderzetter voor drinkbekers of andere voorwerpen die vloeibare stoffen bevatten.

Power and Low Voltage Ports

Main Fuse Characteristics

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

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



⚠ Any fuse replacement must conform 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. Observing 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 unit's location.
- **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. 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 AoIP Codec Manual

Thank you for purchasing the Audio over IP Codec Module from WorldCast Systems. We have developed this unit to be as user-friendly as possible, and it contains many advanced features designed to make this product's use straightforward.

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

It is recommended that new users of the Audio over IP Codec Module should read the complete 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.

This manual is supplied with each AoIP card delivery.

1.1 Release Information

This Manual describes how to operate the Audio over IP Codec Module suitable for the Modular Codec Chassis 1U and is the primary reference covering the configuration, installation, operation, and troubleshooting. You can find the description of the 1u chassis in the hardware manual.

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

1.1.1 Standard Applications for SR 4.0.4:

- **ScriptEasy version 2.9.17.001**
- **MasterView 2.1.0 web application**
- **APT NMS 1212 or higher**

1.2 Critical Network Security Advice

1.2.1 This AoIP Audio Codec is a network device!

As a network appliance, the AoIP Codec can create security vulnerability between your internal LAN and the WAN domain. The AoIP Module provides built-in firewall and policy routing capabilities, but you should ensure 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 firmly 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. Do not use the trivial default names (refer to section 3.5.10.1)*

1.3 Introduction AoIP Codec Module

The AoIP Codec Module is a four-channel standalone Codec Module able to deliver four independent audio IP streams or multiple of these (multiple unicast). It is a full duplex, multi-algorithm audio codec offering conventional analog left and right audio interfaces and AES/EBU digital audio connections operating through IP. It separates the sending and receiving audio data paths by running in asymmetric audio mode. This allows an anywhere-to-anywhere routing without any clocking conflicts.

This codec generation incorporates the enhanced versions of the aptX® algorithm, Linear PCM 16 and 24-bit, MPEG 1/2 Layer II, the full MPEG 2/4 AAC suite of algorithms, including MPEG 2/4 HE-AAC as well as OPUS. In addition, MP3 for decoding (MPEG 1/2 L III) and an Auto Detect mode has been added to the Decoder path.

The AoIP codec optionally allows the transmission of a digital composite/MPX signal fed into the AES interface. This option has been extended to include the new APTmpX format, which transmits compressed composite/MPX at a bit rate of less than 1 Mbps.

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

The AoIP Codec Module runs an embedded WEB GUI, which can be accessed from a web browser or the NMS. A headphone socket provides for additional monitoring of the audio input or output. The rear panel audio I/Os can be switched to accept analog or digital signals. The digital output can be synchronized with an external digital reference signal if required. Additional interfaces allow for the connection of auxiliary data 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 check the equipment status and perform user actions remotely with a web browser.

Script Easy and MasterView are implemented as standards.

1.3.1 System Options

SureStream License

Reliable and lossless connectivity over lossy IP networks and the Internet, utilizing redundant streaming.

Digital Composite/MPX over IP License

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 or with the compressed APTmpX format. Three MPX modes are available, full linear MPX or MPX for audio and RDS only (MPX bandwidth 64kHz) and APTmpX for low bitrate Composite/MPX transmissions (< 900kbps)

Analog MPX Input/Output Card:

This interface module provides BNC connectors and supports the connection of **analog** MPX signals. This interface can run in simplex modes (dual Encoder or dual Decoder) or bi-directional Codec mode (Input/output).

1.4 Unpacking and Inspection

After unpacking:

Check the delivered hardware for damage during shipping. Then, immediately report any damage to your local sales office or WorldCast Systems HQ.

Check that the list of contents is complete as follows:

AoIP Codec Modules

Please check that the correct number and type of hardware were delivered.

XLR Audio Breakout Cable

The AoIP Codec Module terminates all audio signals on a 37-way D-Type connector. In addition, an XLR breakout cable is supplied with each standard audio input/output module.

AoIP Cards

Confirm that the correct types of codec cards, including all licenses, are supplied per the original order instruction. If an AoIP card 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	HTTPS (port 443)	Static
ETH1	192.168.101.111	HTTPS (port 443)	Static

Please ensure that only one card is connected to your network simultaneously with this default IP address!

If the equipment supplied does not match the requested items, please immediately contact WorldCast Systems or your local distributor and report any shortages. Please do not connect the system to the network or apply power to the unit if you doubt the contents, as this could cause damage to the hardware.

More information about connection and installation is provided in section 1.5 of this document.

1.5 AoIP Codec Module – Frame Installation

The AoIP Codec Module is a stand-alone IP Codec designed for the WorldNet Oslo 3U Frame (legacy) and the modular 1U Chassis with its management and IP transport facility. It doesn't need a System Controller (MCU) or a primary IP Transport card for administration and IP streaming (legacy).

The 1U Chassis can be populated with up to four AoIP modules, and the 3U Frame offers an extended capacity to host up to eight AoIP modules.

1.5.1 WorldNet Oslo 3U Frame – Card slots

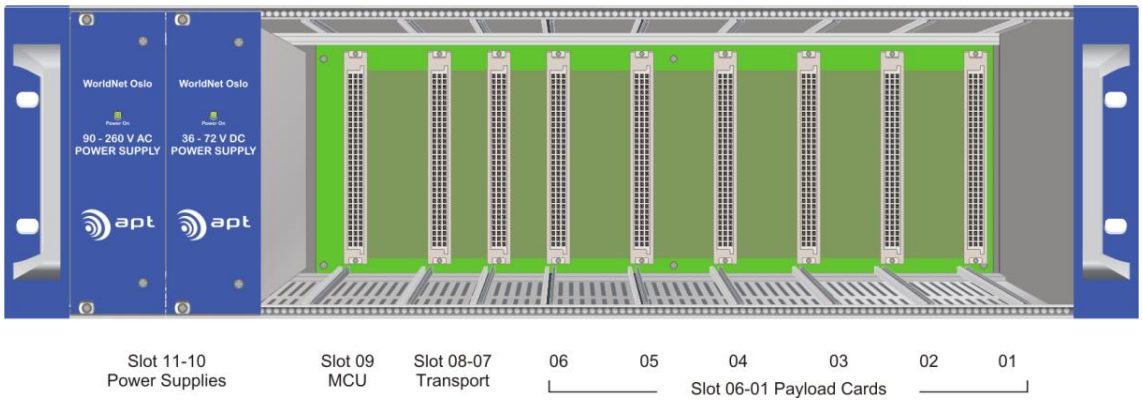


Figure 1-1: Oslo 3U Frame card slot assignment – front panel view

Card Slots	Type of Cards
#01-06	These slots are reserved for payload cards like AoIP Codec Module, audio, auxiliary data cards and all future payload cards from the contribution category.
#07	This slot is reserved for a second network transport card or another (7th) AoIP Codec Module (6HP size)
#08	This slot is reserved for a network transport card or another (8th) AoIP Codec Module (6HP size)
#09	This slot is for the System Controller (MCU) only (legacy)!
#10 #11	These slots are reserved for the primary and optional redundant Power Supply.

The 3U frame card slot seven (#7) and eight (#8) can be populated with two more AoIP Codec Modules.

ⓘ *Note: AoIP cards for slots #7 and #8 on the 3U Frame must be ordered as 6HP-sized modules!*

ⓘ *The AoIP Codec Module does not require a System Controller card (MCU)*

1.5.2 APT Codec Frame 1U – Card slots

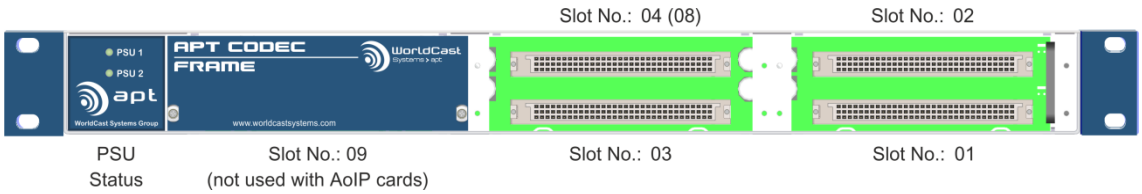


Figure 1-2: 1U chassis card slot assignments – front panel view

Card Slots	Type of Cards
#01-04	These slots are used for AoIP cards (with standard or analog MPX interface)
#(08)	This logical slot is for an (legacy) E1/T1 transport card (physically on pos. 04)
#09	This slot is reserved for the (legacy) System Controller (MCU) required for the E1/T1 version but is not used with AoIP Codec Modules.

ⓘ *The AoIP Codec Module does not require a System Controller card (MCU)*

The Codec Chassis supports the standard and the analog MPX rear module sitting side by side in the same frame.

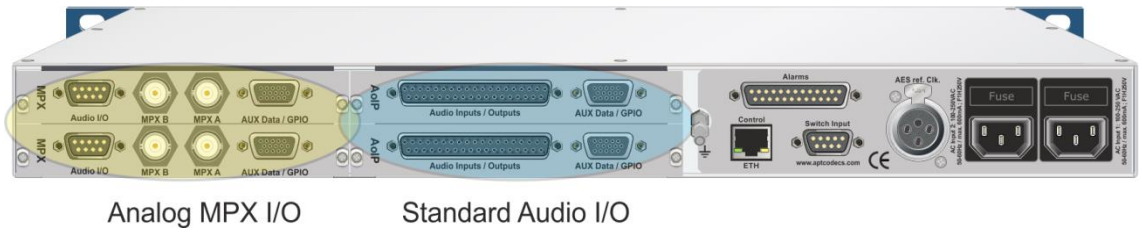


Figure 1-3: Shows a combination of both rear module types in the same 1U chassis

Notes:

1.5.3 Codec Module

The main board of the AoIP card inserted into the front of the chassis has a corresponding interface card that mates with it and is inserted into the rear of the frame. Each AoIP Codec Module connects to its corresponding Input/Output module sitting on the same card slot number on the frame's rear. The main board and the rear panel card represent a standalone AoIP Codec.

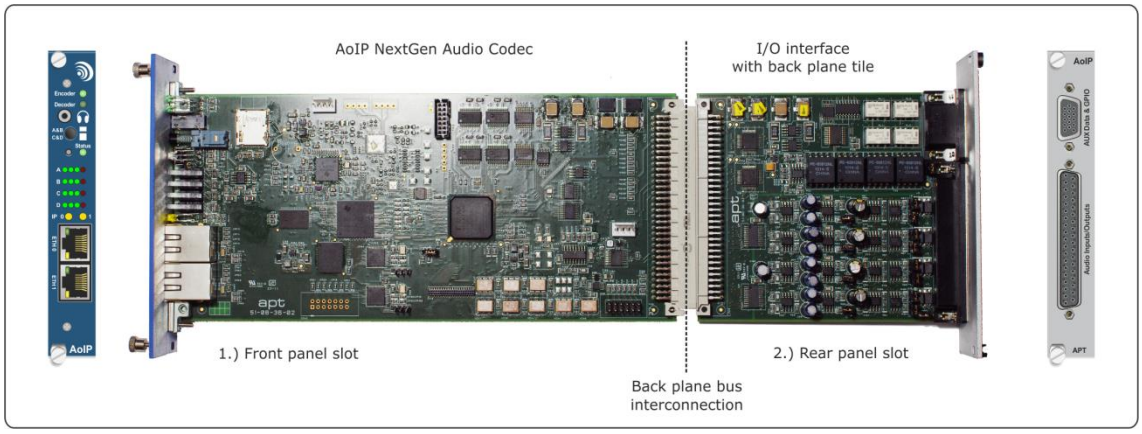


Figure 1-4: AoIP set of modules: 1) Mainboard 2) AoIP I/O interface (4HP version shown)

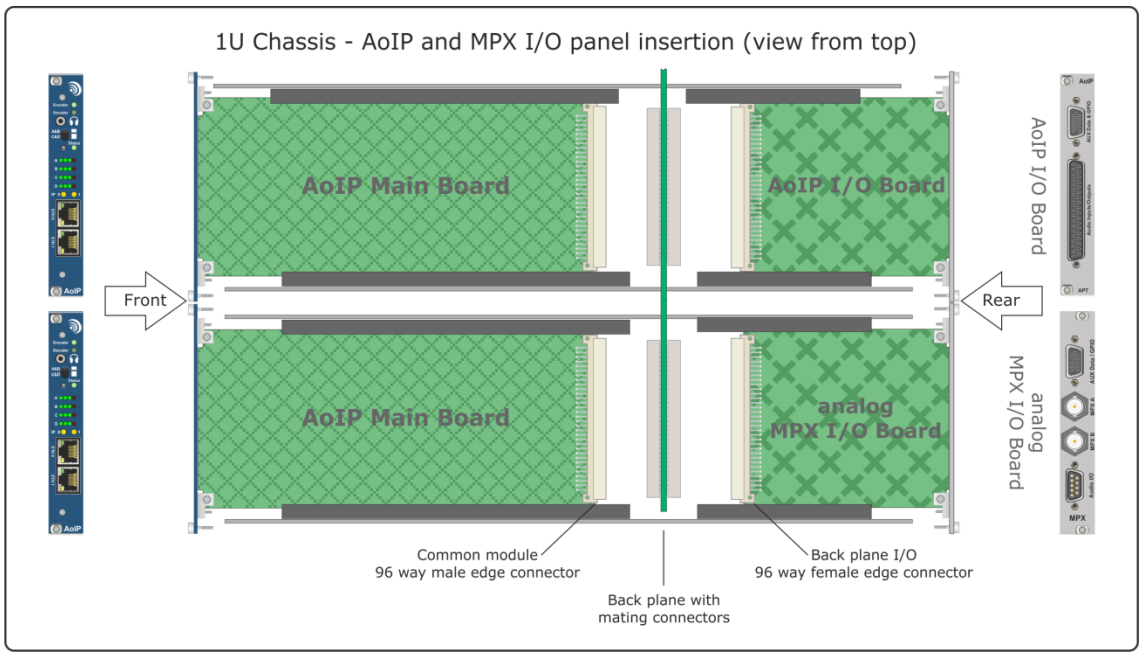
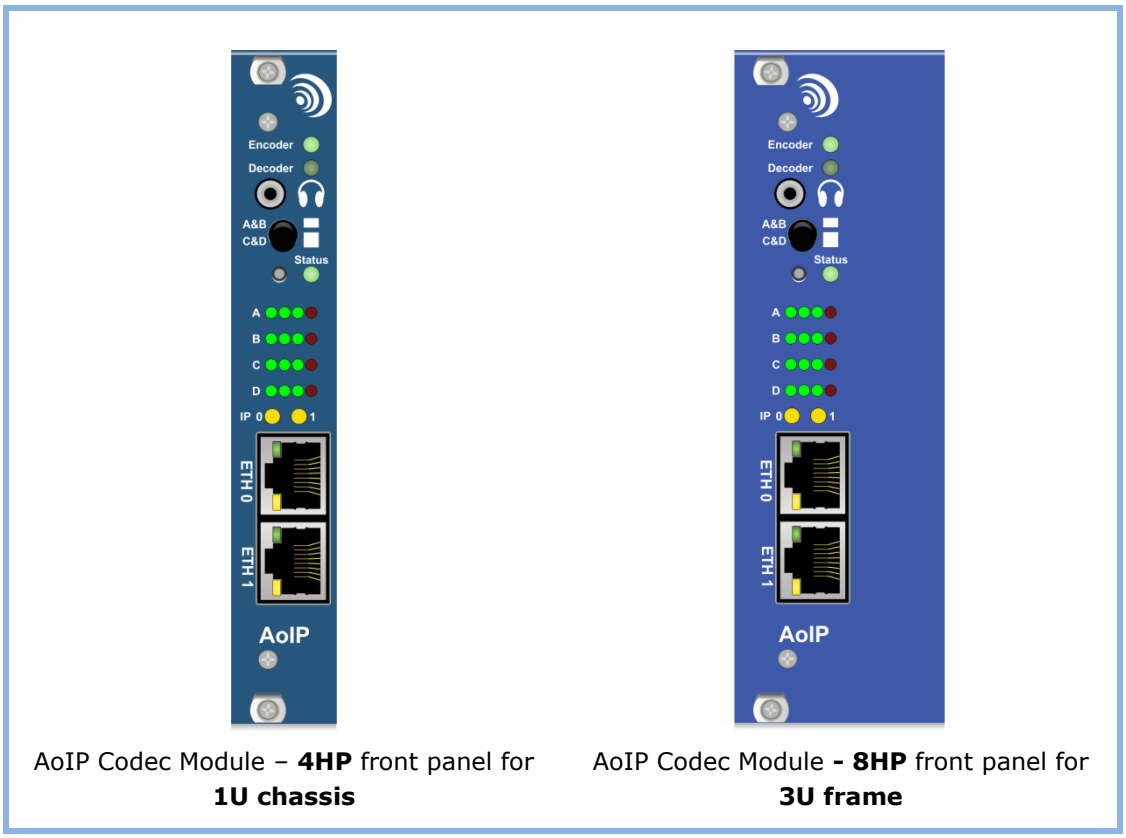


Figure 1-5 The top view of a 1U shelf illustrates the insertion of modules and the corresponding backplane interfaces (standard audio and MPX card).

1.6 The Audio-Over-IP-Module – AoIP

1.6.1 Physical Designs

Physically this AoIP module is available with different front panel sizes. The 8HP size (wide) is the standard sized module for the 3U Frame. The 6HP version is for the 3U frame also, but for sitting in the transport slots (slot 7/8). The 4HP (thin) version is designed for the 1U Codec Frame.



AoIP Codec Module – **4HP** front panel for **1U chassis**

AoIP Codec Module **- 8HP** front panel for **3U frame**

Figure 1-6: Shows the variant of possible module form factors (4HP and 8HP)

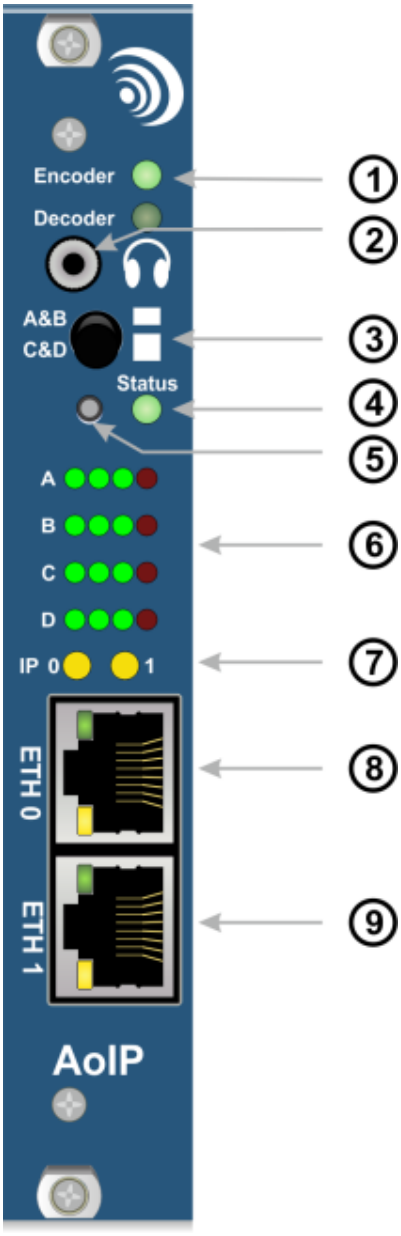
The AoIP module is a four-channel standalone Codec module able to deliver independent audio IP streams or multiple of these (multiple unicast). This allows sending and receiving audio on different formats and bit rates, e.g., sending with high quality and receiving with voice graded quality.

Independent clock domains for transmitting and receiving audio allow an anywhere-to-anywhere streaming method on the network on a per program basis. Furthermore, there are no restrictions caused by clock bonding between the audio programs (currently dual stereo). On the network receiving end, a de-jitter buffer, clocked by a dedicated VCXO or the system time for each stream, allows independent stream management.

An AoIP Codec Module provides two physical ETH interfaces allowing for streaming into different networks or separating the audio streams from the management network completely. In addition, both physical network ports support virtual interfaces and VLAN tagging.

AoIP Codec Module provides two AUX data interfaces (asynchronous RS232) and four GPIO inputs with corresponding relay contact closures.

1.6.2 Front Panel Components



AoIP Card front panel components

01 Indicates the operational mode configured by software:

Encoder: Encoder Mode – Transmit only
Decoder: Decoder Mode – Receive only
Both: Duplex Codec Transmit & Receive

02 3.5 mm Monitor Output:

Drives a headphone with fixed volume or can be used for active monitors

03 Monitor Source Selector

Select a pair of signals, either A&B or C&D. Signal source can be either Input/Output A/B or C/D or Input A/B Output C/D, depending on the selected operation mode

04 Module Status Indicator – Tri-Color

- Applying Power — static orange
- Rebooting from GUI — static Orange
- On firmware update — flashing Orange
- Any failure on Card — static Red
- I/O interface missing — static Red
- Normal operation — static Green

05 IP Address Reset Button (recessed)

Pressing this button for more than 5sec. sets the AoIP card to default IP addresses (status LED: orange)

06 Signal Level Light Pipes

Indicate the presence of audio signals for channel A/B/C/D (Red = 0 dBFS)

07 RTP Traffic Indication – Streaming LEDs

Other than the LEDs on the network interface (ETH), these LEDs indicate only RTP traffic from and to the AoIP card.

08 Network Interfaces:

09 Two network interfaces are provided: ETH0 and ETH1. Both operate independently and must be configured for different sub-networks. Both are configurable for audio streaming and WEB browser access.

Table 1-1: AoIP Card front panel components

1.7 Default IP Addresses

1.7.1 Default Network Settings

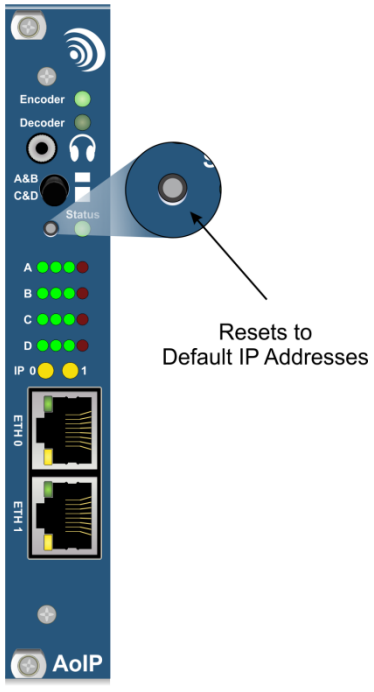
The AoIP card provides two IP interfaces: ETH0 and ETH1. You can use both interfaces for control/management, LAN connection, and WAN connections. Both Ethernet interfaces are open by default to connecting to your Web browser. The GUI allows you to manage the services available on each interface at any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

ⓘ *. HTTPS port 443 is the standard protocol used for the Web browser access*

Ethernet Port	Default IP Address	Port	DHCP / Static
ETH0	192.168.100.110	HTTPS (port 443)	Static
ETH1	192.168.101.111	HTTPS (port 443)	Static

1.7.2 Hardware Reset to Default IP Addresses

In a situation where the default IP address has been changed and not noticed, the AoIP card can be reset to its default addresses without affecting other configurations.



On the AoIP module's front panel, there is a small hole where behind this hole sits the IP Addresses Reset Switch. To change both IP Addresses of the AoIP Codec Module to the default addresses, insert a small tool and press the switch. Hold it until the Status LED starts to flash (about 5 seconds) – then remove it.

The unit has changed both IP addresses; it does not need to reboot. It takes a short while (~10sec) until the Web GUI is accessible again on the default addresses.

It is recommended to delete the browser cache before re-connect to the GUI.

ⓘ *Note: All cards have the same default IP addresses! You must connect one card after another to the network to change the IP addresses to avoid address conflicts.*

1.8 IT Security Recommendations

1.8.1 IP Codecs – Network Connection

As a network appliance, the AoIP Codec can create security vulnerability between your internal LAN and the WAN domain. The AoIP module provides built-in firewall and policy routing capabilities, but you should ensure 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. Care must be taken that the management ports are inaccessible on the streaming network (the external network).

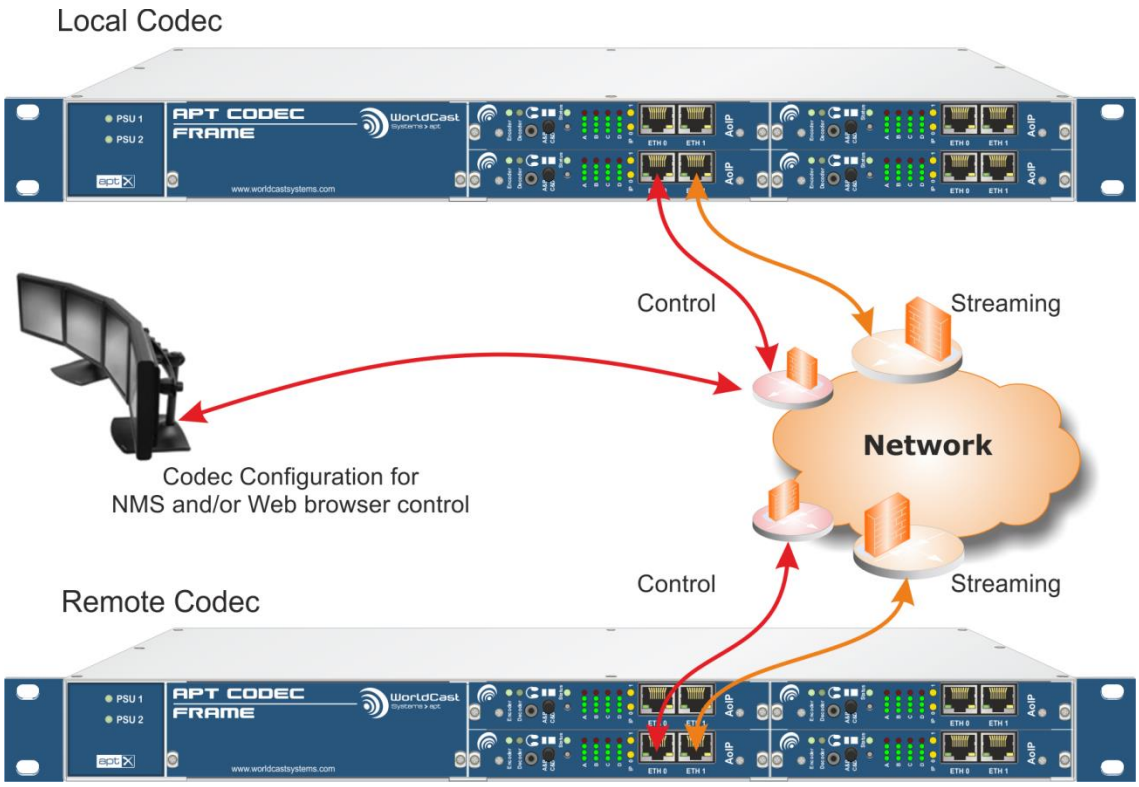


Figure: 1-7: Shows the recommended network installation: Audio Codec connected to a switch with firewall mechanism.

In the example above, ETH 1 is used for management and ETH 0 for audio streaming. A user decides 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 codec suits your security policy; refer to section 3.5.7.9 (internal firewall configuration).

1.9 Connecting via Web Browser

The codec is controlled and managed using a standard web browser. **By default**, the web browser access for management is possible on both Ethernet ports; some service filters (firewall) are enabled with the factory default configuration.

Ethernet Port	Default IP Address	Port	DHCP / Static
ETH0	192.168.100.110	HTTPS (port 443)	Static
ETH1	192.168.101.111	HTTPS (port 443)	Static

1.9.1 AoIP Module Firewall – internally managed Ports

The following table shows the TCP/UDP ports that should be considered while planning your security. The internal firewall individually allows port management on both ETH interfaces (section 3.5.7.9).

Port	Service	Protection
TCP 21	FTP	Internally protected
TCP 80	HTTP, WEB Services	Internal firewall
TCP 443	HTTPS, Web Services	Internal firewall
UDP 5060	SIP	Internal firewall
UDP 161	SNMP	Internal firewall
UDP 162	SNMP TRAP	Internal firewall
UDP 7777	APT NMS communication	External protection required
UDP 7778	APT NMS communication	External protection required

1.9.1.1 Firewall Default Settings

Port	Service	Internal Firewall
TCP 21	FTP	closed
TCP 80	HTTP, WEB Services	closed
TCP 443	HTTPS, Web Services	OPEN
UDP 5060	SIP	OPEN
UDP 161	SNMP	OPEN
UDP 162	SNMP TRAP	closed

1.9.1.2 Firewall Usage

You can open the ports that are closed by default. Please keep in mind that you are potentially creating security vulnerabilities that you need to address.

⚠ Each time the device is rebooted, the firewall settings are reset to the default settings.

1.9.2 Accounts LogIn and Services

GUI Passwords

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

⚠ Before commissioning the unit, we strongly 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. The default names of community strings, particularly the Private Community, are widely used and therefore commonly known. Because SNMPv2c does not support password the strings' password protection, the recommendation is clearly to create more "cryptic" community strings. Refer to section 3.5.10.1 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 3.5.10.1).

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

Please refer to the 1u chassis' hardware manual.

3.0 WorldCast Web-Browser GUI

The WorldCast Web GUI is the control and monitoring tool that communicates with the AoIP codec module. It is used to configure the unit, create audio streams, and get status and alarm information.

This section outlines this application and describes all aspects of the AoIP codec module configuration options.

3.1 Web Browser

The device is controlled and managed using a standard web browser. The web browser access for management is possible on both Ethernet ports; service filters are enabled with the factory default configuration. Please check the firewall settings of the Codec (section 3.5.7.9).

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

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 Transport Layer connection (HTTPS, TLS 1.2 and higher) to the AoIP codec module requires installing the WorldCast Systems SSL Certificate. You can download the certificate from the unit (refer to section 3.5.15.1)

3.1.1 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 by pressing Ctrl+F5 on all WIN browsers).

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 Browser Cache – Error Messages

Equipment busy

Communication blockage by Anti-Virus or Browser: CRL+F5 solves the issue.

Software not Responding

The boot process is not yet complete. After a few seconds, reload the page in the browser with the F5 key.

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 are prompted with the LogIn screen.

ⓘ *When you first connect the codec, you have to prefix "https://" to the IP address.*

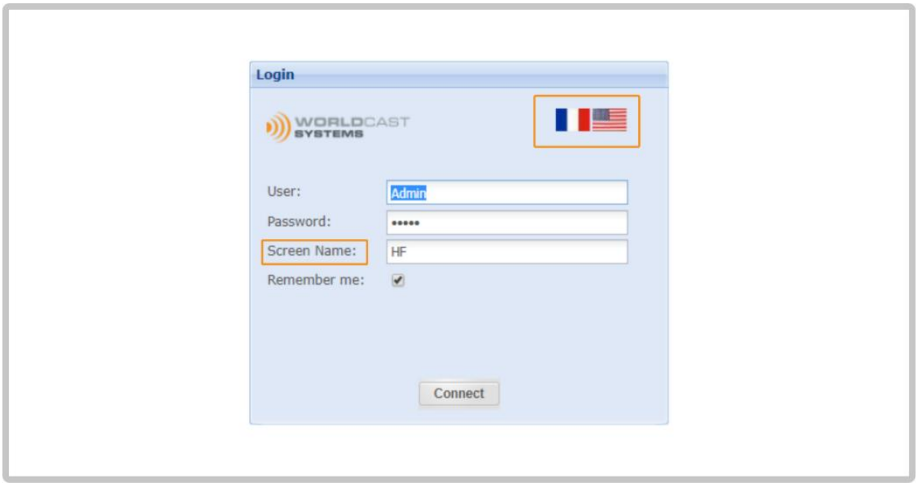


Figure 3-1 shows the WEB GUI LogIn screen

The multi-lingual GUI currently supports 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 is used to identify the participants. The chat box is described in section 3.5.15.1.

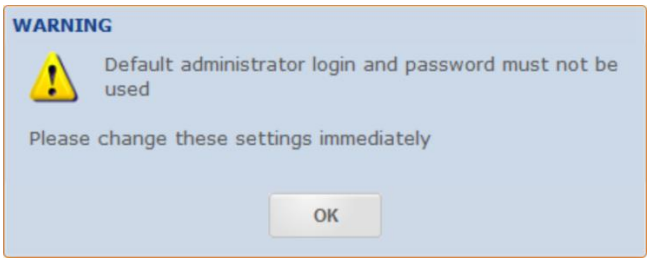
Activating the tick box "Remember me" allows the browser to remember your last LogIn for a new session.

3.2.1 Default LogIn

By default, the Administrator account is selected. However, the user management allows modifying this account and setting up a read-only account.

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

A security alert pops 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 the date correctly, the web browser starts loading the web application.

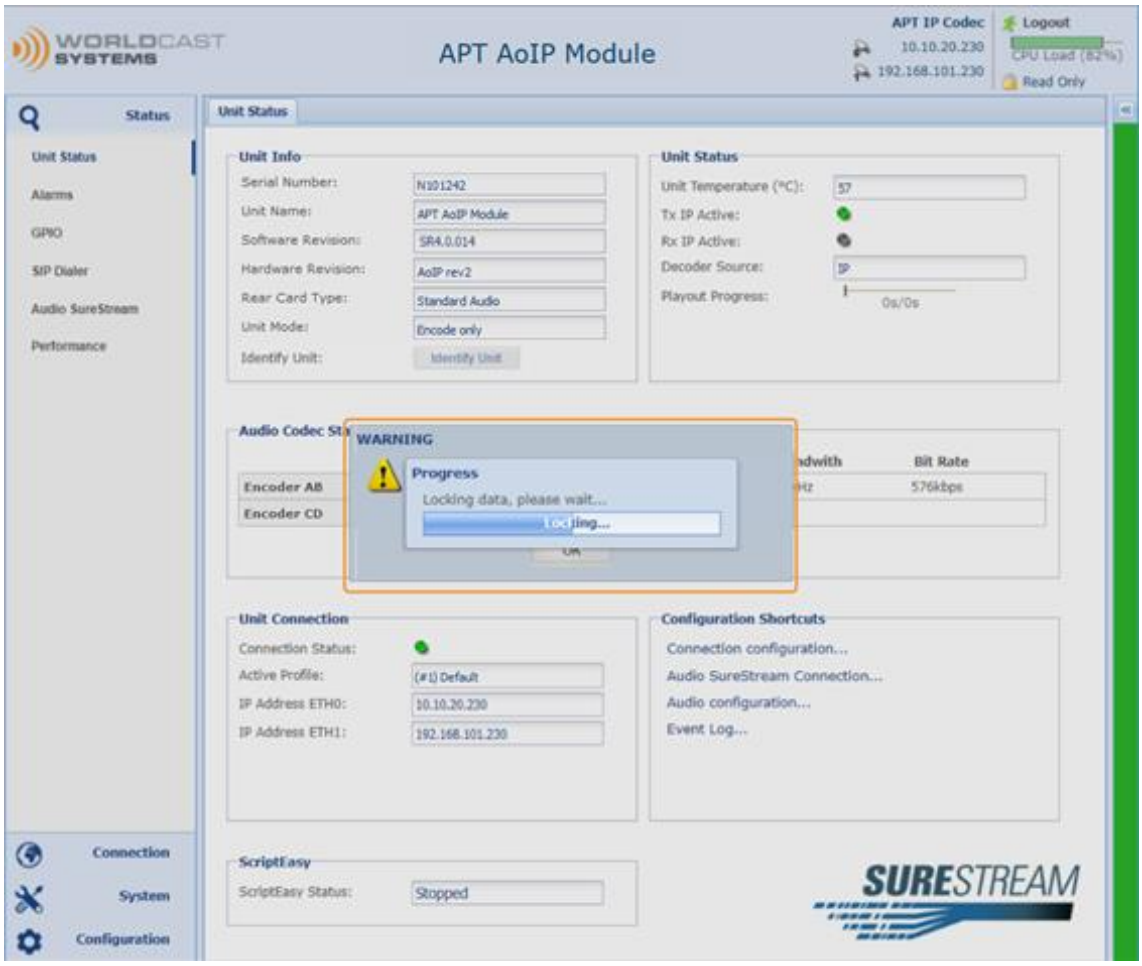


Figure 3-2 after loading the status page, the GUI tries to lock the current session for read/write access

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

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

3.2.3 Activated Applications and Options

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

The image below shows that the AoIP card has a ScriptEasy script loaded. If a script is loaded, it is activated during start-up. The alert window indicates this status and asks the user to acknowledge it.

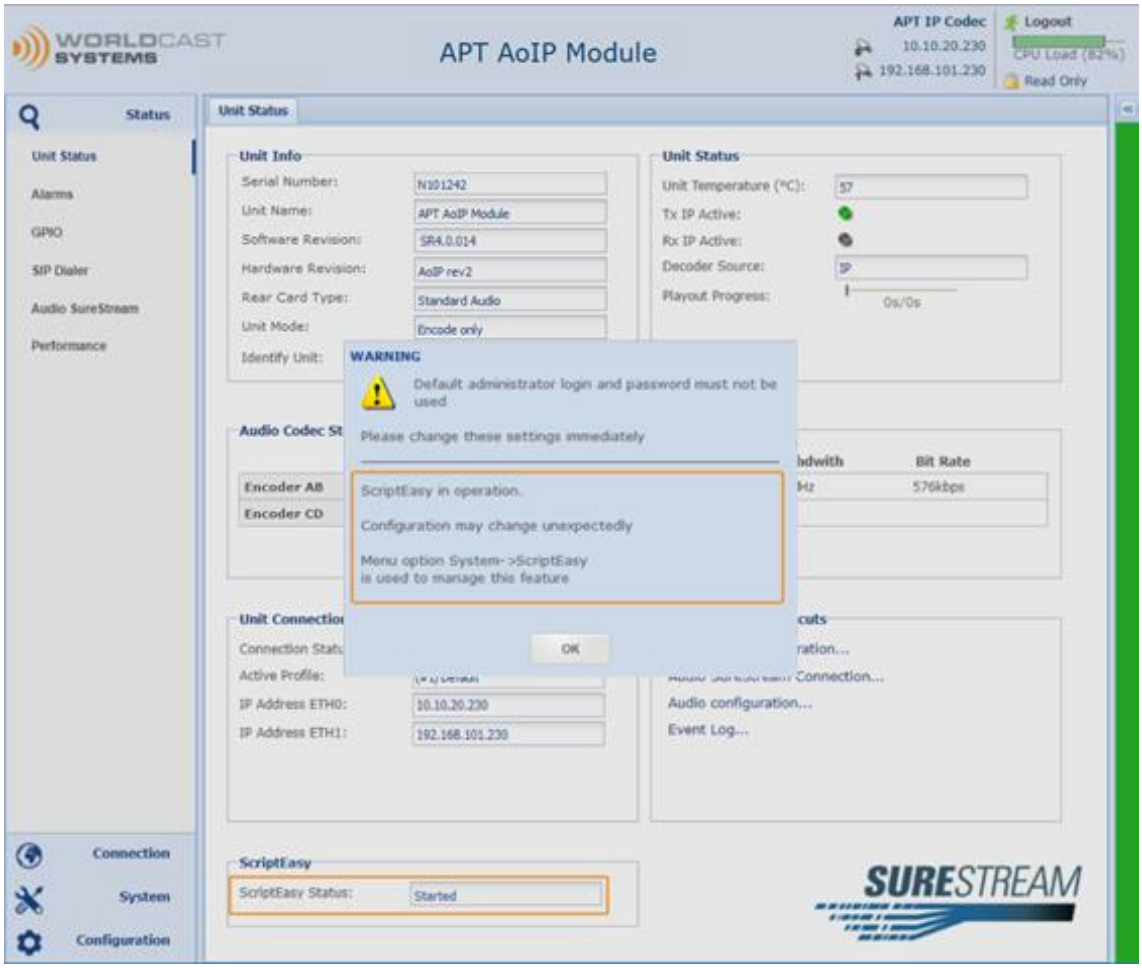


Figure 3-3 shows the warning window during start-up, listing various information and the SureStream license applied

ⓘ *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 3.5.10.3*

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 CPU utilization in real-time. The CPU load can vary significantly depending on the number of IP streams and the selected audio algorithm.

ⓘ *It is essential not to overload the CPU! A healthy threshold is 80 to 90%.*

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, Yellow, or Red depending on current alerts.

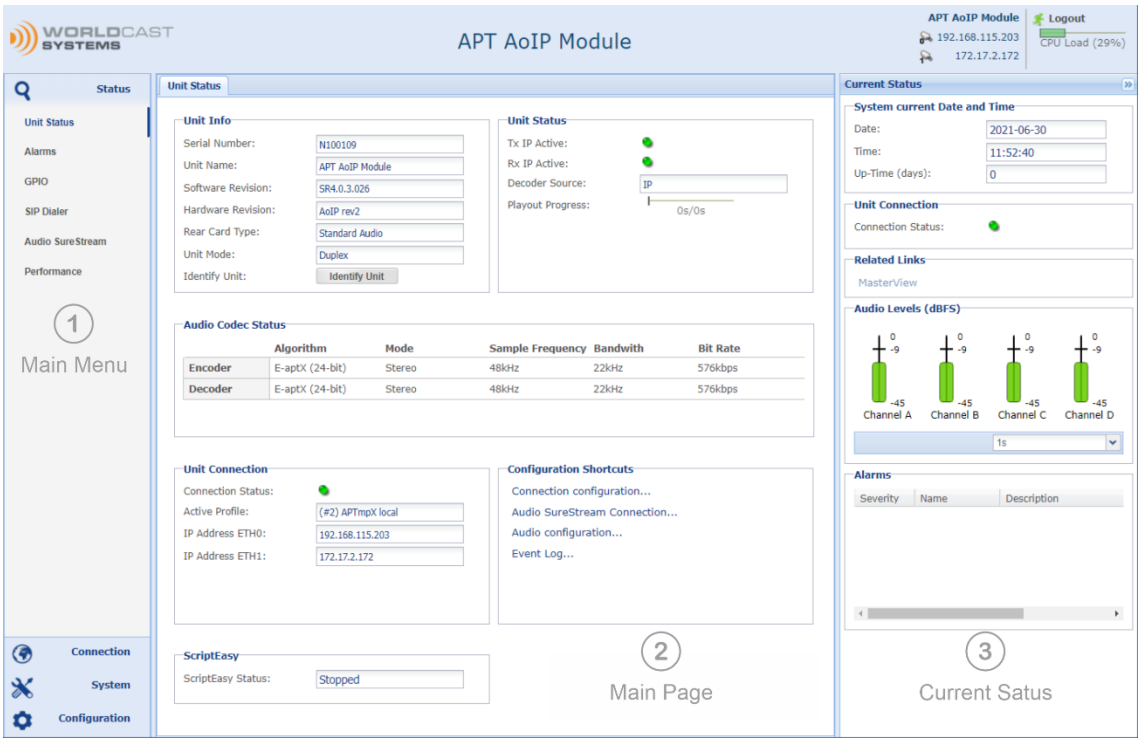


Figure 3-4 shows the Main Page with popped up "Current Status" frame

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 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 is the first Admin user connected for the session; subsequent logins are given "Read Only" status.

For a different user to obtain complete read-write control, the prior connectee must log out. The GUI automatically closes a session after ~30 minutes of inactivity, so access to a unit cannot be blocked accidentally.

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

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

3.2.6 Main Menu

The main menu is always present on the left-hand side of the browser window. Depending on the selected menu item, it expands and shows related submenu items.

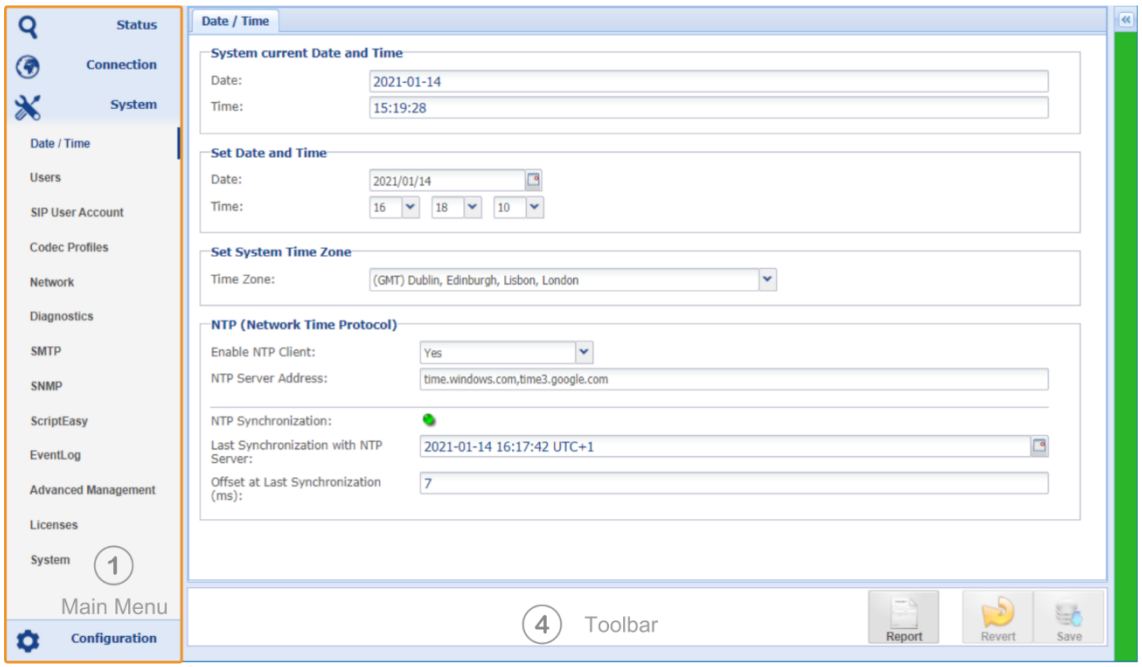


Figure 3-5 The Main Menu expands depending on the chosen menu item. The "Current Status" frame is hidden and indicated by the green bar on the right-hand side ("good" condition).

The screenshot above shows the Main Menu (1) and 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 color depending on the current conditions. Possible colors are GREEN (no error), YELLOW (minor error), RED (major error) and light BLUE (no active configuration).*

3.3 Main Menu – Unit Status

Starting the WEB application opens the Main Menu "Unit Status" with the Unit Status page and the corresponding sub-menu items loaded. Various sections structure the Unit Status page.

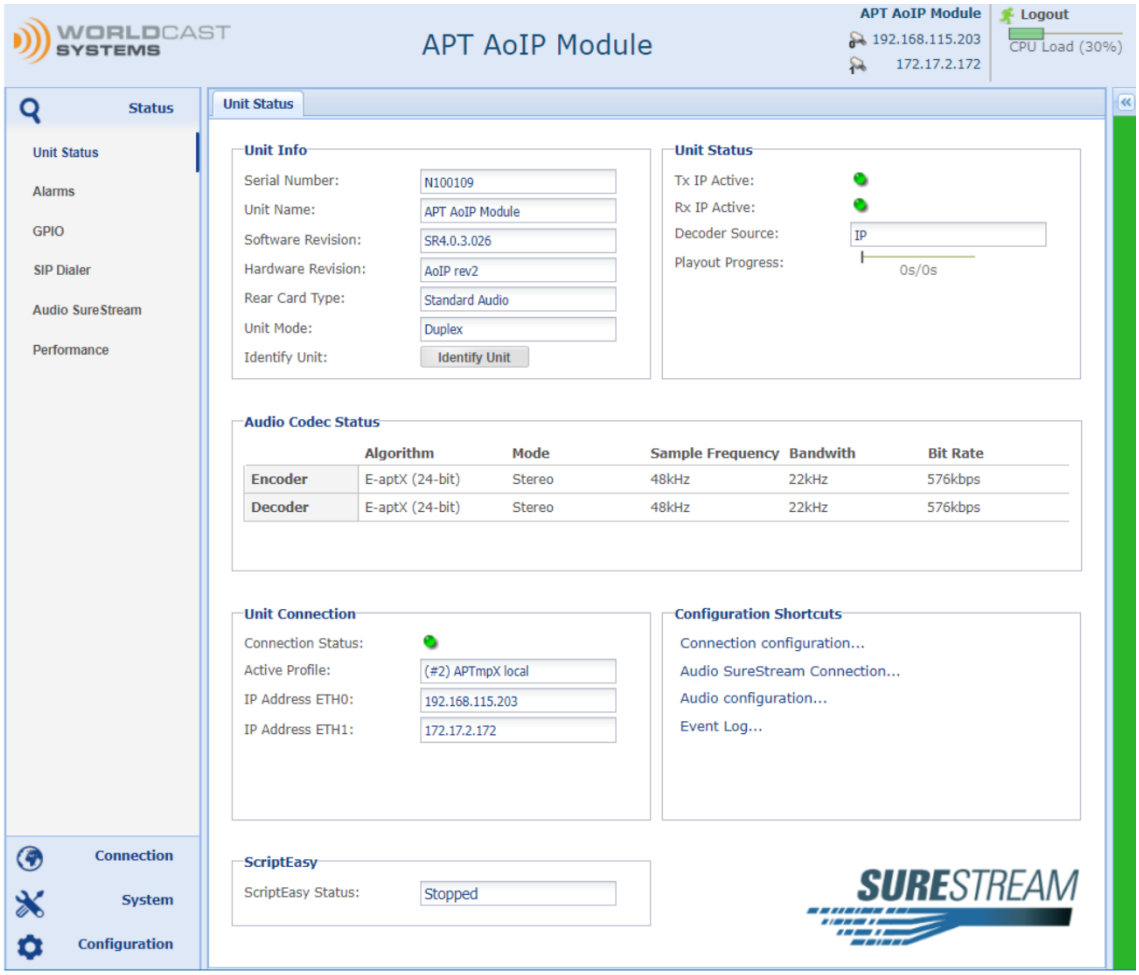


Figure 3-6 shows the Unit Status page

Main Frame

In the upper right corner of the main browser frame, you find the IP address of ETH0 and ETH1, the name assigned to the unit, the CPU utilization meter, and the logout button. This is also where the "Read Only" indication appears if another user has already logged in with read-write privileges.

Unit Info

This section displays the hardware and software release versions:

- Serial Number of the unit and unit Name (individual Name as applied)
- Software and Hardware Revision
- Rear Card type (currently "Standard Audio" or "Analog MPX" available)
- Unit Mode (Encoder/Decoder/Duplex)
- "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

- 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 triggers a change in this status indicator by utilizing RTCP (Real Time Control Protocol). RTCP alarms have a latency of about 10-15 seconds due to the RTCP timeout (Gray=no stream active, Green=no error detected, Red=Rx or Tx error detected)

- Decoder Source

The Decoder source can be data from the IP stream (normal mode) or "SD Card." SD Card means that the decoder decodes 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 AoIP Codec Module can be set up for asymmetric audio operation. This section provides information about the current 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). In addition, the stylized LED indicates any network-related error on any active IP interface if a stream is assigned to the interface.

Configuration Shortcuts

This section contains helpful links to other pages, currently to:

- Connection Configuration page (advanced stream configuration)
- Audio SureStream Connection (if SureStream license is applied)
- Audio Configuration Page (configuration menu)
- Event Logs

Optional 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

The "Current Status" frame allows a quick inspection of the current condition of a running configuration. The little arrows on top of the bar open it as a browser frame. In this mode, it is pinned on the right and re-sizable, and parameters can be changed (level bar refreshment cycles). Clicking on the colored bar opens this window as a popup overlay window.

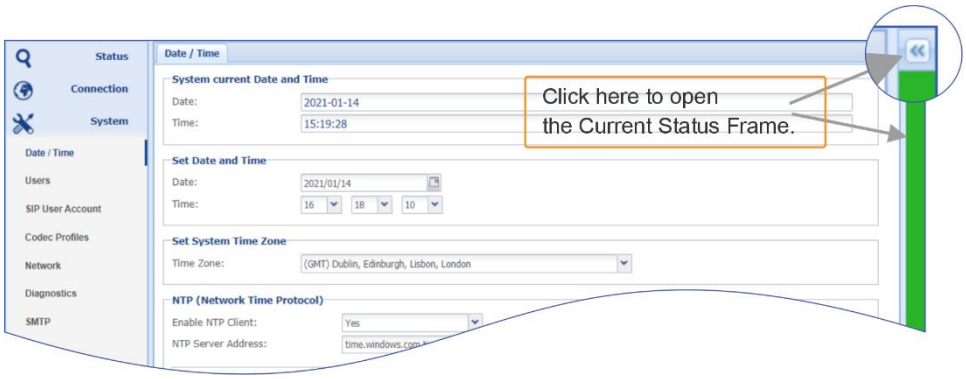


Figure 3-7 shows two methods to open the "Current Status" frame.

ⓘ *Note: The "Current Status" bar changes its color in dependence on the current conditions. Possible colors are GREEN (no error), YELLOW (minor error), RED (major error) and BLUE (no active configuration).*

System current 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)

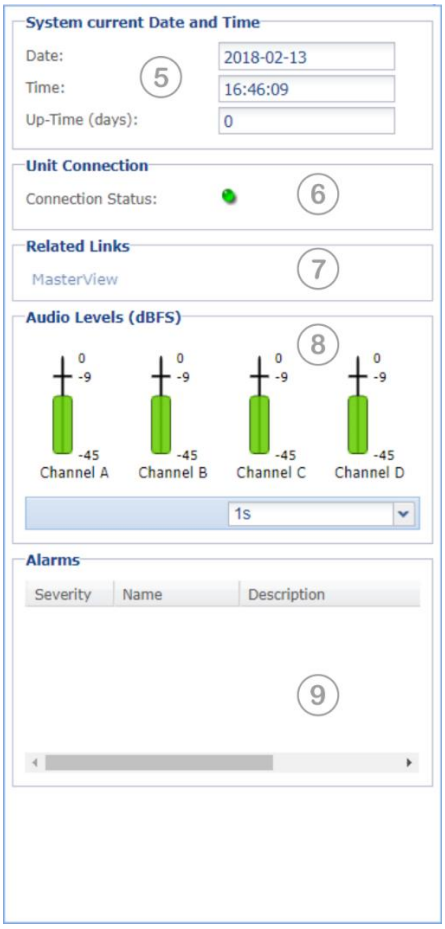
If a ScriptEasy application is loaded, this link to MasterView becomes active. It opens MasterView in a new browser tab.

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 the current system or connection alarms in real-time. In addition, it indicated the severity level 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 the monitored parameter has no alarm. **Gray** means this alarm is not enabled or not applicable. The failure of one of the PSUs is signaled as a warning. This warning is displayed as a yellow alarm on the right side bar (currently shown in green on the screenshot).

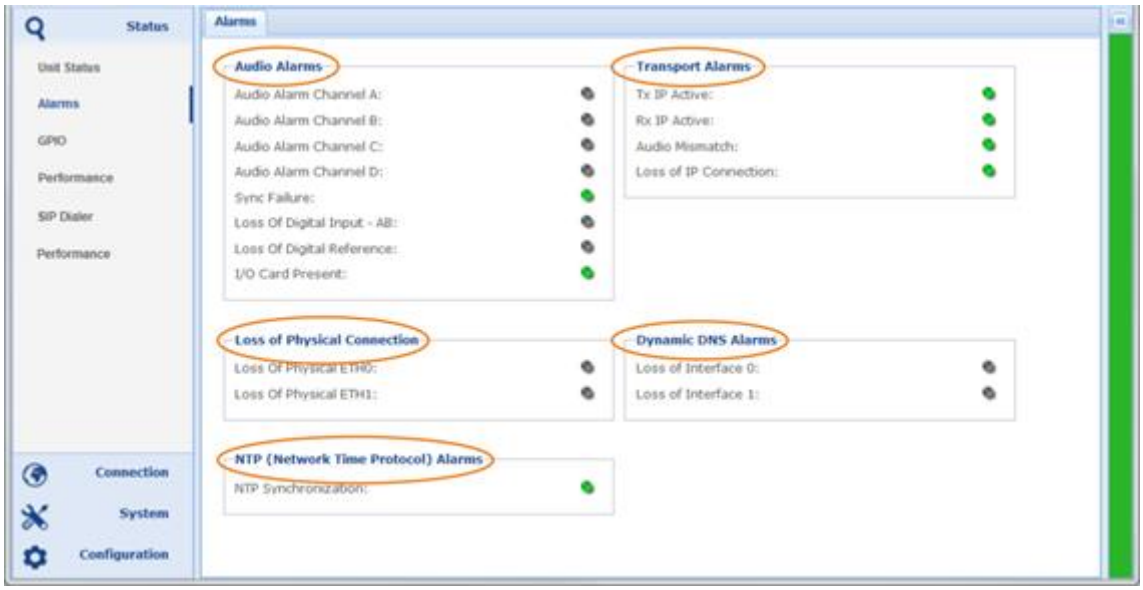


Figure 3-8 Main Menu Status – Alarms page

3.3.2.1 Audio Alarms

This section indicates the status of the audio alarms. The alarms listed here are Silence Detection for channels A/B/C/D, Sync Failure, Loss of Digital Input (A/B) and Loss of Digital Reference.

Audio Alarms (Silence Detection)

The Audio signal has decreased below the threshold and timeout specified in the audio configuration menu. This alarm is flagged if a network fault causes silence, 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 number 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 embedded in the aptX® audio stream that allows a very rapid resumption of decoding after a gap in the bit stream. This alarm is flagged if the following conditions occur (for network faults, usually along with other network alarms):

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

Alarms Status (*continued*)

Loss of Digital Input

This alarm indicates the loss of the AES input signals. In duplex mode, it shows only Input A/B; in Simplex Encoder mode, it shows A/B AND C/D.

Loss of Digital Reference

This alarm indicates the loss of the external AES clock.

I/O Card Present

This alarm indicates that the rear panel module (I/O Card) is not inserted or is not functional.

3.3.2.2 Transport Alarms

This section shows IP alarms only, such as IP Rx and Tx errors, 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 codec.

IP Receive (Rx) Error

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

Audio Mismatch

This alarm is raised if the algorithm and packet size does 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.

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.

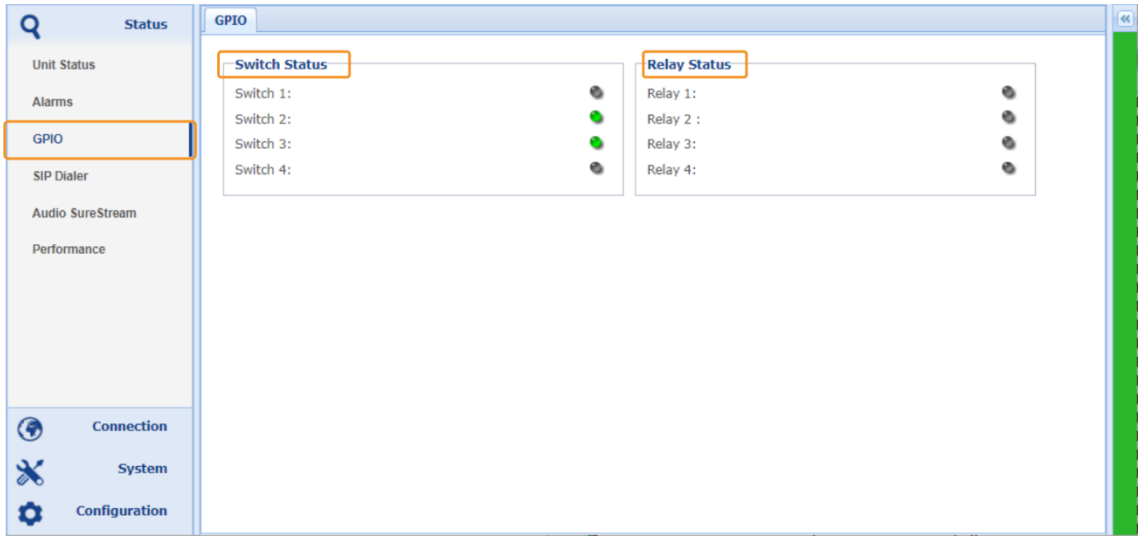


Figure 3-9 Main Menu Status – GPIO page

Switch Status

This section displays whether the switch input is active by showing a green LED on the particular switch. Gray means 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. Gray says the relay is inactive.

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

3.3.4 SIP Dialer (SIP – screens from SR 3.1)

At this point, only the components of the SIP Dialers Page are described. For general information about the SIP connection mode, please refer to Appendix 9.0

SIP is an alternative connection mode and, if selected, disables the RTP/UDP direct connection mode!

The SIP Dialer is the SIP directory of the SIP contacts and allows you to insert, edit, or delete SIP contacts and establish a call. Some configurations must be done in the System menu to use the SIP Dialer. These are described in chapters 3.5.4 and 3.5.5.

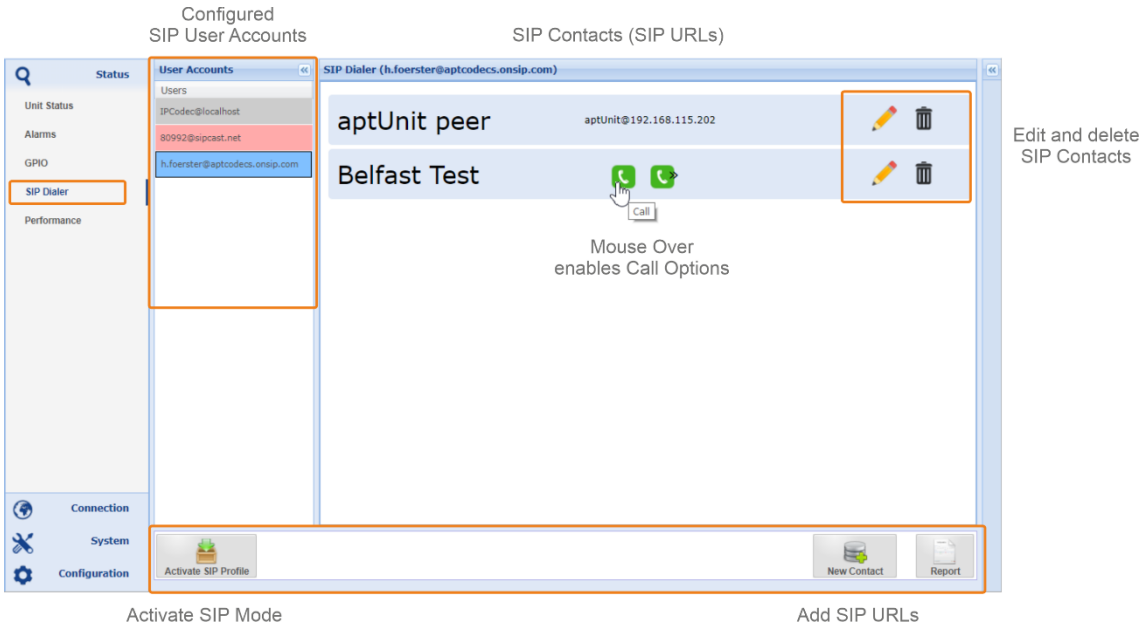


Figure 3-10: Shows the SIP Dialer page (SIP User Agent)

User Accounts

A Peer-Mode SIP User Account is initially configured (but disabled on default). This is displayed in grey and indicates no SIP server registration (peer-to-peer mode does not use a SIP server).

The other two accounts were created in the system menu at "SIP User Accounts." Red indicates that registration on the server has failed. Blue indicates the successfully registered state. If a connection via one of these accounts is successfully established, this active account changes to green.

SIP Contacts (SIP URIs)

The list of contacts shows all entries in alphabetical order. The sorting is automatic and can be controlled by pre-fixing the contacts. A SIP URI is the address of the SIP contact and is described as SIP:user@domain. The figure above shows two contacts with individual names. The upper one is a peer-to-peer contact and uses the codec SIP name and its IP address as URI. This connection can be established without registering on a SIP server, but you need to know the current destination IP address.

The second contact uses the account SIP URI registered on a SIP server. The advantage of registration is that you do not need to know the current IP address of the contact; the SIP server automatically updates changing IP addresses (one main advantage of SIP mode).

Edit and delete SIP Contacts

Click on the icons to delete or edit the SIP contact. You can change the SIP URI of the name or the name of the SIP URI.

ⓘ *If you enter only the username of the SIP URI, the SIP domain of the current SIP account is appended automatically.*

Activate SIP Mode

You can manually activate the SIP mode by clicking on this button. Also, the SIP mode is automatically activated when you establish a SIP call. In this case, a warning appears that all active RTP direct connections are canceled.

Deactivating SIP Mode

If you load a "normal" RTP direct profile, the SIP mode is deactivated, and the device allows regular RTP connections.

3.3.4.1 Establishing a SIP Call

Figure 3-10 shows two green connection symbols in the "Belfast Test" contact when you hover the mouse over the name of the URL. The left one with the designation "Call" dials the connection immediately when clicking and uses the profiles determined at the selected SIP User Account (left in the picture) for sending and receiving (also refer to chapter 3.5.4.1).

Clicking on the second connection symbol (with the small arrows Figure 3-11) opens a selection window that allows using another previously defined SIP Codec profile. In this calling mode, the default profile configuration for the active SIP account is overwritten, and the use of the selected profile is **always symmetrical** (receive is the same as transmit).

ⓘ *The nature of a SIP connection is that only a single point-to-point connection can be established at a given time.*

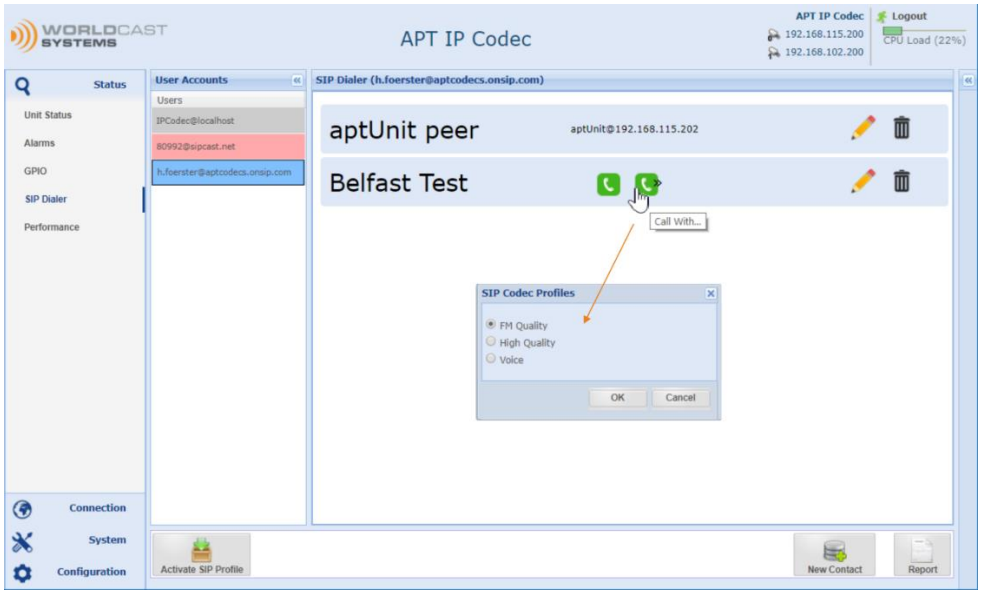


Figure 3-11: Mouse Over the icon with the small arrows opens a selection menu with predefined profiles.

3.3.4.2 Disconnecting a SIP Call

After a connection has been successfully established, it appears as a green entry on the top of the list and shows the red hang-up icon. In addition, the currently active SIP account also appears in green.

Click on the red hang-up icon to disconnect. The green entry in the list then disappears and the SIP account changes back to blue (registered but in inactive status).

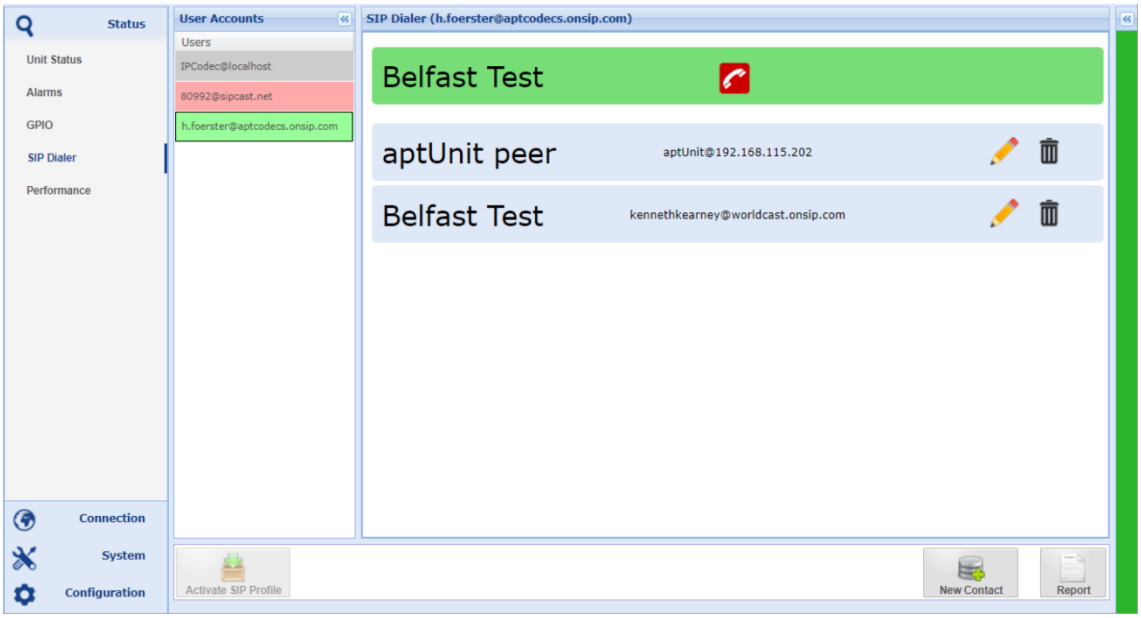


Figure 3-12: An active call is indicated by the green entry of the active URL at the top of the list.

SIP Profiles and Performance Monitoring

The creation and special features of the SIP connection profiles are described in detail in chapter 3.5.5.

The SIP performance can be monitored in the usual way on the performance monitoring page. The display does not differ from an RTP direct connection; please also refer to chapter 3.3.5.

Notes:

3.3.4.3 Incoming SIP Call

You can define in the SIP User Account configuration whether SIP calls should be answered automatically or not. If the auto-answer function is not active, the incoming call is alerted both on the SIP dialer page and in the top banner. You must accept the call manually in the dialog box. The alert in the top banner is a shortcut. Clicking on it opens the SIP dialer regardless of the currently opened page of the GUI.

ⓘ *Note, if the SIP mode has been activated, the SIP Dialer page is always displayed as the GUI start page.*

Move the mouse over the green banner to make the caller's address visible.

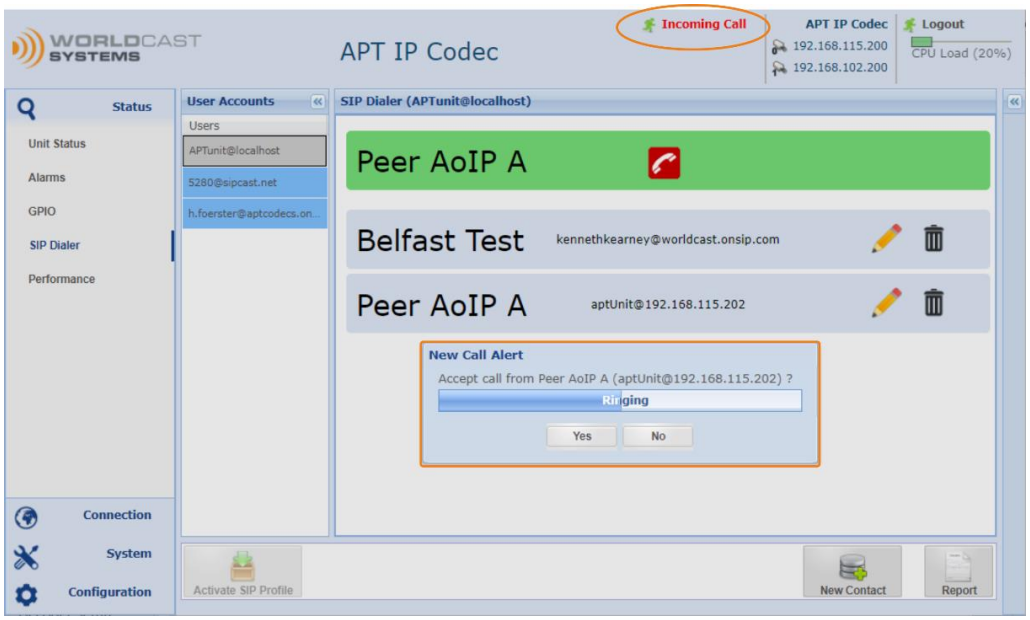


Figure 3-13: Shows the call alert in a dialog box and on the top banner of the GUI.

3.3.4.4 Incoming SIP Call – add to Contact List

An accepted incoming SIP call can be easily added to the contact directory by clicking on the "Add" icon. The name of the caller can be edited individually.

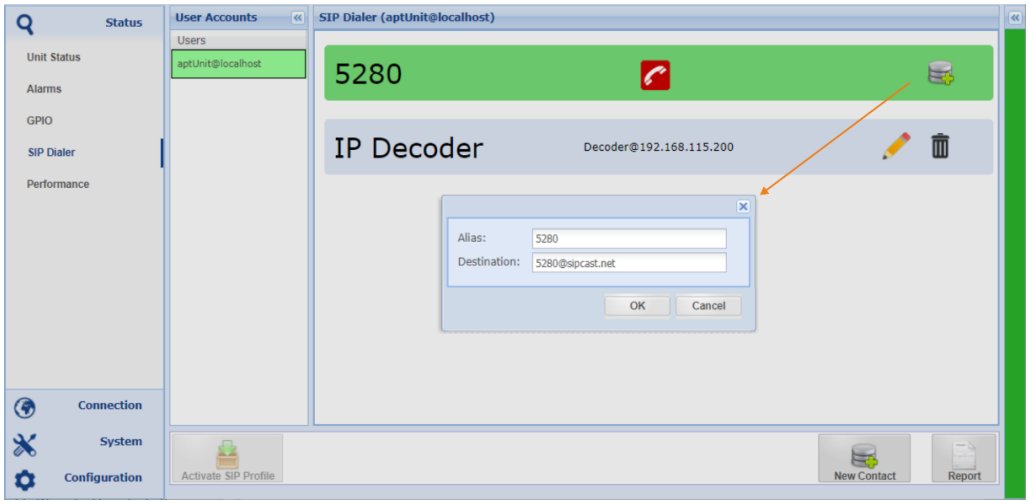


Figure 3-14: Shows an incoming call and how to add a caller to the contact list

.

3.3.4.5 SIP Call Monitoring

The result of a SIP/SDP negotiation for a multi-algorithm profile or a simple connection is displayed on the Unit Status page.

Here you can see which algorithms have been selected for the encoder and decoder.

The dynamic SIP connection profile is loaded automatically (Active Profile) in SIP mode.

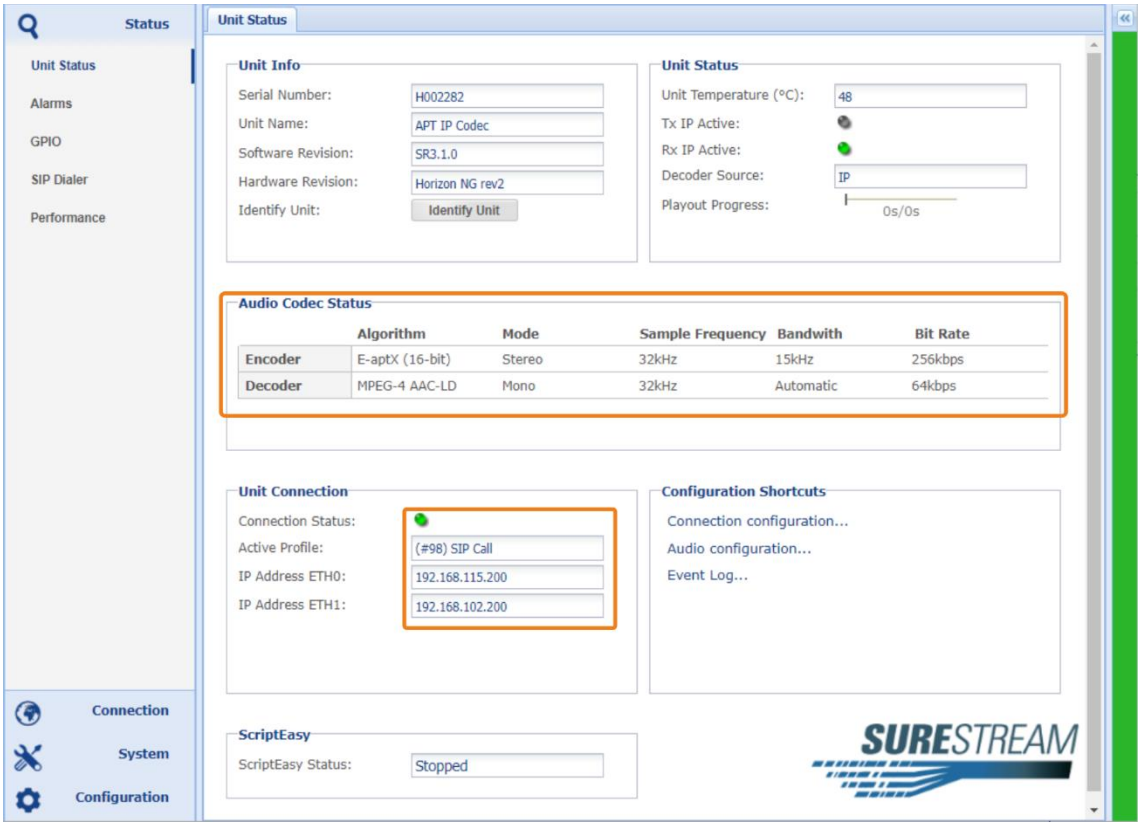


Figure 3-15: Shows the codec status of an active asymmetrical SIP connection (peer mode).

Notes:

3.3.5 Stream Performance Monitor

The performance monitor applies to all active send and receive streams, regardless of RTP/UDP or SIP connection mode. If you click on an individual stream in the stream performance table, the performance details are displayed below the streams table. The IP statistics show transmit or receive values or both depending on the selected stream type.

Additional parameters are displayed if a **time-synchronous** transmission mode is enabled (refer to Appendix 8.0).

The data refresh time interval is set to 1 second by default but can be selected by the user between 10s and 500ms.

A click on the "Reset" button resets the IP statistics. A shortcut allows direct navigation to the "Connection Configuration" stream configuration page.

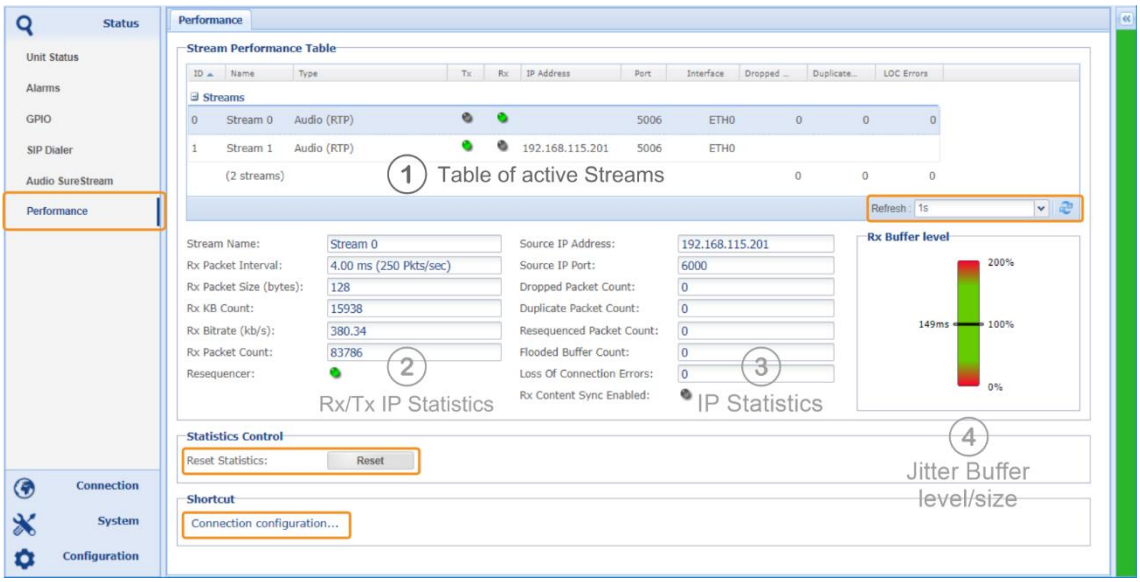


Figure 3-16: Performance Monitor details of a bi-directional stream

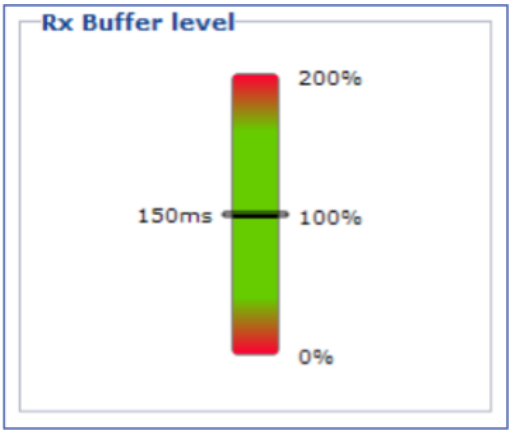
3.3.5.1 Packet Re-Sequencer

The Decoder utilizes a Packet Re-Sequencer to keep arriving packets in the correct order even if they arrive in the wrong sequence because of the network delay jitter behavior. The Re-sequencer performs best with a minimum number of six (6) packets in the buffer. Consequently, the buffer size should be chosen according to the six packet sizes. The validation engine prompts you to modify this setting whenever a packet and buffer size mismatch is identified (also refer to section 3.4.11 pos. 14); the re-sequencer is always enabled. Even with a validation warning, the Re-sequencer stays active.

3.3.5.2 IP Statistics – Receive Buffer Level

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

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



3.3.5.3 IP Statistics – Details

This section shows the IP statistics (2) & (3) of Figure 3-16 of a selected stream. The table below describes each of the statistics. Clicking on "Reset" resets all values.

Statistic	Description
② Stream Name	Shows the name of the analyzed stream
② Rx or Tx Packet Interval	Shows the packet time (p-time in msec.) and the packet interval per second
② Rx or Tx Packet Size	Size of the received or transmitted packet in Bytes
② Rx or Tx kB Count	Kilo Bytes received or transmitted
② Rx or Tx Bit Rate	The bit rate of receive or transmit stream (data & IP overhead)
② Rx or Tx Packet Count	Number of packets received or transmitted
② Rx Re-Sequencer	Indicates that the re-sequencer is enabled (no configuration options)
③ Rx Source IP Address	IP Address of the transmitting Codec
③ Rx Source IP Port	IP Port on which the transmitting Codec is sending the stream
③ Rx Dropped Packets Count	Number of dropped packets
③ Duplicated Packets Count	Some duplicated packets arrived on the Rx stream.
③ Re-Sequenced Packets Count	Number of packets that reached the de-jitter buffer out of sequence (also indicates the level of re-sequencer activities)
③ Flooded Buffer Count	The Buffer has detected above 200%. The buffer level has been normalized to mid-point by the engine
③ Loss of Connection (LOC)	Loss of connection is detected if the buffer level has dropped to 0%.

3.3.5.4 About Streams Tables (general)

A Stream Table (1) is a list of IP-Stream configurations organized in a table. The table can be directly accessed by changing values and entries on the connection pages. It appears in read-only mode depending on where a stream table is accessed, e.g., on the performance monitor page,

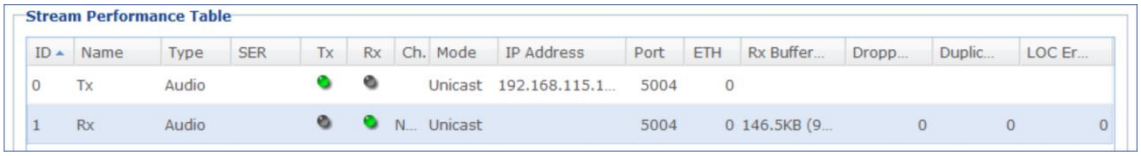


Figure 3-17 shows a Stream Table with two active streams in read-only mode (Performance Monitor)

Streams Table Exposure Options

The exposure of the Stream Tables 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 column's visibility. In general, the stream table exposure also depends on the current browser window size. The width of the columns can be adjusted by clicking between the columns and dragging the border as appropriate.

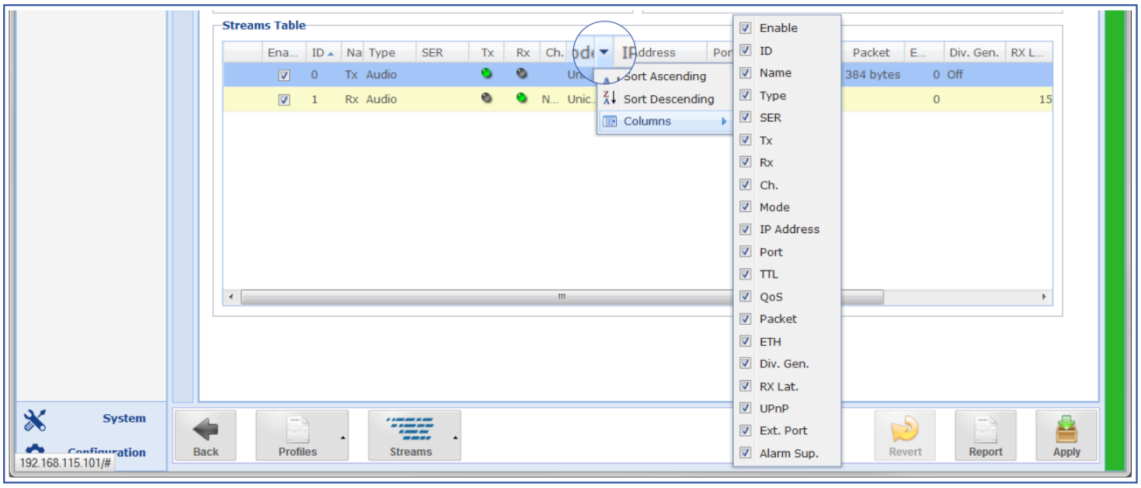


Figure 3-18 Exposure options on the Streams Table (connection page)

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 the codec format and IP streams settings.

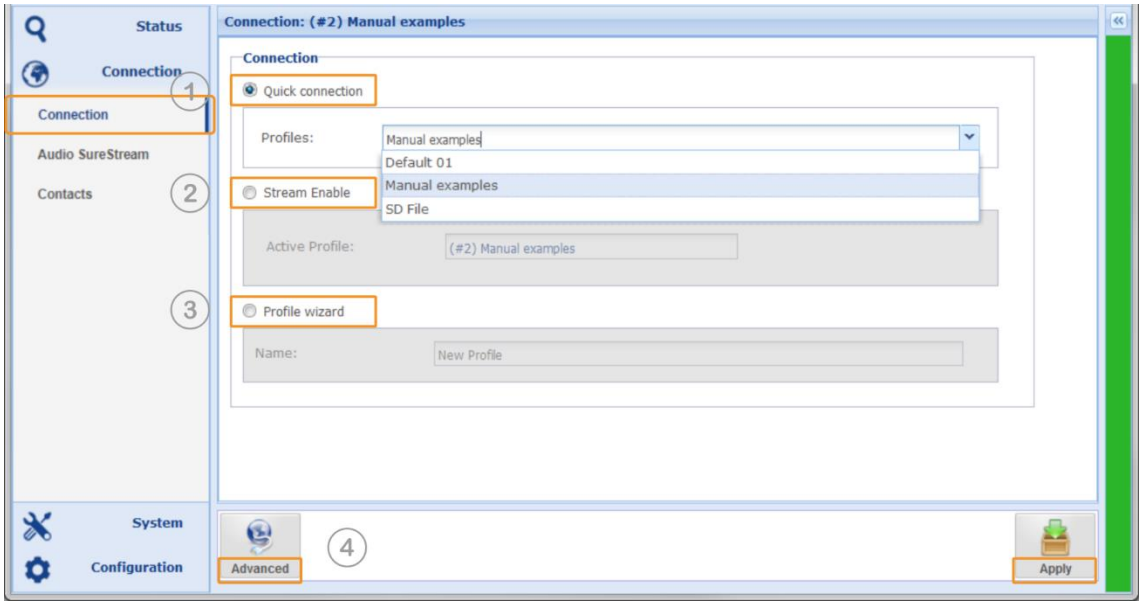


Figure 3-19 shows the Connection Page with all options

The WEB GUI offers three ways to create, manage and 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 are not active until it is 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 is 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. For example, the profile on the screenshot below has two streams. Clicking on the "Push to Enable" / "Push to Disable" button immediately enables or disables this stream. Applying this change is unnecessary; therefore, the "Apply" button disappears for this function.

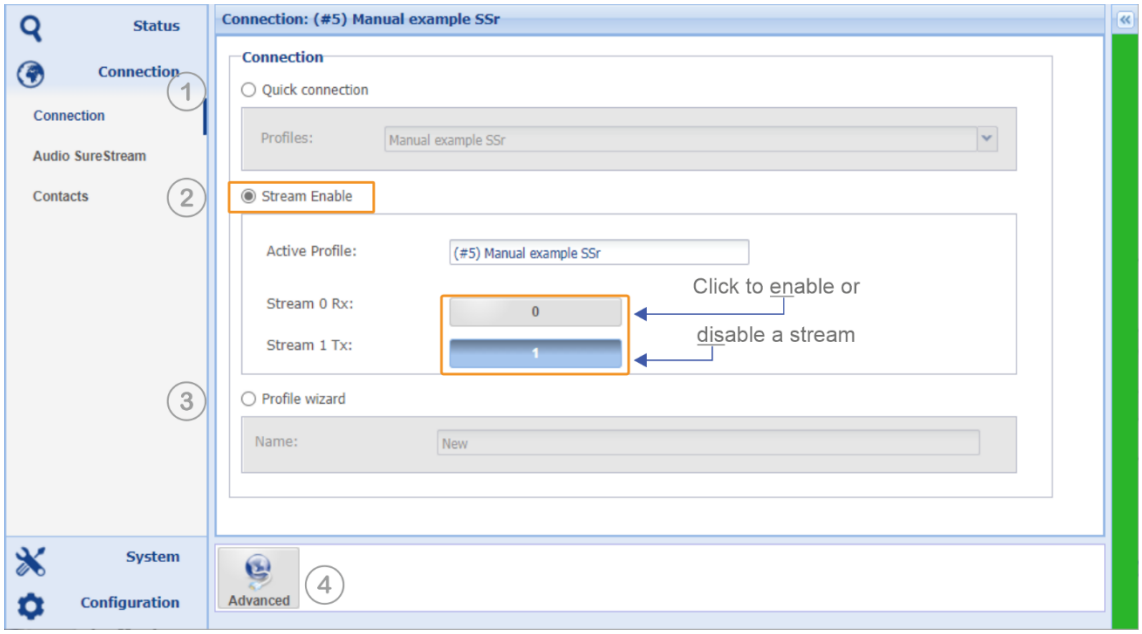


Figure 3-20 shows the Connection Page – Stream Enable

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 (refer to section 3.4.1 and following).

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. In addition, it provides choices and tools to edit already created profiles (refer to section 3.4.18).

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, click the "Next" button to move on to the audio settings.

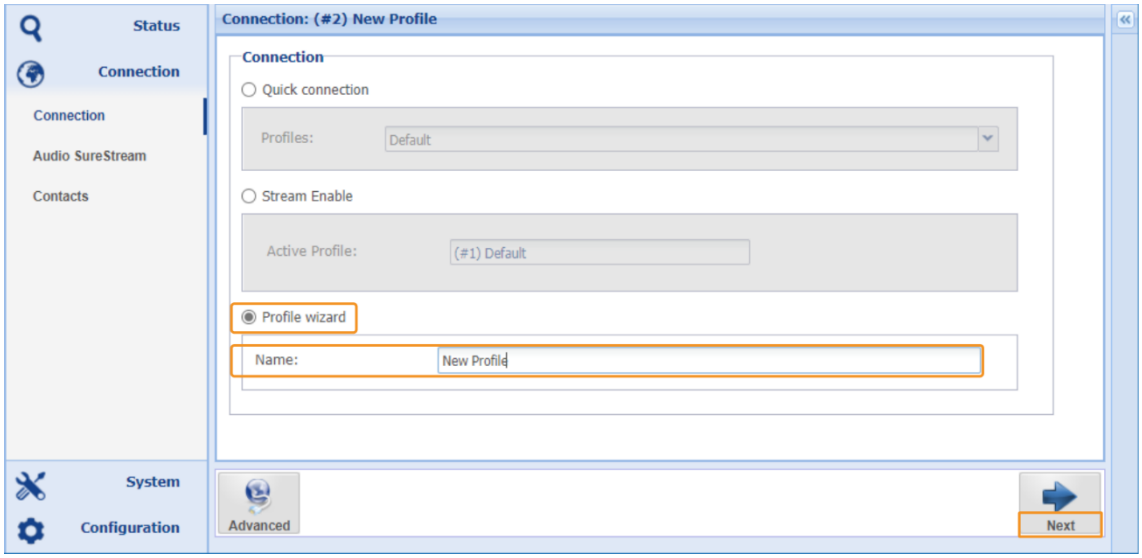


Figure 3-21 shows the Connection Wizard's first page

Notes:

3.4.2 Profile Wizard – Encoder Settings

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

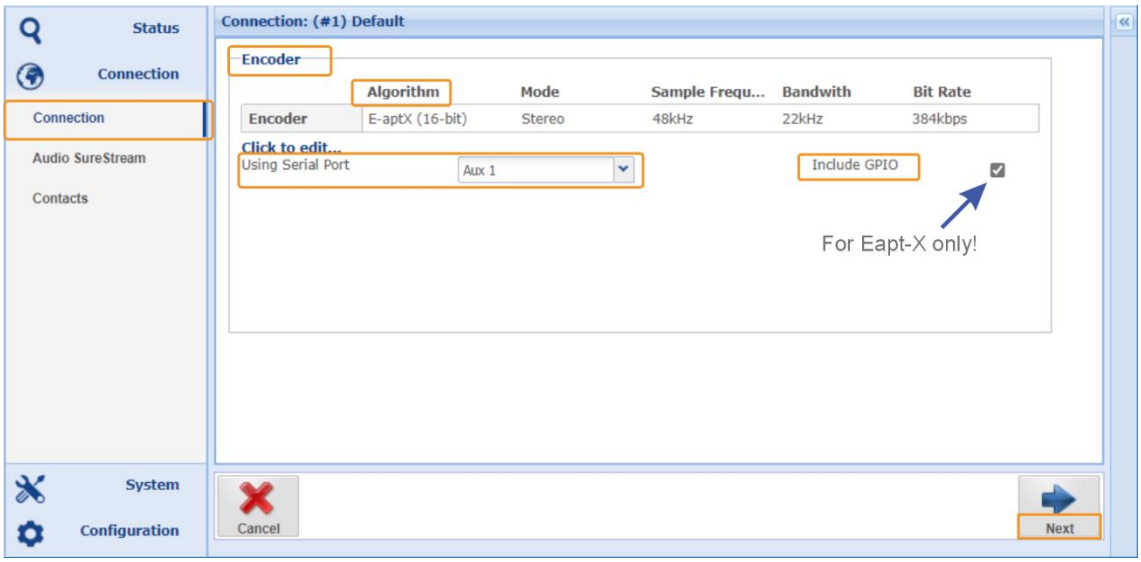


Figure 3-22 Encoder options of the profile wizard

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)

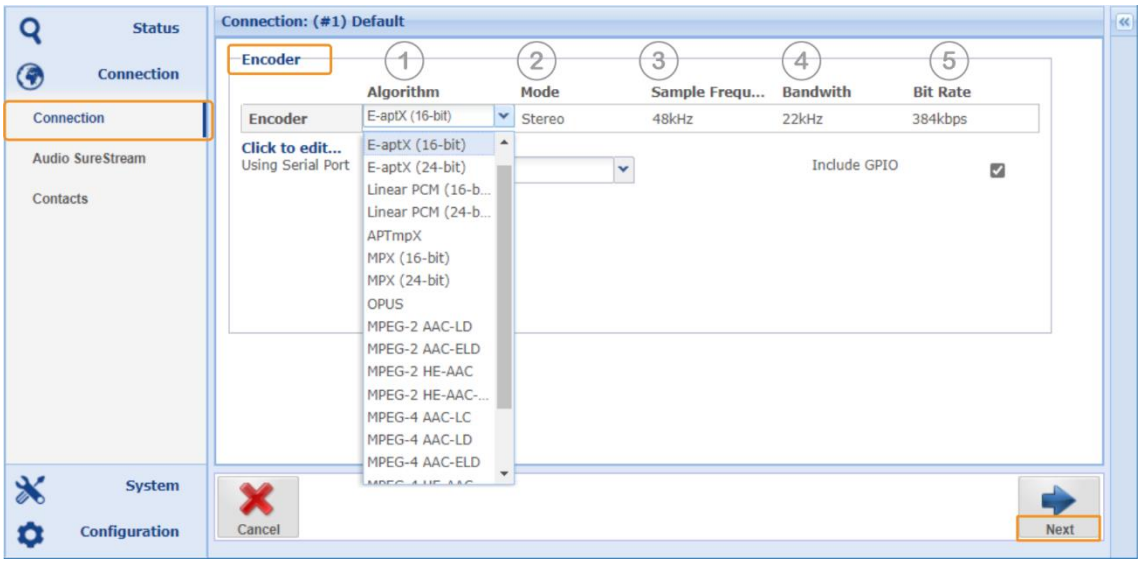


Figure 3-23 shows the Encoder configuration page

(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 following 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 you want to configure a bi-directional connection). The principle of the Encoder and Decoder configuration is almost identical.

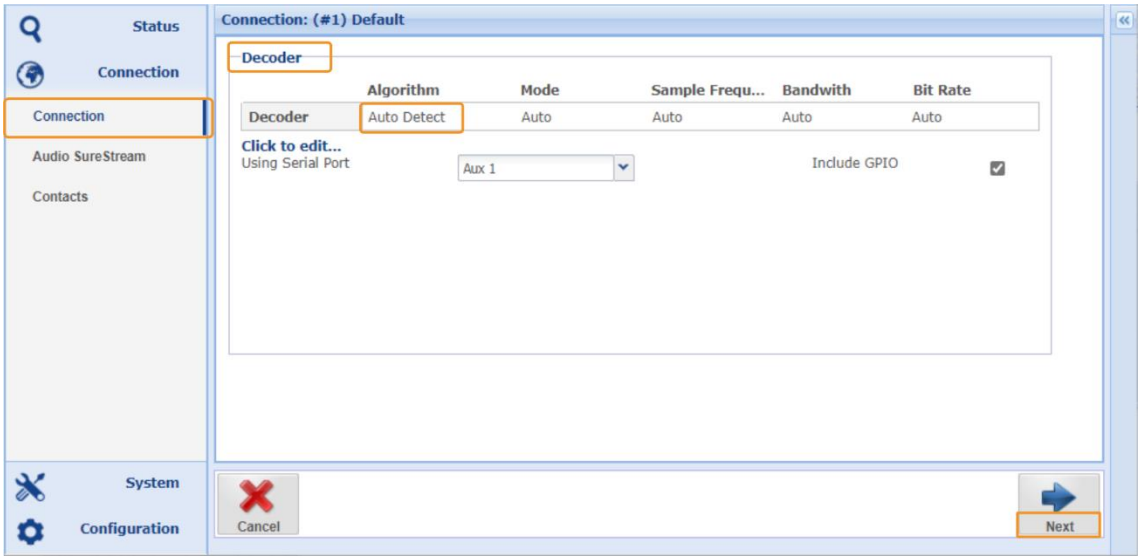


Figure 3-24 shows the Decoder configuration page in "Auto Detect" mode

In addition to the manual selection of audio algorithms, the Decoder supports the "Auto Detect" 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 set up the IP streams.

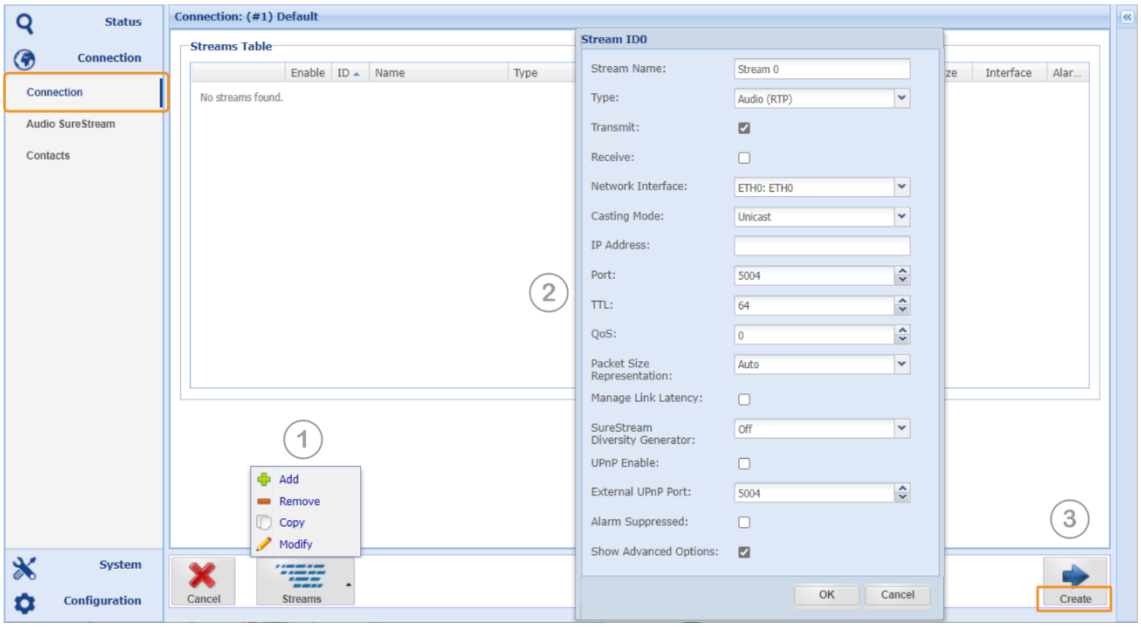


Figure 3-25 shows the IP Stream configuration page with the stream setup window open

The Wizard first presents an empty stream table from the audio settings page.

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, the second or more streams can be added by clicking on the "Add" button. Each stream gets a unique ID assigned by the system. Users cannot modify this ID.

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.

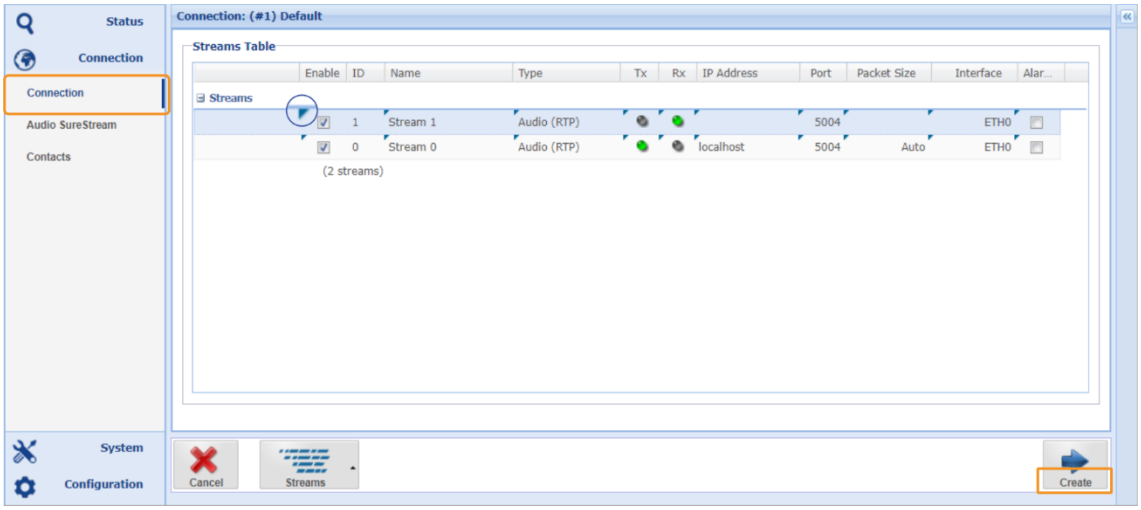


Figure 3-26 shows two streams ready to be merged into a profile

Clicking on the "Create" button 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 3.4.18) provides all options on a single page. A shortcut link on the status page opens the advanced configuration page directly.*

3.4.7 Profile Wizard – Apply a Profile

How to apply the "New Profile" you have just created is described in detail in section3.4.18. The "Advanced" configuration page provides all stream and profile configuration options on a single page.

Notes:

3.4.8 Audio SureStream Connections

The Audio SureStream page simplifies a connection with SureStream in the way that this page combines configured profiles and contacts from a list and establishes a SureStream connection with a few clicks.

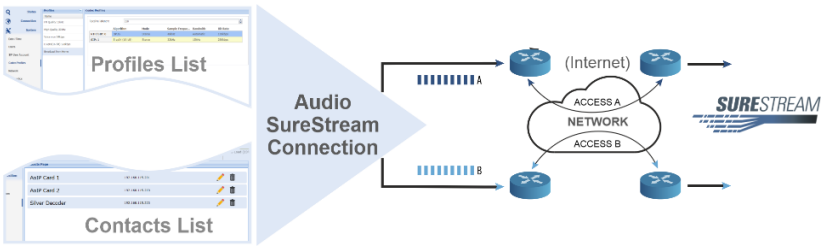


Figure 3-27: Audio SureStream configuration with a few clicks

If you do not want to use the Audio SureStream configuration page, please refer to chapter 7.0 to configure SureStream individually. The individual configuration is recommended if you want to deviate from a standard Audio SureStream Connection with two streams.

Audio SureStream is linked to the Codec's SureStream license. If no license has been applied, this menu option does not appear.

Audio SureStream Page

You can reach the Audio SureStream configuration in the main menu or the Connection menu.

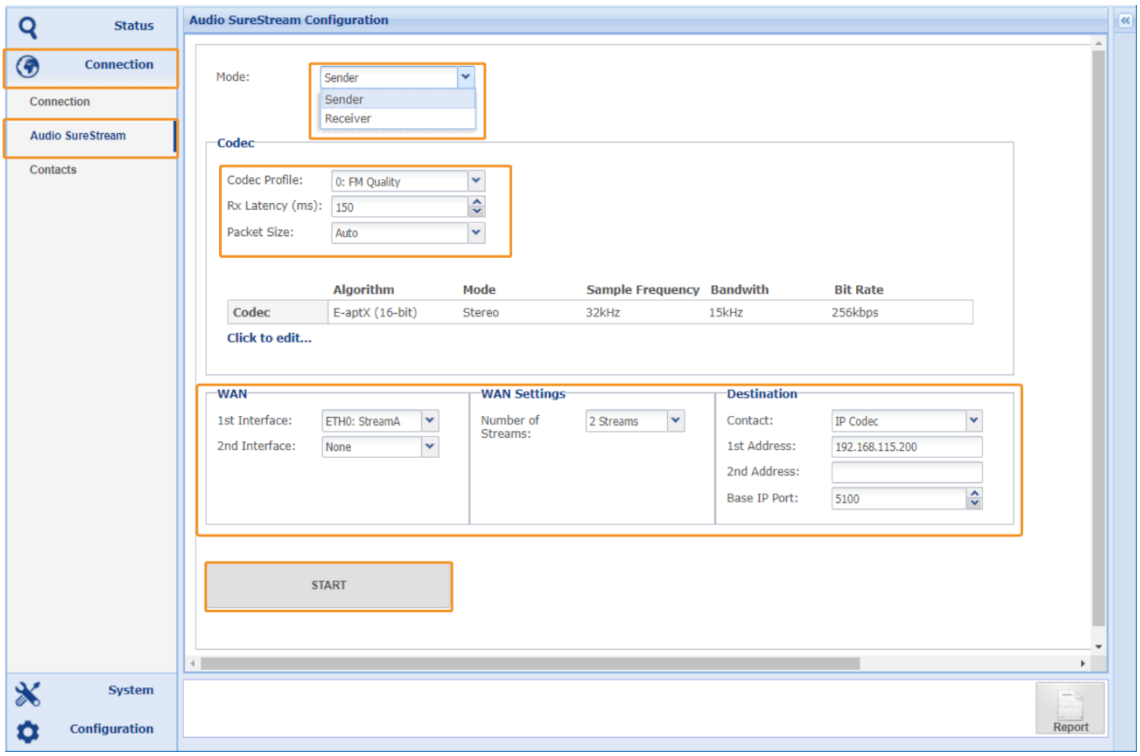


Figure 3-28: Shows the Audio SureStreamer page (reached from the Connection menu)

The designations "Sender" and "Receiver" of the Audio SureStream configuration only describe the role of the dialer and the called party. The audio connections are always bi-directional.

3.4.8.1 Sender Mode – Audio SureStream

As a sender, you select the mode "Sender." Then, in the next panel, "Codec," you define the parameters of the connection.

- **Codec Profiles** choose from one of the existing profiles from the drop-down list.
- **RX Latency** sets the size of the jitter buffer of your codec.
- **Packet Size** here, you can further influence the connection's latency with the packet size.

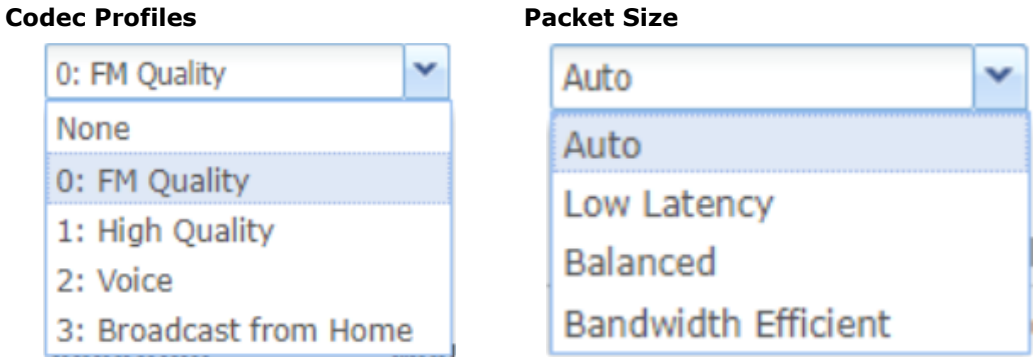


Figure 3-29: Shows the Connection Profiles and the Packet Size drop-down lists

Codec Profiles – Audio SureStream

This list contains all connection profiles that you have created in System Menu -> Codec Profiles. For the Audio SureStream connection, select a profile from the list.

How to create profiles is explained in section 3.5.5.

Packet Size – Audio SureStream

Here you determine the packet size of the stream in the direction of the receiver, i.e., this setting affects the latency between you and the caller. The Packet size is described in terms of its effect on transmission and is algorithm specific.

- **Auto** is enforced by framed algorithms. In non-framed formats, "Auto" tries to respect a p-time of 4ms except in formats where the packet size would exceed the MTU of the system.
- **Low Latency**: Here, the smallest possible size is selected. This results in lower latency and a higher network load.
- **Balanced**: This medium size allows lower latency with moderate network load.
- **Bandwidth Efficient**: This generates large packets and reduces the network load. The link latency can increase significantly depending on the audio format.

Codec – Audio SureStream

Here you can see the details of the audio format created by the selected profile. You can make changes with a click on "Click to edit...". These overwrite the current settings but not the profile.

Network and Destination – Audio SureStream

The following descriptions also refer to Figure 3-28 on page 54.

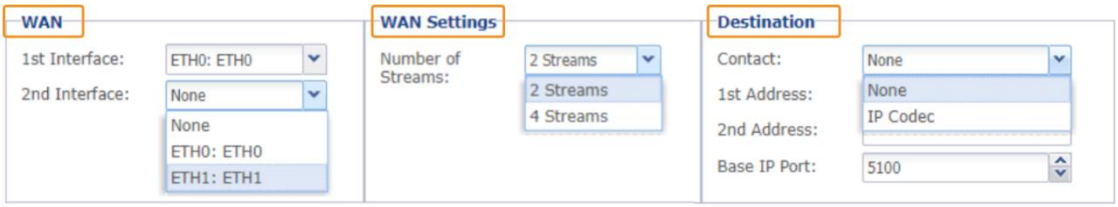


Figure 3-30: Shows the network and destination controls

WAN here, you determine which network interface of your codec you want to use. You can stream over a single network interface (e.g., your xDSL) or both. The advantages of the dual network connection are described in section 6.1.

- In the "1st Interface" list, select your codec's ETH port. This can be ETH0 or ETH1.
- In the list "2nd Interface," select:
  for single network access, select the same ETH port as for "1st Interface" or "None".
  for dual network access, select the remaining ETH port.

ⓘ *Note: If you have only one network access, you can select either "None" in the "2nd Interface" list or the same interface as for "1st Interface". In both cases, all streams are routed through a single interface.*

WAN Settings here, you define how many streams you want to send to the partner codec. In standard DSL connections, these are usually 2 streams. However, if you stream, e.g., via mobile networks, a four-way connection is recommended.

Depending on the settings under "WAN," the streams are distributed to the respective selected ETH interfaces.

ⓘ *Note: Both interfaces must have a valid gateway address for dual network access.*

Destination, whether you enter only one destination address or two, depends on the installation of the partner to be called.

- Enter the destination IP address in the field "1st Address."
- Enter a second destination IP address in the field "2nd Address."
- Enter the Base IP Port number in the corresponding field. A base port can be any even number in the 5000 port range. The default base port is 5004.

As shown in the picture, you can also select a previously created contact from your contact list. This selection also applies the destination address(es) and the base port. To learn how to create a contact list, see section 3.4.8.3.

Start – Audio SureStream

After you have selected a connection profile and a contact, click on "START." This saves your configuration for this connection and starts the connecting process. You cannot make any changes during the connection. Click again on this field "STOP" to terminate the connection.

3.4.8.2 Receiver Mode – Audio SureStream

You can reach the Audio SureStream configuration in the Main or Connection Menu. The following figure shows the access via the Main Menu.

The designations "Sender" and "Receiver" of the Audio SureStream configuration only describe the role of the dialer and the called party. The audio connections are always bi-directional.

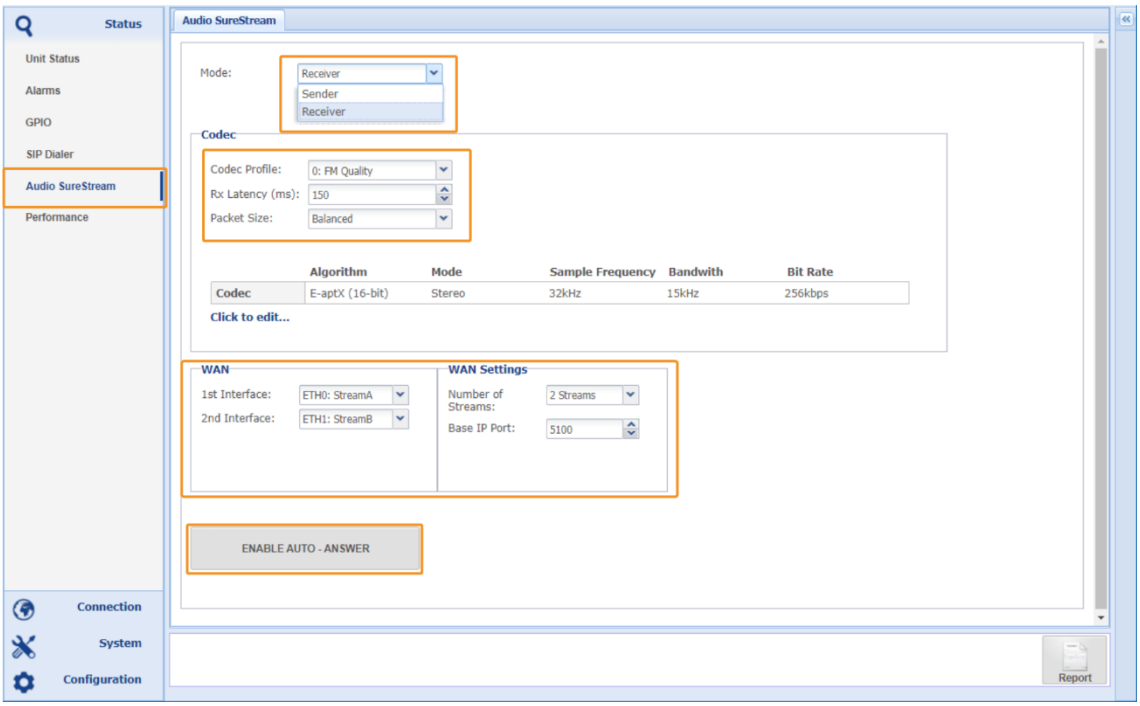


Figure 3-31: Shows the Audio SureStream page in Receiver Mode

Receiver Mode Requirements

The receiver mode is a passive mode in which the codec is switched ready to receive and waits for the sender's connection. The receiver cannot and does not need to do anything to establish a connection. The connection is established if "Auto Answer" is activated and the connection parameters match.

Audio SureStream does not negotiate the connection parameters. Therefore, unlike a SIP connection, the two devices must operate in the same mode.

Receiver Mode – Complementary to Sender Mode

To answer a specific call, the receiver profile and the WAN parameter must complement this caller.

- **RX Latency** sets the size of the jitter buffer of your codec. The buffer can be set independently of the setting on the caller. This setting only affects the latency from the caller to the receiver.
- **Packet Size** here, you can further influence the connection's latency with the packet size. The packet size can be set independently of the setting on the caller. This setting only affects the latency from the receiver to the caller.

Network and Auto-Answer – Receiver Mode

The same conditions apply to WAN and WAN Settings as described in the chapter Sender Modes (section 3.4.8.1). In Receiver mode, we do not need any information about the destination.

Receiver Base Port

For an incoming call to be recognized, the base port of the sender must be known, or the sender must address the selected base port of the receiver.

⚠ Base ports must be the same at the sender and receiver.

AUTO ANSWER

As long as Auto-Answer **is not** activated, **no call** is accepted.

➡ Click on "ENABLE AUTO-ANSWER" to be ready to receive.

3.4.8.3 Audio SureStream Contact List

For recurring connections, contacts and their destination addresses can be created and selected from the "Destination" panel on the Audio SureStream connection page in sender mode (refer to section 3.4.8.1)

ⓘ *This contact list is part of the SureStream License and does not appear if SureStream has not been unlocked.*

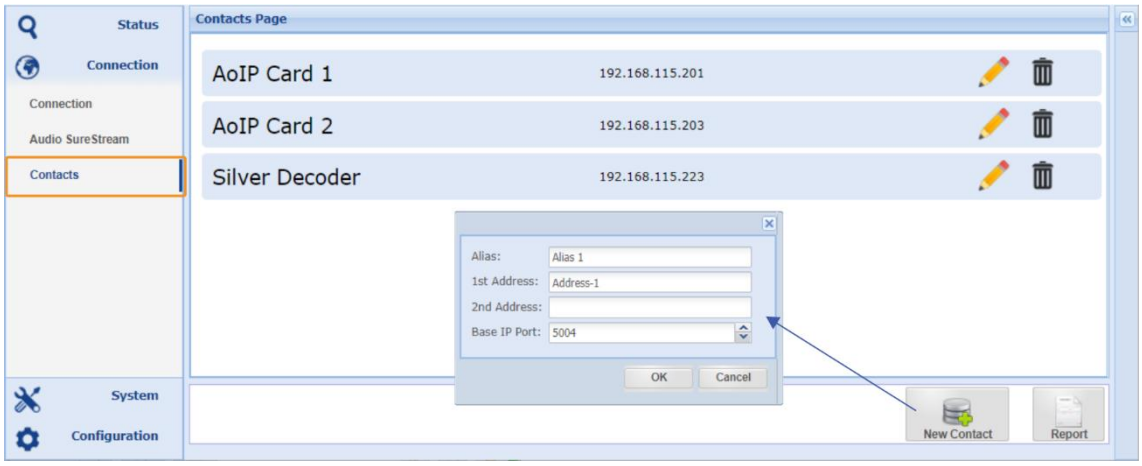


Figure 3-32: Shows the Contacts List of the Audio SureStream connection page

Create a new Contact

Double-click in the page's empty area or on the "New Contact" field to open the window for entering new contact data.

Enter a name (the list is sorted alphabetically), one or two destination addresses (these can also be hostnames) and the base IP port. Confirm your entries with "OK." The new contact is now added to the list.

3.4.9 IP Stream Configuration – General

The stream configuration window provides options for different stream types and operational modes.

Adding a new stream opens the configuration window with basic options. Enabling "Show Advanced Options" expands the configuration window presenting all stream options

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

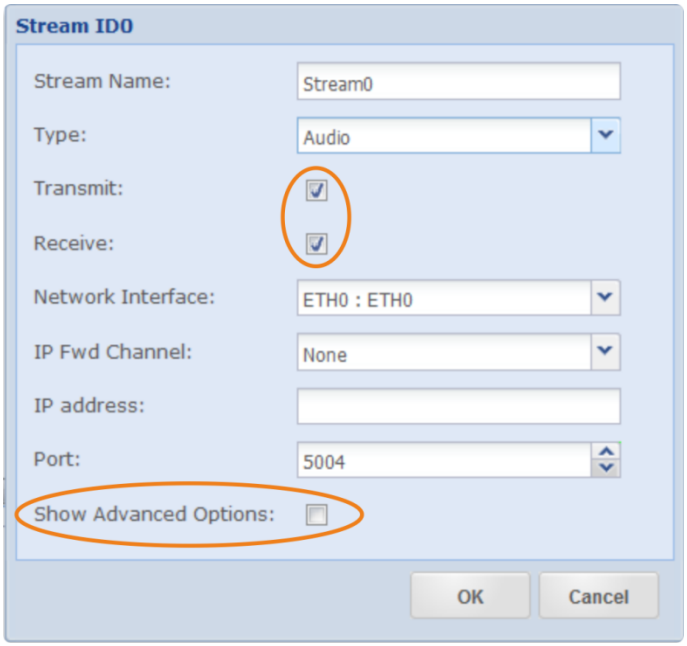


Figure 3-33 shows the basic configuration options for Audio streams

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

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

3.4.9.1 About Stream Types

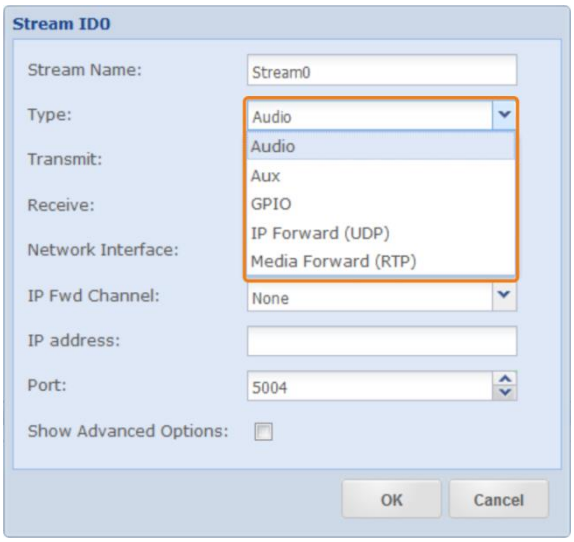


Figure 3-34 shows the stream type selection menu

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 precisely 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 of the same nature as 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)

3.4.10 About Stream Forwarding

The APT Codec range supports IP Stream Forwarding as standard. This unique feature allows receiving and forwarding of audio or non-audio data streams, like RDS, PAD, E2X and 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, EDI or E2X over UDP from a server, the Encoder receives the UDP stream and allows forwarding the same. It is a user's 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 selected separately for receiving and transmitting. However, the splitting in Receive and Transmit enables the use of both modes on the same stream, thus re-encapsulating UDP to RTP/UDP (refer to Figure 3-41).

IP Forwarding – UDP Forwarding

We use the term "**IP** Forward" for forwarding 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 it can also be utilized for media streams. 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, EDI, or E2X and any protocol.

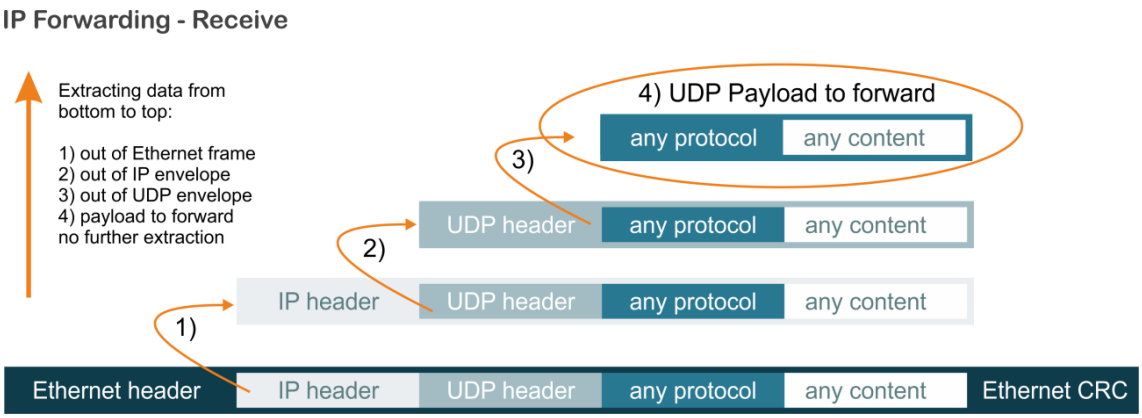


Figure 3-35 shows how "IP Forward receive" extracts the payload on a receiving stream from the bottom to the top of the image – this mode is payload agnostic.

IP Forwarding (continued)

IP Forwarding Transmit

This mode complements IP Forward Receive and describes the opposite flow direction. It must be used on the Decoder to forward the received data to the final destination.

⚠ The Forward "Receive" and the Forward "Transmit" method (RTP or UDP) must be the same on both ends of the link.

If the stream is bi-directional, 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.

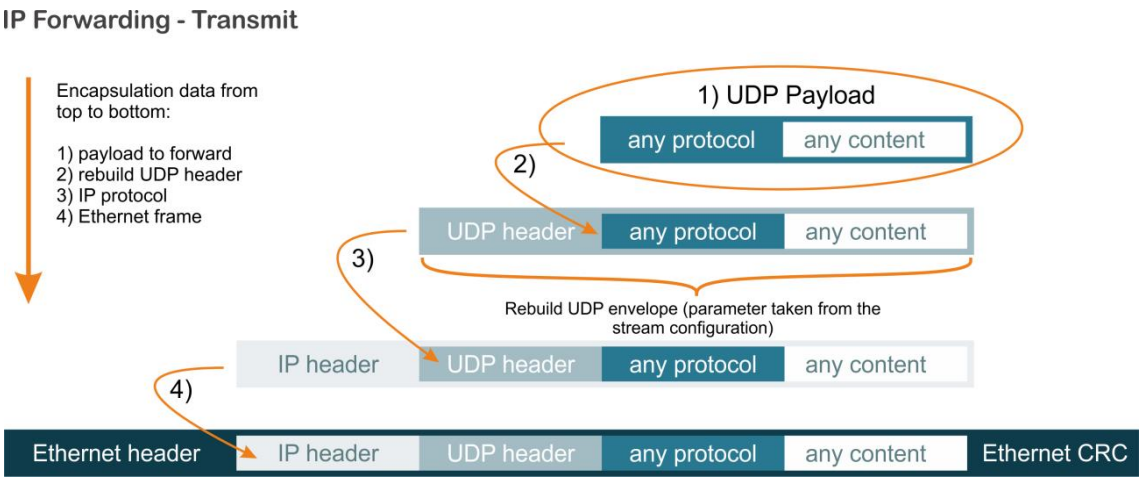


Figure 3-36 shows how IP Forward "Transmit" encapsulates the payload on a transmit stream from the top to the bottom of the image.

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

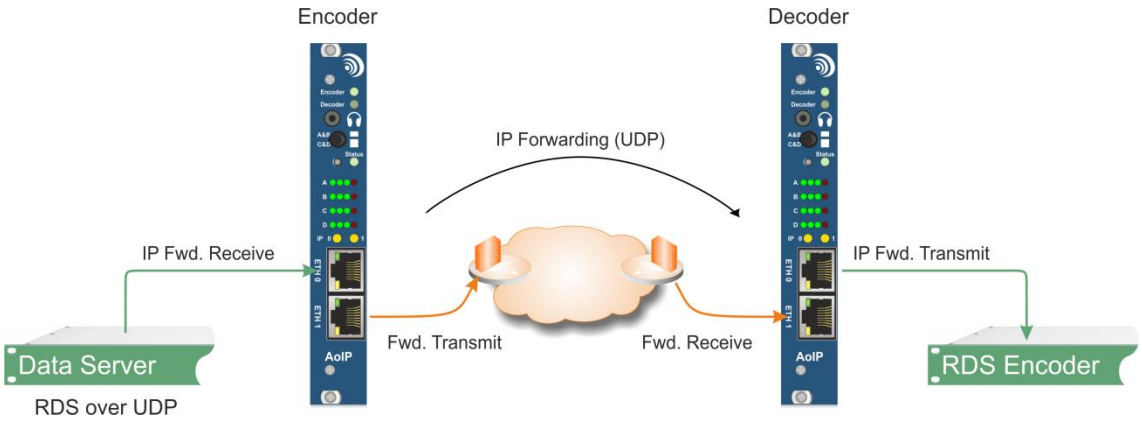


Figure 3-37 shows an example of IP Forwarding for RDS data over UDP.

3.4.10.1 Media Forwarding – RTP Forwarding

We use the term "**Media** Forward" to forward content carried by the RTP protocol. The typical payload is audio or media content for real-time transmissions.

⚠ The modes for "Forward Receive" and "Forward Transmit" must be the same on both ends.

- 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 is rejected.

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

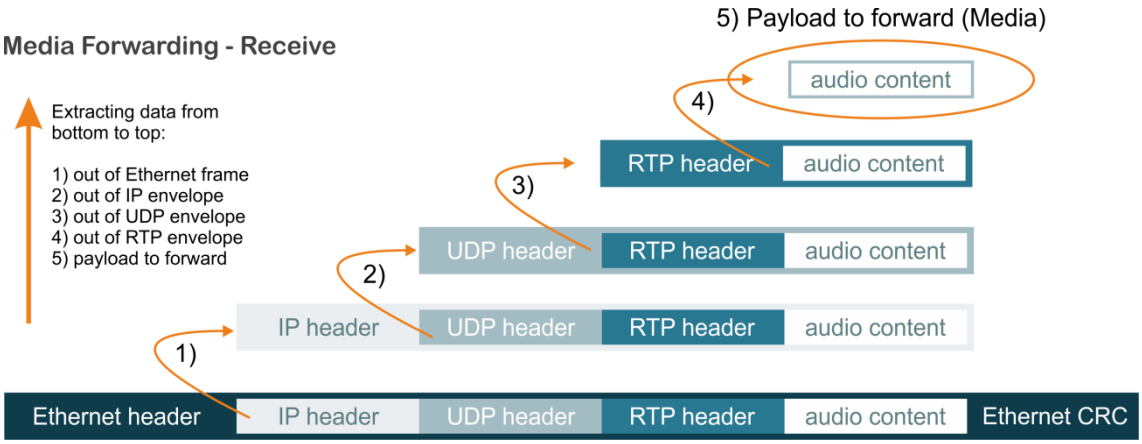


Figure 3-38 shows how Media Forward "Receive" extracts the payload on a receiving stream from the bottom to the top of the image – this mode is payload agnostic.

ⓘ *Media Forward Receive only expects the RTP protocol. Therefore, any UDP stream not containing the RTP protocol is 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 complementary to Media Forward "Receive" and describes the opposite flow direction. Media Forwarding Transmit encapsulates the media content in packets with a new RTP header and 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 3.4.10.

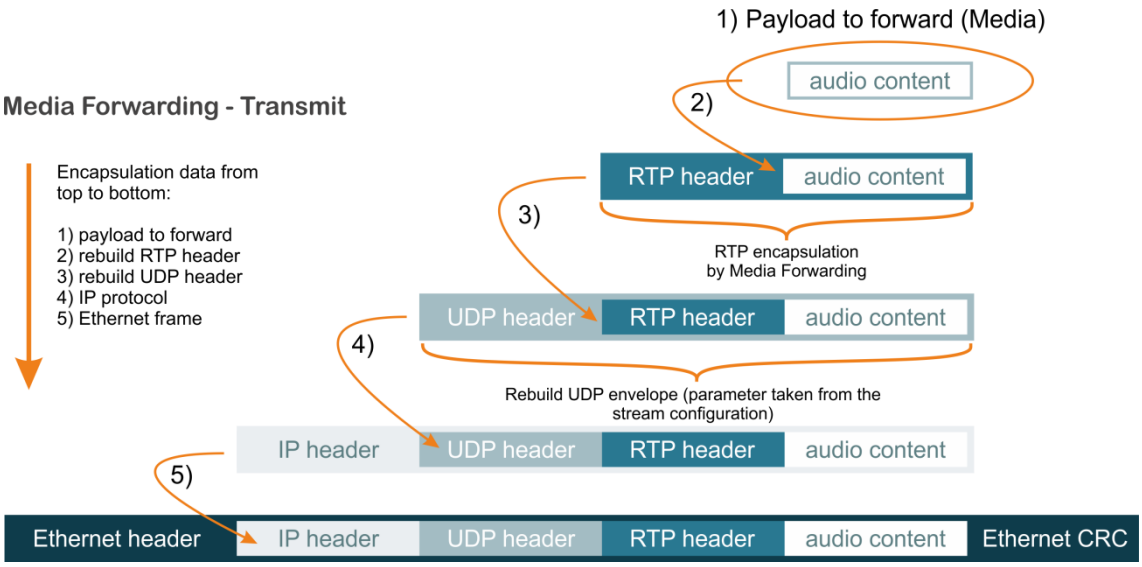


Figure 3-39 shows how Media Forward "Transmit" encapsulates the media payload on a transmit stream from the top to the bottom of the image – this mode is payload agnostic.

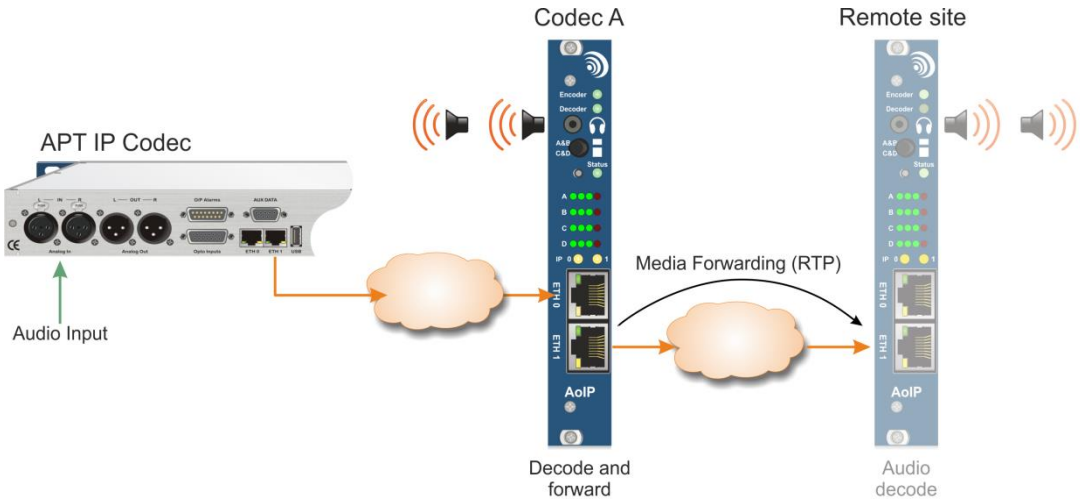


Figure 3-40 illustrates a typical Media Forward Transmit application with local content decoding (on Codec A).

3.4.10.2 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, redundant streaming and re-sequencing of the packet order and passing through the de-jitter buffer.

- Enc. – IP Forwarding Receive (Rx): UDP header removed
- Enc. – Media Forwarding Transmit (Tx): New UDP and RTP header added
- Dec. – Media Forwarding Receive (Rx): UDP and RTP header removed
- Dec. – IP Forwarding Transmit (Tx): New UDP header added

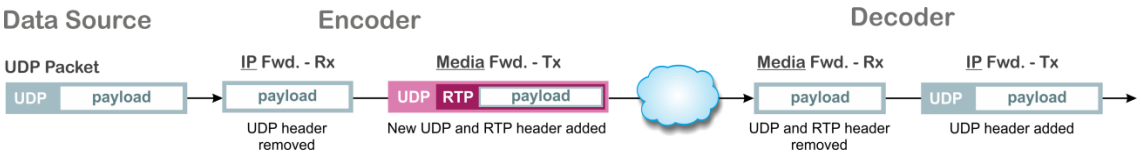


Figure 3-41 shows the signal chain of re-encapsulated UDP data in the RTP protocol.

Notes:

3.4.11 Audio Stream Configuration

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

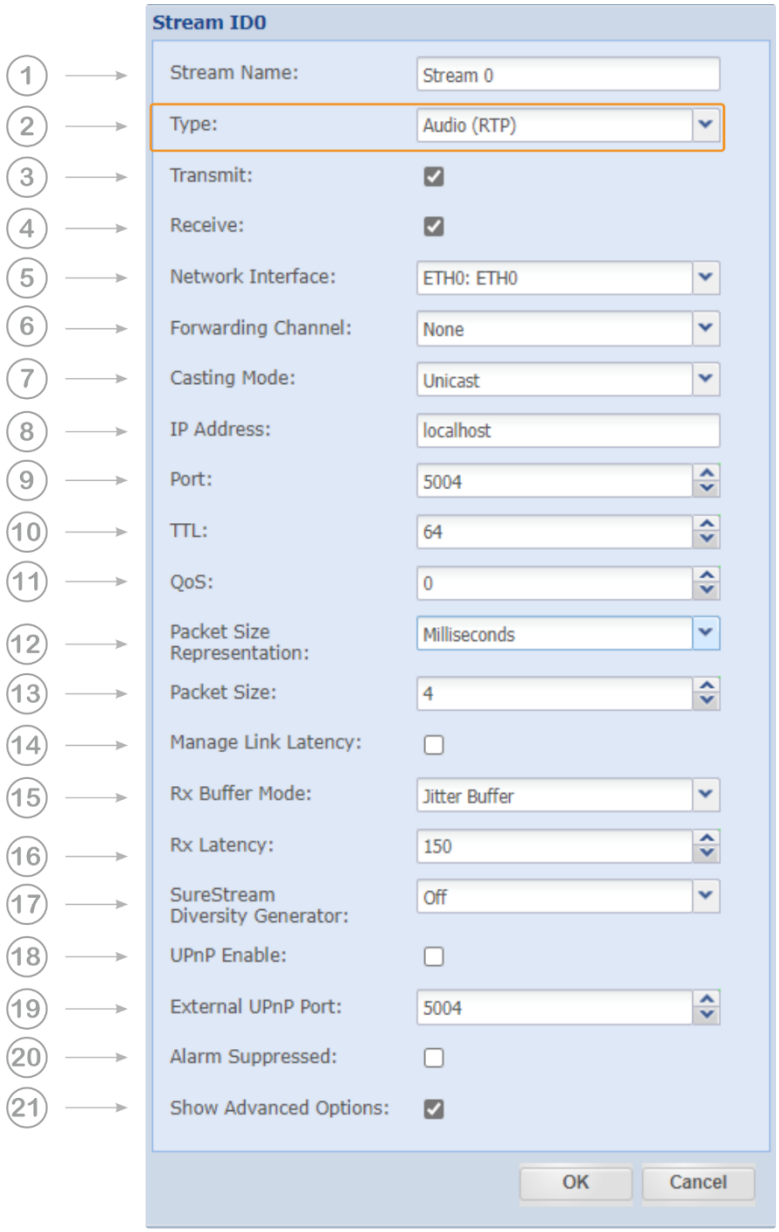


Figure 3-42 The IP Stream configuration window showing all available audio options

Manage Link Latency

For information on setting up the timing and synchronization functions, see section 8.0 (Appendix C).

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

ⓘ *SureStream is a cost option. For more details, refer to the SureStream section 7.0 in this document*

Audio Stream Configuration (*continued*)

1. **Stream Name:**
   Enter the name of this stream
2. **Type:**
   The selected Stream Type is: Audio (RTP)
3. **Transmit or**
4. **Receive or**

   Bi-directional (transmit and receive)
   Note: A bi-directional stream usually allows passing a NAT gateway without any further configuration on the external gateway.
5. **Network Interface**:
   Select this stream's network interface (ETH 0/1) or any pre-configured virtual interface. Both physical and all virtual interfaces can be used.
6. **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 to manage multicast joins and leaves; IGMPv2 and v3 (SSM) are 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 remote receiver's unique IP address, the network gateway, or a hostname. Using a Hostname requires an active Dynamic DNS service (refer to section 3.5.7.2). For multicast: Enter the multicast group address.
9. **UDP 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. Therefore, each stream must use a different port number. Port numbers for audio streams are even in the 5000 range (5004/5006/5008 …); 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 gets 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 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 only allows the QoS tagging of the packets. The range of the DSCP value is 0 (off) to 63 (highest priority). It is essential to know about the QoS implementation of the network before entering a value – the network router may not accept all values.

12. **Packet Size Representation**:
    A packet size can be described in Bytes/Packet or 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 following 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 or time per packet for all non-framed algorithms. For MPEG and the OPUS algorithms, use "Full Frame." If p-time is the representation mode, the millisecond value describes the amount of audio in a packet. The recommendation is 4ms or higher; less than 4ms is possible.

14. **Manage Link Latency**:
    This feature allows controlling the target latency of a link for FM MFN applications. This feature is described in detail in section 8.0

15. **Rx Buffer Mode**:
    The size of the jitter buffer can be determined by manual entry or by the time stamps of the encoder. This feature is described in detail in section 8.0

16. **RX Latency**:
    In Buffer Mode, this is the manual setting of the de-jitter buffer. 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 to cope with the network's delay jitter and maintain the minimum number of packets required for reliable operation. The recommended number of packets in the buffer is six, allowing the re-sequencer to work correctly.

17. **SureStream Diversity Generator**:
    This setting allows selecting the diversity generator level for SureStream component streams in Encoder Mode (Tx). It should be used when more than one component stream is connected to the same network via the same ETH port. This setting ensures that diversity is maintained under this condition (refer to the section: 7.1.5)

18. **UPnP Enable**:
    The "Universal Plug and Play" check box enables the IGD "Internet Gateway Device" feature for this stream. It is used to control the router's port management if the router allows it.

19. **External UPnP Port**:
    If UPnP is enabled, on default, the internal port equals the external port. Therefore, it 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.

20. **Alarms Suppressed**: Enabling this check box suppresses all alarms generated by this stream. Sometimes it is good to suppress alarms on a stream that do not apply to the given situation.
21. **Show Advanced Options**:
    Allows changing from "Basic Options" to "Advanced Options." This tick box expands the configuration window.

3.4.11.1 About Packet Sizes

A small packet size allows a lower latency transmission but adds significant packet overhead to the network.
A large packet needs more time to get "loaded" with payload, adding latency to the transmission. On the other hand, the overhead is significantly lower for larger packets. It depends on the network which packet size can be used.

Less powerful networks may require a larger packet size, while a high-performance network can get by with smaller sizes. The codec engine can generate multiple unicast streams. Streams with a small packet size require more engine power than larger packet sizes. The CPU usage bar in the top frame of the GUI indicates the CPU performance

3.4.11.2 Packet Sizes of Framed Algorithms

Framed algorithms like the MPEG formats and OPUS require full algorithm frame packet sizes. Each algorithm's frame size is different and presented in milliseconds of audio.

These algorithms set the packet size automatically and cannot be changed manually.

Coding 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
OPUS	20 ms	Not variable

3.4.12 IP Address Keywords

Keywords can be used instead of a destination IP address in the streams table. Keywords are not generic hostnames and serve specific purposes.

3.4.12.1 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.

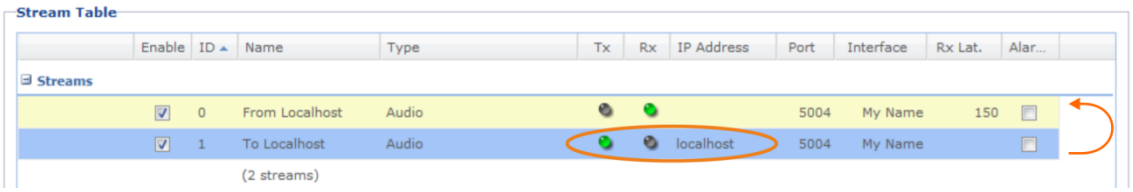


Figure 3-43 shows an example of the Keyword "localhost" is the IP destination

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

IP Address Keywords (*continued*)

3.4.12.2 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.

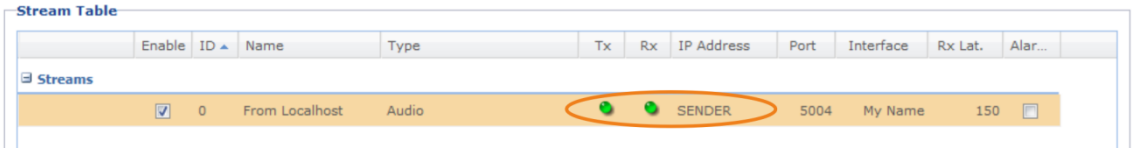


Figure 3-44 The Keyword "SENDER" is the IP destination

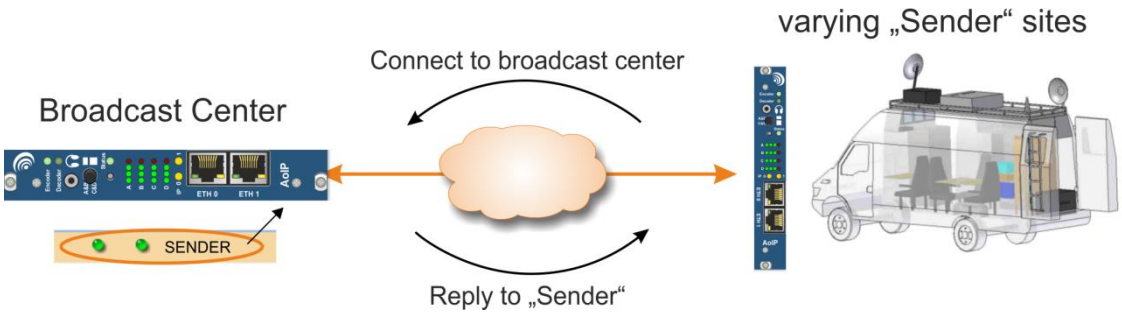


Figure 3-45 shows a typical application with varying remote sites – "SENDER" replies to the current sender address automatically.

3.4.13 NAT Traversal Streaming Mode

NAT (Network Address Translation) traversal is needed whenever a firewall or gateway prevents access from a network to a receiver.

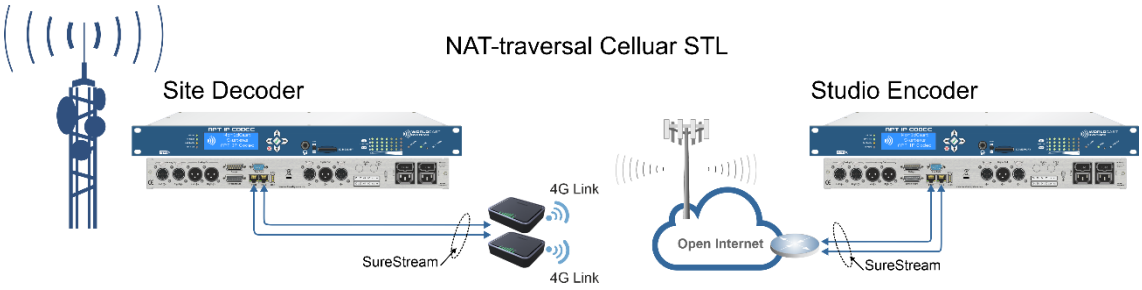


Figure 3-46 A cellular STL requires NAT-traversal streaming mode

A decoder receives the audio IP stream at the transmitter site over the cellular network. In this configuration, the encoder must transmit from the wired Internet to the air interface of the 4G/5G base station. Without action **by the receiver**, this transmission direction is blocked, and the receiver modem's public IP address is unknown.

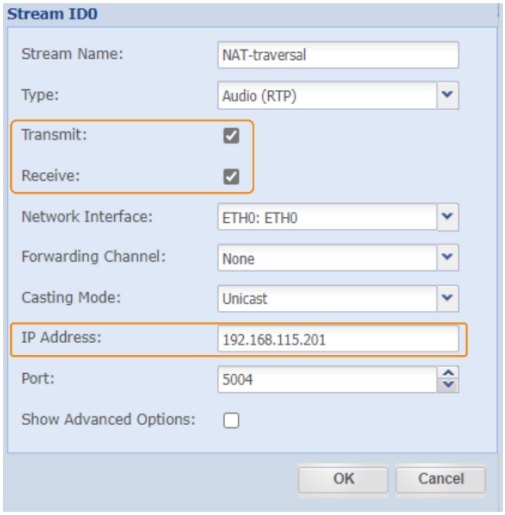
With NAT-traversal streaming mode, the receiver provides the transmitter with its current IP address and unblocked access.

3.4.13.1 NAT Traversal – **Decoder** at the Transmitter Site

- Open the stream configuration window
- Activate the tick boxes of Receive and Transmit
- Select the physical interface ETH0 or ETH1
- Enter the public IP address of the sending encoder
- Select the port through which you want to reach the encoder
- After you enter all data, deactivate "Transmit" by unchecking the box.
- Confirm all settings with "OK."

ⓘ *You configure the desired audio (Codec) format only in the decoder path of the stream.*

Activate "Transmit" and "Receive"



Deactivate "Transmit" and confirm "OK"

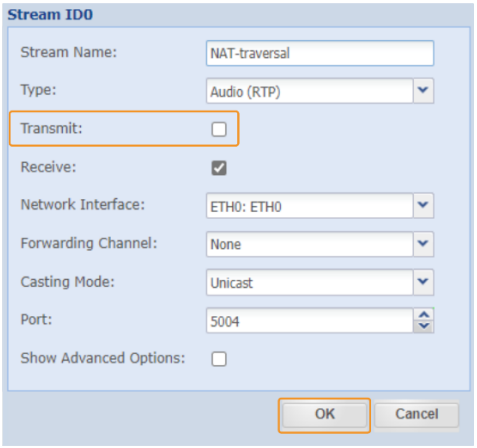


Figure 3-47 shows the configuration steps described above

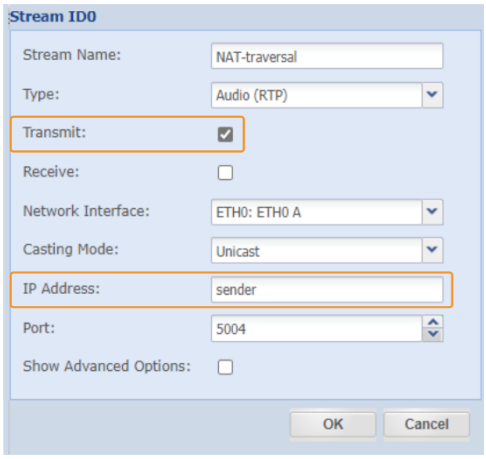
3.4.13.2 NAT Traversal – Studio Encoder

The stream configuration of the encoder is done as described in section 3.4.11. Set the keyword "Sender" as the destination IP address (refer to section 3.4.12.2).

The Decoder provides information about its current IP address to the Encoder and opens the network ports.

With the keyword "Sender," the Encoder responds to the Decoder's current IP address. Determining the IP address of the receiver is a periodic process to respond to updated IP addresses by the modem's DHCP server.

Figure 3-48 shows the configuration of the transmit stream.



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

Creating an AUX or GPIO data stream follows the same principle 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.

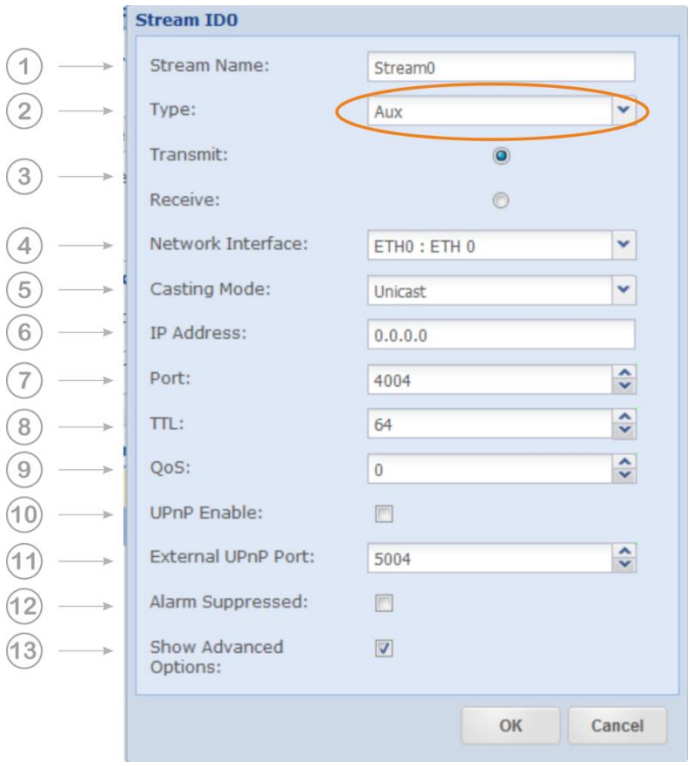


Figure 3-49 shows the configuration options for AUX or Opto/Relay streams

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 remote receiver's unique IP address, the network gateway, or a hostname. Using a Hostname requires an active Dynamic DNS service (refer to section 3.5.7.2). For multicast: Enter the multicast group address. The multicast group address must be entered if Multicast is selected for the Rx stream.
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. Therefore, each stream must use a different port number. Port numbers for AUX data streams are even numbers in the 4000 range (4004/4006/4008 …).
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 gets 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 only allows the QoS tagging of the packets. The range of the DSCP value is 0 (off) to 63 (highest priority). It is essential to know about the QoS implementation of the network before entering a value – the network router may not accept all values.
10. **UpnP Enable**:
    The "Universal Plug and Play" check box enables the IGD "Internet Gateway Device" feature for this stream. It is used to control the router's port management if the router allows it.
11. **External UpnP Port**:
    If UPnP is enabled, on default, the internal port equals the external port. Therefore, it 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.

AUX Data or GPIO Stream Configuration *(continued)*

12. **Alarms Suppressed**: Enabling this check box suppresses all alarms generated by this particular stream. Sometimes it is good to suppress alarms on a stream that do not apply to the given situation.
13. **Show Advanced Options**:
    Allows changing from "Basic Options" to "Advanced Options." This tick box expands the configuration window.

3.4.14.1 About Packet Size of AUX Data and GPIO Streams

The unit sets the packet size for AUX data streams automatically – 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 sends 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:

3.4.15 Audio Stream Forwarding

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

3.4.15.1 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.

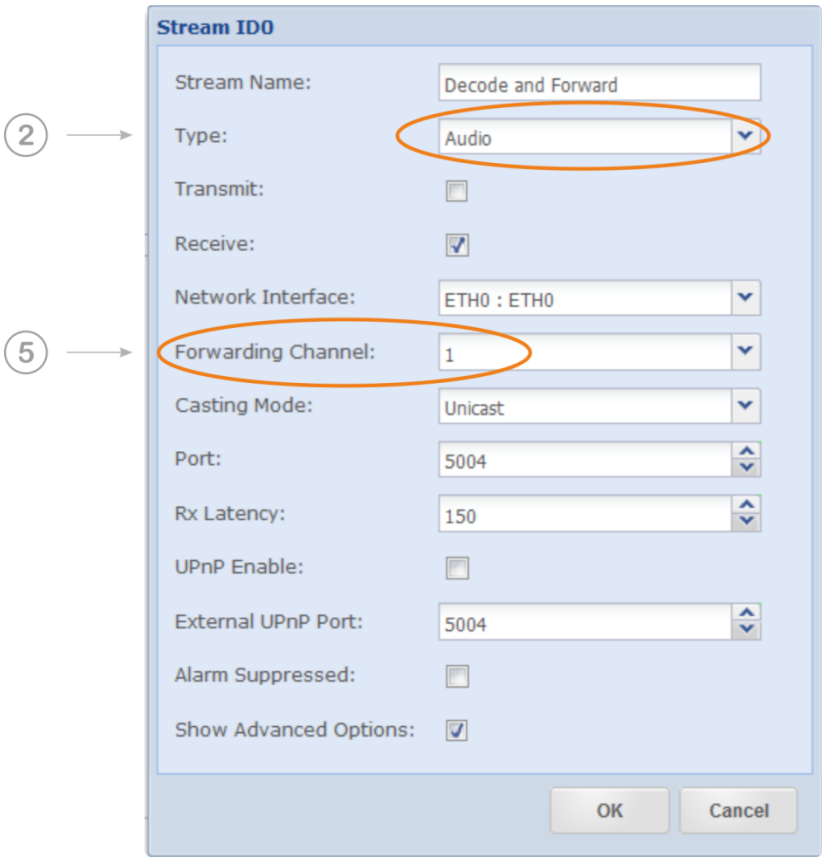


Figure 3-50 shows the configuration options for local Decode and Forward

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

(2) Select the Stream Type: "Audio (RTP)" for receiving the desired audio stream. All other values must be set for receiving an audio stream (refer to section 3.4.11)

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

ⓘ *By selecting a forwarding channel number, you make the stream available in this channel for the transmitting path.*

3.4.15.2 Forwarding an Audio Stream (Tx)

To forward an audio stream implies receiving and making it available in a forwarding channel first (refer to section 3.4.15.1). Audio streams consist of RTP/UDP packets; therefore, Media Forwarding must be chosen to forward the audio in RTP packets.

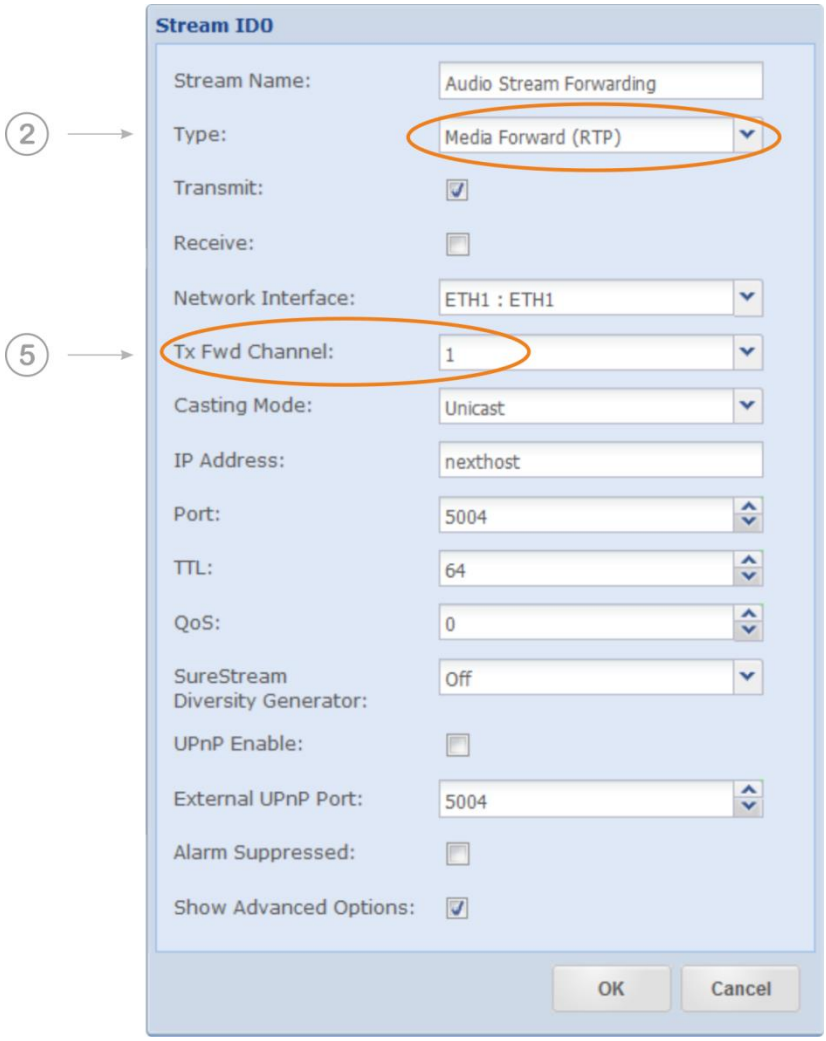


Figure 3-51 shows the configuration options for IP Forwarding

This configuration is the same 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 3.4.11).

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

ⓘ *The data source for Stream Forwarding (RTP and UDP) is the content in the selected forwarding channel! The example above reads from channel 1 and forwards the IP stream (RTP).*

⚠ The Media Forward (RTP) option allows the configuration of bi-directional streams – this configuration 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 3-50 (Rx) and Figure 3-51 (Tx). Codec A receives an audio stream from the network, decodes it and makes it available for Media Forward to any other remote site.

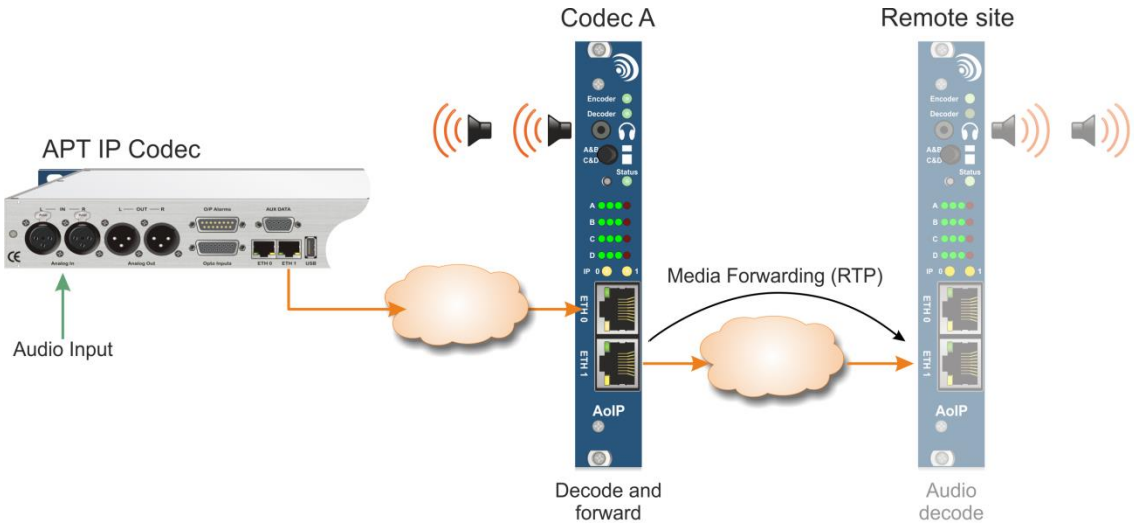


Figure 3-52 shows the application of Media Forwarding (RTP)

Stream Forwarding in Duplex Mode

You can configure the forwarding streams also in duplex mode. In duplex mode, the configuration window provides the Rx Forwarding Channel and the Tx Forwarding Channel.

3.4.16 IP Stream Forwarding (UDP)

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

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

A 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.

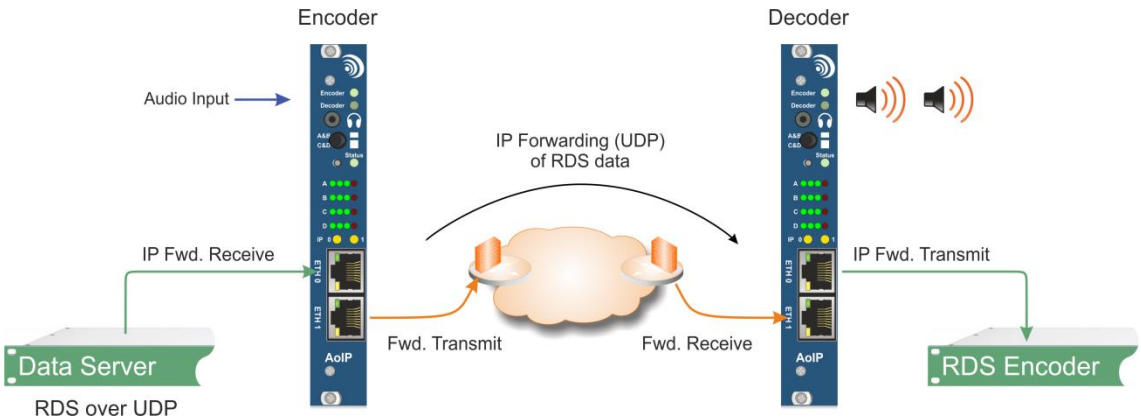


Figure 3-53 shows a typical application for non-audio data forwarding

3.4.17 Combination of UDP/RTP Forwarding

The principle of UDP/RTP re-encapsulation is described in section 3.4.10.2.

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

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

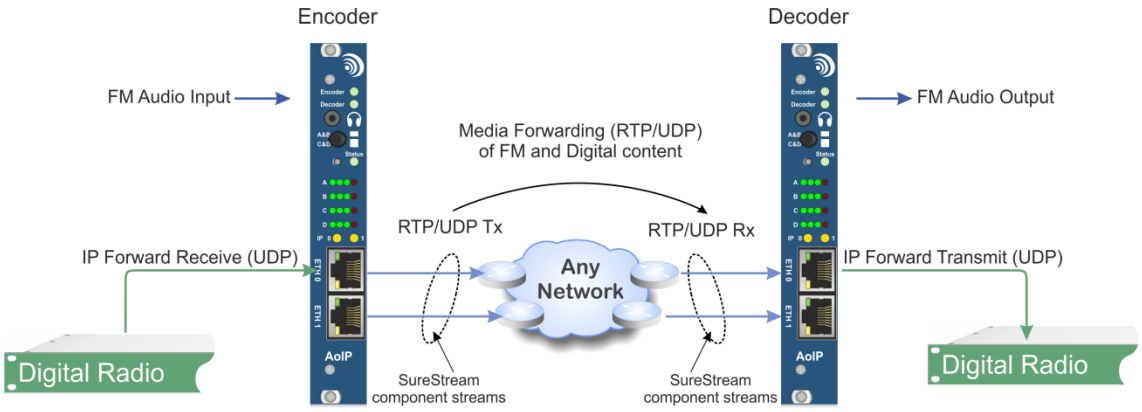


Figure 3-54 This example shows the FM Audio Input and the Digital Radio data streams protected by SureStream

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.

3.4.18 Advanced Stream Configuration

You can reach the "Advanced" configuration page directly from the Connection Page, from a shortcut on the Status Page (refer to Figure 3-6 "Configuration Shortcuts") – bypassing the profile wizard – or after the Configuration Wizard procedure has been completed. This page presents all configuration parameters of the IP streams.

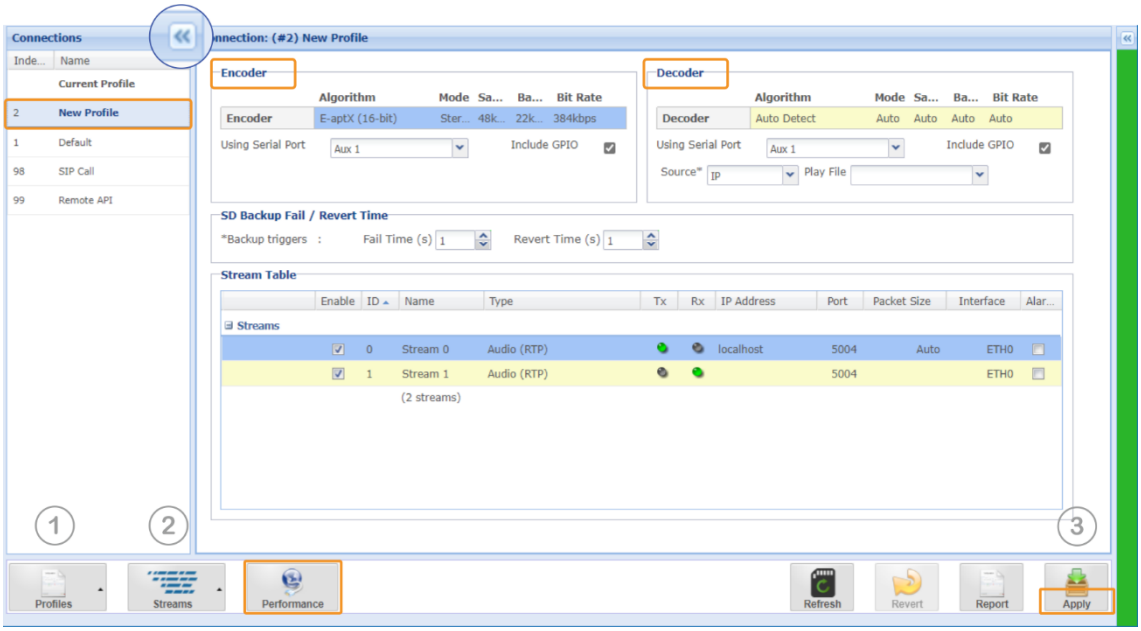


Figure 3-55 shows the Advanced configuration window

The Connection Wizard, described in section 3.4.1 and following, 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, modifying an existing one, or deleting profiles from the list. It also allows changing the currently applied (and active) configuration.

Profile Templates

Some profiles are used as templates for dynamically configured profiles. These are managed by the codec and cannot be edited. Currently, there are two templates: "98 SIP Call" and "99 Remote API".

Current Profile

"Current Profile" shows the currently active profile name. In the example of Figure 3-55, 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 "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 the "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 on the toolbar ("save" appears if any profile was edited but not the "Current Profile"). This action does not affect the actual running configuration. The modified profile is now stored and can be applied to the hardware by clicking on the Apply button (3).

Creating and Deleting a new Profile

Clicking 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. Editing any profile while a "Current Profile" is applied 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 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 interrupts the IP transport.

Access the Performance Page

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

3.4.18.1 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.

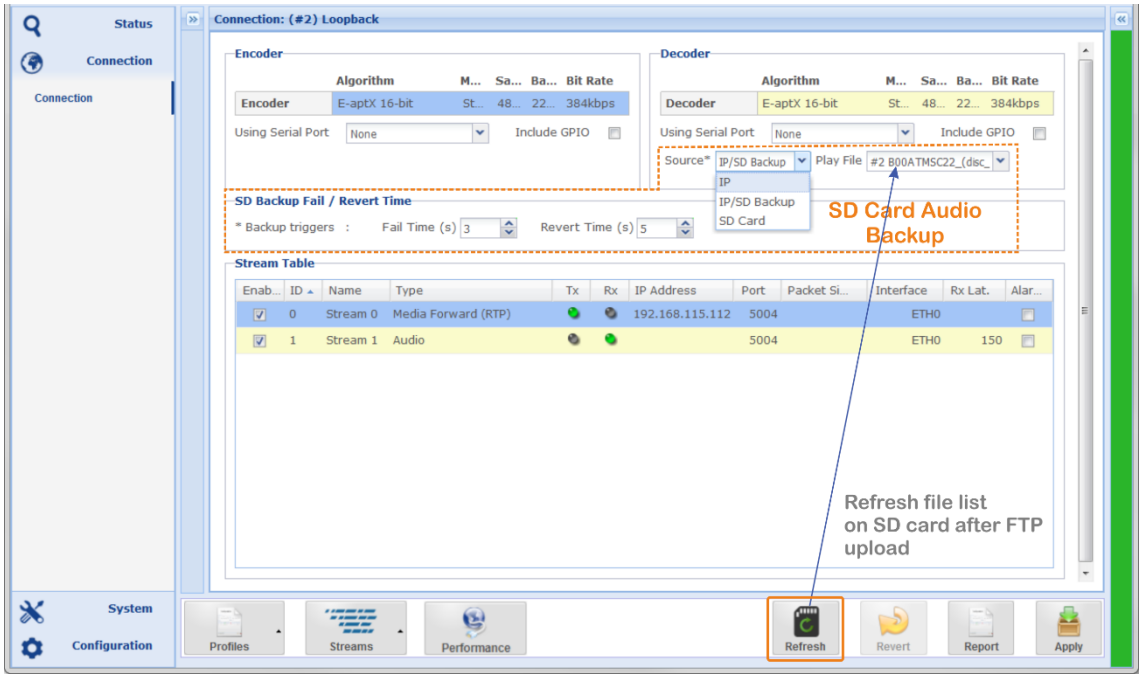


Figure 3-56 shows the configuration of the SD Card audio backup

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 until a network error occurs. The network error is "Loss of Connection, " meaning that the de-jitter buffer has run empty. In this event, the Decoder starts playing from the selected SD card file according to 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 plays one audio file from the SD card. You must select the file used for your backup as described earlier. You can store several files on the card, but only the selected file is 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 SD card size only constrains the duration of the program file.

Fail Time / Revert Time

The "Loss of IP connection" event triggers the backup function. The "Fail Time" defines the period in which the error must have occurred before the backup plays the file. The "Revert Time" defines the period in which the error must be corrected before the decoder returns to decoding 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 ensure the SD card is mounted correctly (refer to section 3.5.13.1).
- You can upload the files directly to the inserted SD card via an FTP connection. 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 uploading new files via FTP. However, clicking on the "SD Card Refresh" button in the toolbar of the page updates the file list (refer toFigure 3-56).*

SD Card Type and Format

The card type should be SDHC for audio files playback. There is no limit on the 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 audio format of the SD card; 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 when decoding an IP stream. Therefore, creating the audio file with the same digital level is essential 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 errors.

Audio Backup – Timing

⚠ You may perform some tests 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, ensure that the detection periods are not too short.

Notes:

3.4.18.2 Simplex Mode – IP Stream Configuration

Creating an IP stream in simplex mode follows the same procedure as duplex mode. Each of the two stereo signals generates its stereo IP stream in simplex mode. The two stereo programs keep fully separated on different IP flows. The image below shows the stream configuration options from the Encoder mode (dual stereo Input).

ⓘ *Note: The System Menu must enable simplex mode (operational mode of hardware). Refer to section 3.5.15 for more information! A simplex mode is also indicated by the front panel LEDs (Encoder or Decoder).*

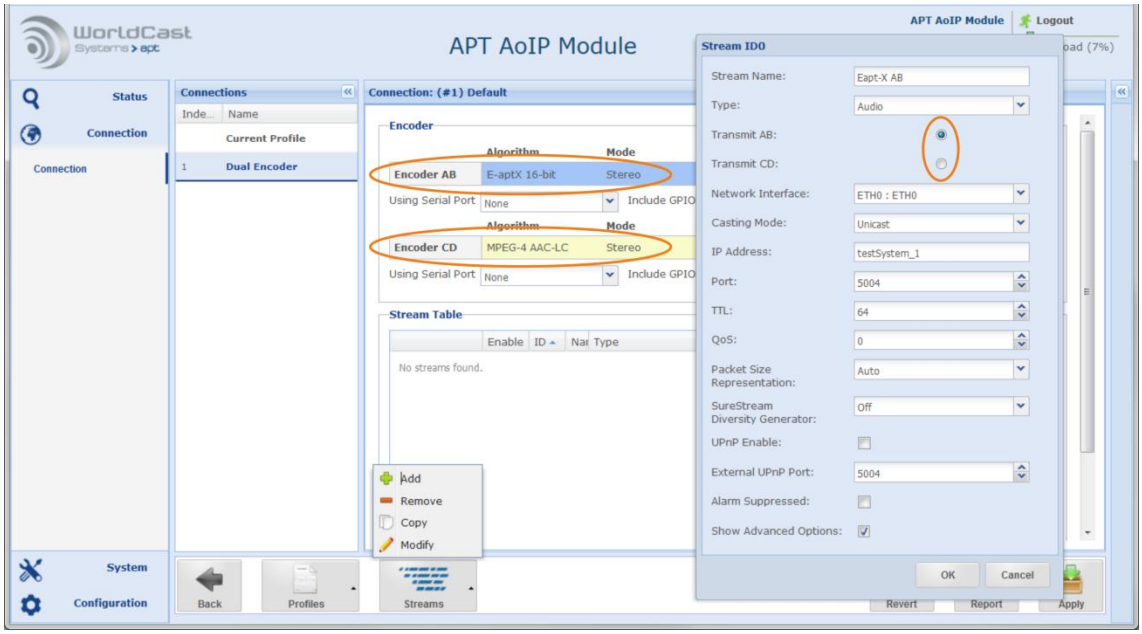


Figure 3-57 shows the IP stream configuration options in simplex (dual Encoder) mode.

The AoIP card also allows an asymmetrical audio configuration in simplex mode. The example above highlights the different audio algorithms for input A/B and C/D. One stereo stream is configured for aptX© Enhanced for high quality and low delay transmission, while the second Encoder C/D is set up for a low bitrate stream with MPEG-4 AAC-LC.

ⓘ *Note: The signal domain selection (analog or digital) on the audio configuration page affects both stereo signals in the same way; the signal domain of A/B cannot be set differently from C/D and vice versa.*

3.4.18.3 Configuration Validation

The Validation Engine (Valex) protects users against incorrect inputs and obvious configuration mistakes. In addition, it validates IP stream configurations made on the local unit regarding consistency and correctness.

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

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

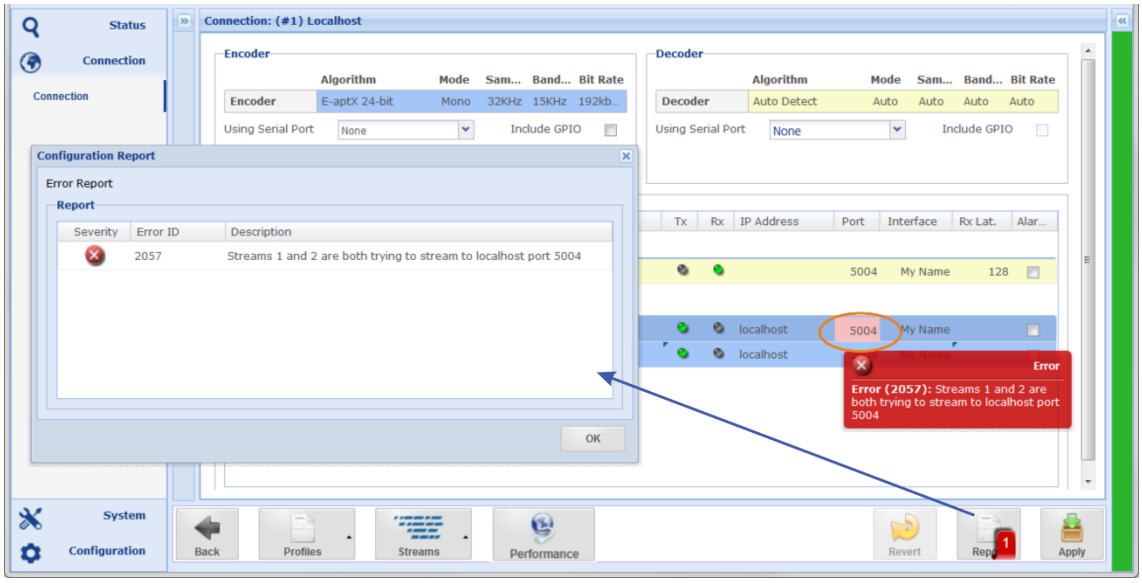


Figure 3-58 demonstrates how the Validation Engine presents error conditions and warnings

The invalid configuration in this example is the assignment Tx 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.

Validation Engine *(continued)*

The image below shows another example of how the validation engine warns on particular configurations.

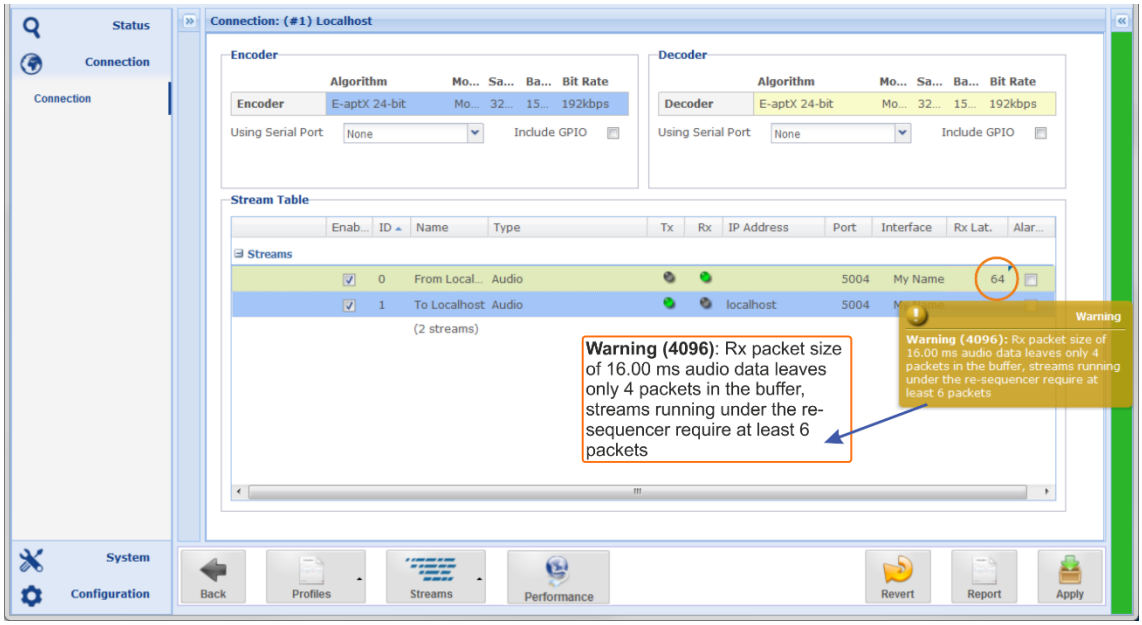


Figure 3-59 shows a yellow warning from the Validation Engine

The Validation Engine has identified a problem within this profile. In this example, the de-jitter buffer is set to 64 milliseconds. However, 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. Therefore, either the buffer size must be set to 96 ms (6x 16 ms = 96 ms), or the re-sequencer cannot unfold the whole performance (which is an accepted condition).

This is a "Yellow" warning and not a critical alarm. The validation report does not automatically pop up, but the warning is visible with a mouse over the highlighted fields.

ⓘ *Due to the nature of the Validation Engine, it cannot foresee a misconfiguration, especially on an Rx stream before the configuration was applied and becomes active. Therefore, in the example above, the Valex Engine must first receive packets before calculating the required buffer size.*

3.4.19 Digital MPX over IP

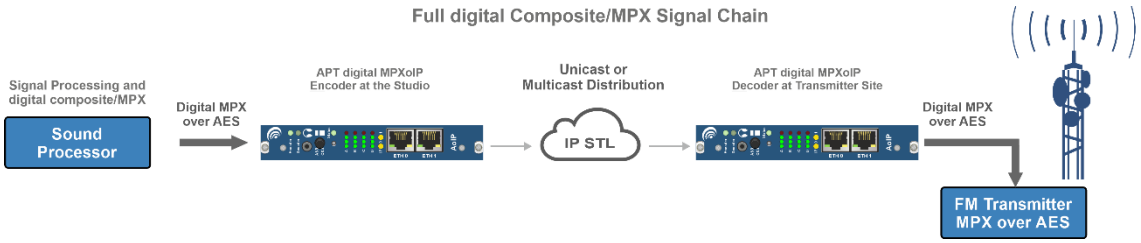


Figure 3-60: Shows the digital composite/MPX transmission path

Applying the Digital composite/MPX license or applying to your Codec adds three MPX transmission modes to the Audio Algorithms list. The Codec receives the digital MPX signal at the AES input and outputs it at the receiver as an AES3 signal with a sampling rate of 192 kHz. You can see the typical fully digital signal path in the figure above.

3.4.19.1 APTmpX (low-bitrate MPX)

APTmpX reduces the data rate of the MPX spectrum and allows it to be transmitted at bit rates equivalent to compressed audio signals. Four modes are available and can be chosen depending on the application and the network capability.

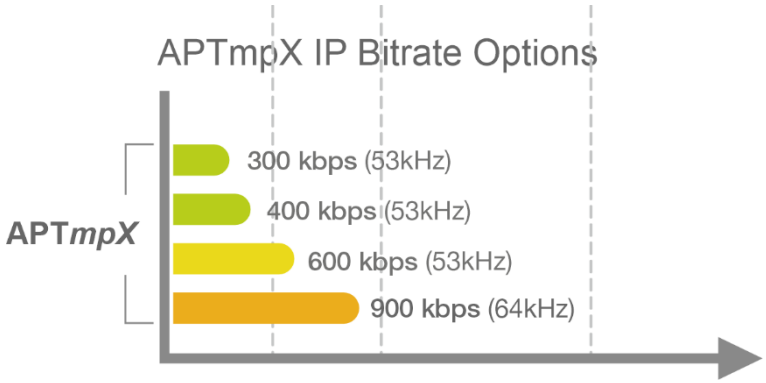


Figure 3-61: Shows the bandwidth options and the resulting MPX spectrum band of APTmpX

3.4.19.2 Linear MPX Modes 16/24Bit

The linear MPX transmission modes apply 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 quantization can be done either with 16 Bit or 24 Bit. The effects on the required bit rate in the IP network are shown below.

Linear MPX Bandwidth and Modes

The Sample Frequency and the resolution of the MPX signal affect the required bit rate in the IP network. The following diagram shows the options for linear (non-compressed) transmissions.

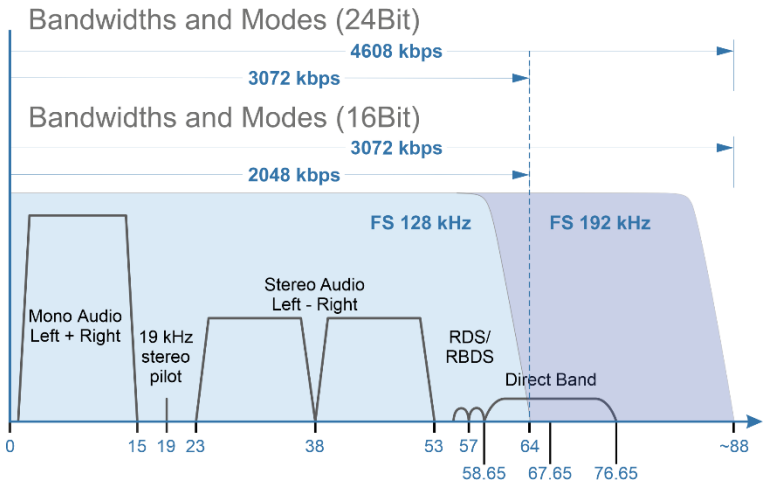


Figure 3-62: Shows the reduced bandwidth requirement of the APTmpX in the IP network

3.4.20 MPX Mode Selection

The stream configuration for digital MPX follows the same procedure of generating an IP audio stream (refer to section 3.4.11). First, the Algorithm drop-down list shows the MPX options. Next, select a format and set the other options. Except for APTmpX900, the formats offer other settings, like sample and data rates.

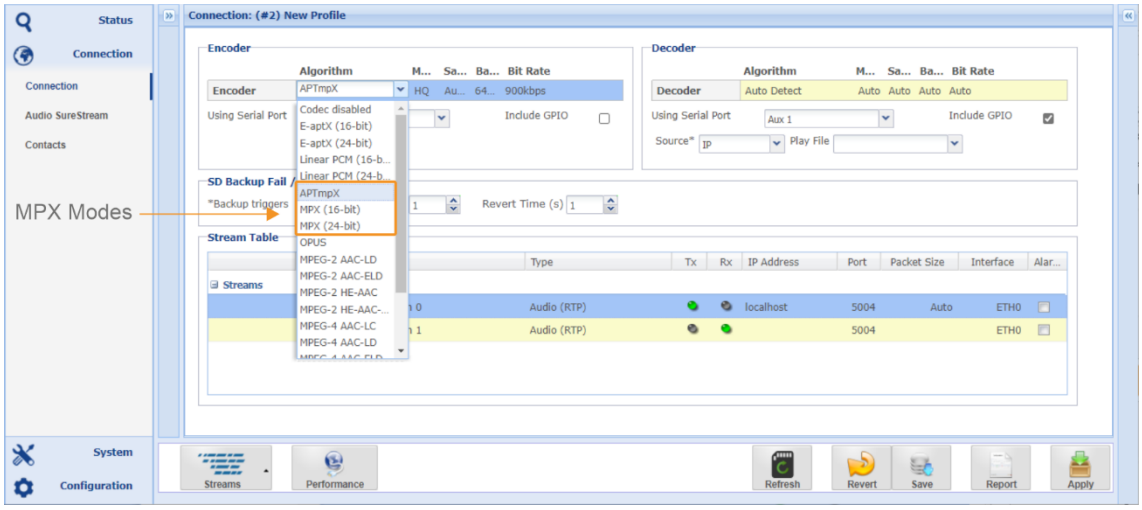


Figure 3-63 shows the audio algorithm selection with the MPX options

3.4.21 MPX Modes and Configuration

Input Format

The AES/EBU interface is the Input of the digital MPX signal. Set the Input Mode in the configuration menu to "Digital" (refer to section 3.6.1). The input sample rate converter detects the sampling rate automatically.

Output Format

The AES/EBU interface is the Output of the digital MPX signal. The AES/EBU output provides the digital MPX signal at a sampling rate of 192kHz regardless of the selected MPX mode (linear or compressed).

➡ Set Digital Output Fso to 192kHz in the Configuration menu (refer to section 3.6.1).

APTmpX – Options

➡ Select APTmpX from the list of formats.

Another dropdown list shows (truncated) the two options for

1. APTmpX (Audio only) and
2. APTmpX (Audio & RDS)

If you select "APTmpX Audio only," a third list opens with the options for the bitrates.

If you select "APTmpX Audio & RDS," the bitrate is set to 900kbps.

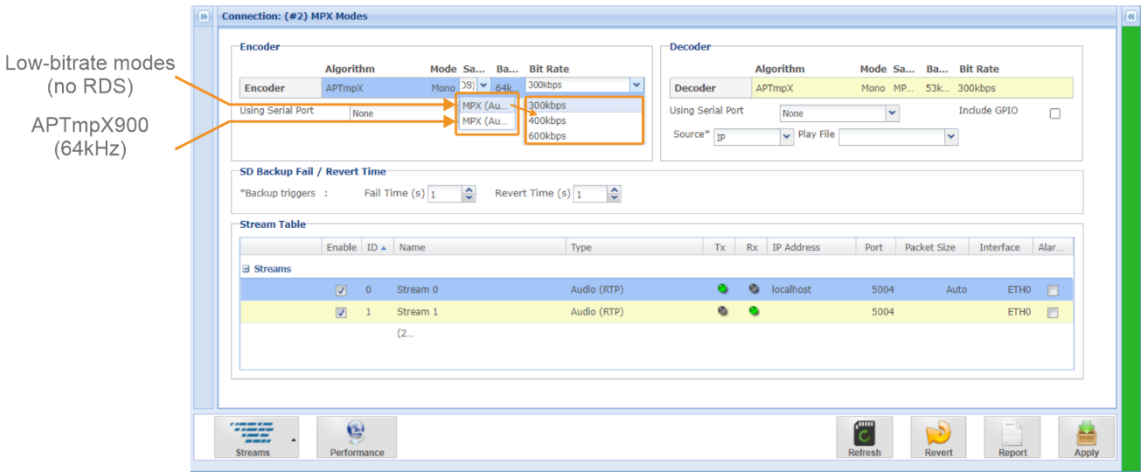


Figure 3-64 shows the audio APTmpX mode selection with the bitrate options for "Audio only"

3.5 Main Menu – System

3.5.1 Date and Time

The AoIP Codec Module 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**, which all timing-related actions refer to, is derived from this UTC timing reference considering the Time Zone shift.

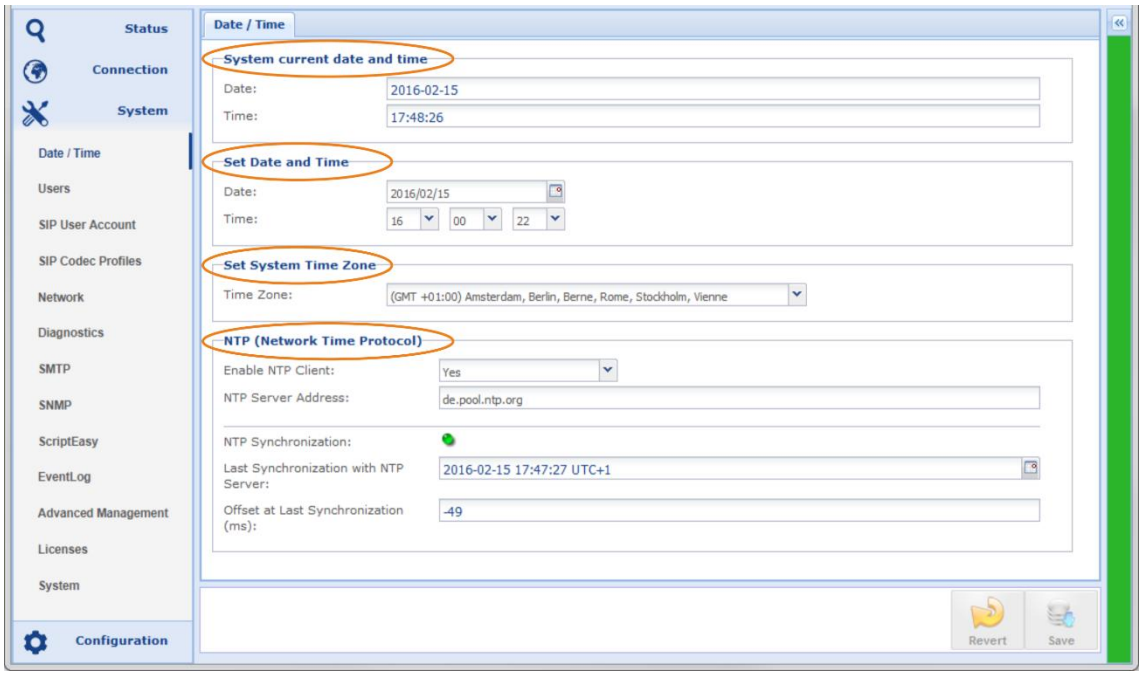


Figure 3-65 shows the system page for date and time configurations

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.

Change date and time here to change the unit System Time manually. You must change a value and click "Save" in the toolbar to take the new values.

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

Ensure the NTP client is disabled if you want to set the system time manually!

Set Local 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) and entering the NTP server IP addresses or Server hostnames. You can enter more than one server name or address here, separated by a comma but without spaces:

"time.google.com,time2.google.com,time3.google.com".

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 continuously while the external server is polled periodically. The poll interval is randomly adjusted and increases after a time to a maximum of 1024 seconds.

ⓘ *The diagnostics page has a monitor tool to assess the state of the NTP server connections.*

It adjusts the system clock to stay in sync with the NTP reference. If 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! To resynchronize, you must disable the NTP client (save) and re-enable it (save).

3.5.2.1 NTP Synchronization Alarm

The NTP alarm is activated if a server becomes unreachable for some time from the current poll interval.

The last synchronization with the NTP server is displayed, and the corrected time is 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 using the default gateway as standard.

It is essential 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 reference 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 the orphan mode for correct operation, e.g., a server using *ntpd* should add "tos orphan 6" to the ntp.conf. configuration file.

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.

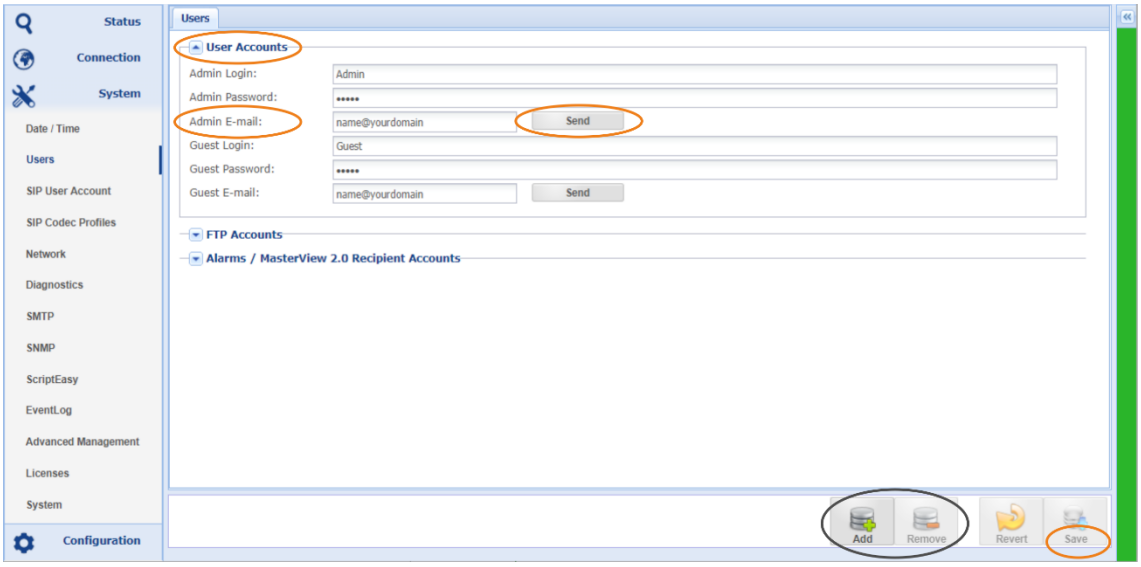


Figure 3-66 shows the user page with account managers

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 following admin user in the LogIn queue.

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

User Account E-Mail Address

The user accounts allow the entry of an email address for each user. The alarms system uses this email address 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 3.5.9).

ⓘ *All changes on this page must be saved before they become active. For example, 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 communication with external applications.

All FTP accounts work on both ETH ports. The firewall allows filtering of the FTP service on each ETH port; it is recommended to enable the filter if not used (section 3.5.7.9).

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. However, care must be taken not to compromise the audio streams by overloading the link capacity. Therefore, you must configure your external FTP client to manage the maximal up- and download speed accordingly.

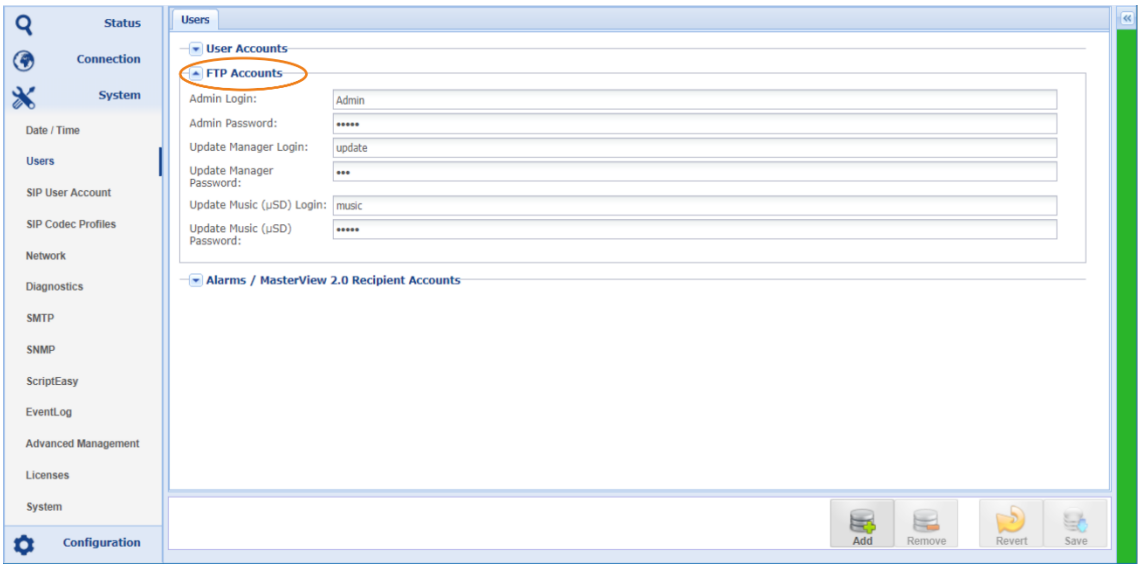


Figure 3-67 shows the user page with the FTP account manager

⚠ 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. However, the FTP account is no longer used once the script is uploaded. Instead, ScriptEasy uses a dedicated and hidden FTP account, invisible to the user (no management access).

FTP Admin LogIn

Currently, there is no specific application accessing the unit by this account. However, you should change the default LogIn to a more robust password if you cannot filter the FTP service entirely on the firewall page.

⚠ The APT Network Management Software (NMS) utilizes FTP for centralized firmware uploads. If the NMS is used, ensure the FTP account is enabled on the firewall (see firewall settings in the network configuration section 3.5.7.9).

FTP Update Manager

Currently not in use

FTP Update Music LogIn (SD Card)

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

You can assign your username and password.

Default LogIn, User: Music – Password: music

3.5.3.3 Alarms / MasterView 2.0 Recipients Accounts

This section creates 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.

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 sending it to that user: critical, major, minor, warning, all or none.

Guest:

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

Notes:

3.5.4 SIP User Accounts

Creating a SIP account is the first step of the SIP setup. There are two types of SIP accounts, several of which you can create.

The Peer-to-Peer Mode

The peer mode is the simplest way to directly connect two SIP clients without utilizing a SIP infrastructure (no switching). In this case, the codec's current (possibly dynamic) IP address must be known and accessible. The disadvantage is that connections in public networks must constantly be reconfigured due to the changing IP addresses. Therefore, the current SIP URL is only temporary.

SIP Server Registration

The SIP Server mode requires creating an account on the SIP Server of the SIP Infrastructure. The account details are assigned to you by a SIP provider or your IT department.

The significant advantage of a SIP infrastructure is its ability to assign the temporary IP address of your codec to a fixed unique SIP address (SIP URL) so that your codec can always be reached globally with the same URL.

3.5.4.1 SIP Server Account Configuration

This page contains all options to set up a SIP User Account on the SIP Registration Server and, in the lower part, further options concerning the SIP Session Description. As described in the later chapter, only a few of these options are required for a peer mode account.

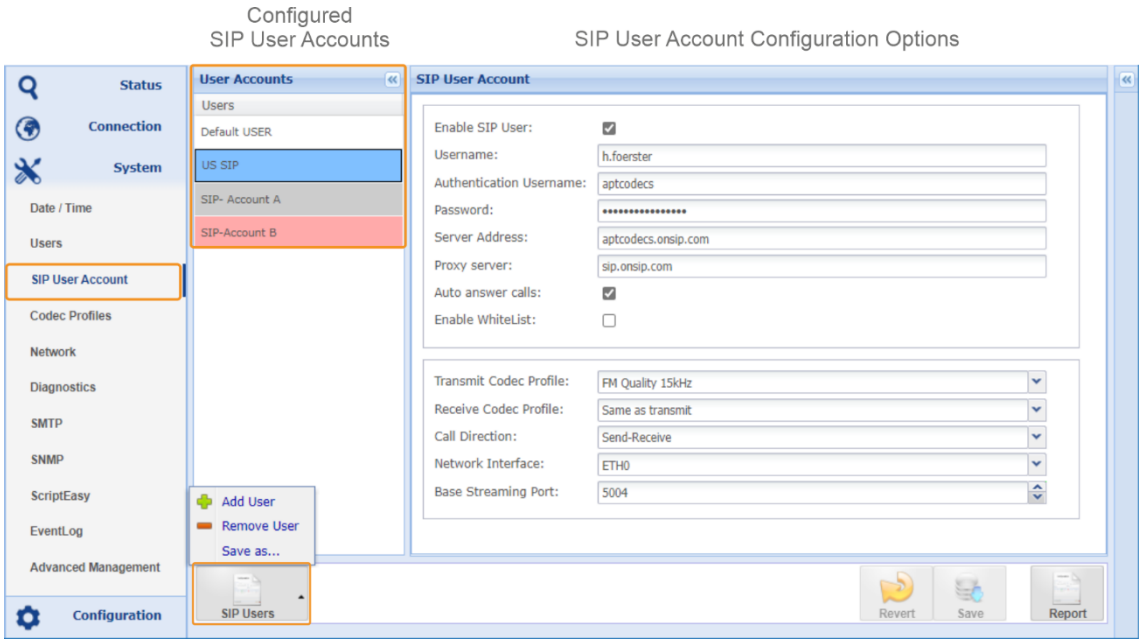


Figure 3-68: Shows a fully configured SIP Server account.

User Accounts Column

This column lists all already created user accounts. The colors indicate the following:

- **Grey**: this means this is a Peer-Mode Account.
- **Blue** means this is a SIP server account that has been successfully registered.
- **Red**: means this is a SIP server account that could not connect to the server
- **Green**: means, on this account is an active call

At the bottom left, are the options to manage these entries. Here you can add, copy and delete additional accounts.

Configuration Options

Enable SIP User

This tick box activates the account. Only if an account is activated, it can be used for SIP connections in the SIP Dialer. A deactivated account is not registered on the SIP server.

Username

The username is the SIP username assigned to you by the SIP provider.

⚠ Important: the username must not contain spaces!
Currently, this input field allows entering blanks.

Authentication Username

This name is another instance to verify the user to this account. Auth. Usernames can but do not necessarily have to be given; it depends on the SIP provider.

Password

This is the password to your username; assigned by the SIP provider.

Server Address

The server address of the SIP registration server.

Proxy Server

A proxy server is a routing server of the SIP provider. You can enter the server address here separately if your Sip account expects it. However, some providers combine SIP registration and proxy servers. In such a case, nothing is to enter here.

Auto Answer Calls

If you activate this box, all SIP calls are answered automatically. If it is deactivated, you must answer a call manually.

Enable Whitelist

The whitelist is the list of registered contacts. If this option is enabled, all calls whose address is not in the contact directory are rejected.

Transmit Codec Profile

The dropdown list shows all connection profiles that you have created. There are three predefined profiles: FM Quality, High Quality, and Voice. The profile selected here is the default profile used by this account when dialing the remote codec.

Receive Codec Profile

Here a profile can be selected, which requests this SIP User Account from the called codec as the default response. There is also the option: "Same as Transmit."

Note: "Same as Transmit" is the currently recommended setting. This mode is NAT traversal, i.e., there is no need to configure ports on gateway routers. However, when a firewall performs port translations, the symmetric protocol may not be able to pass through either, in which case the firewall needs to be configured.

You can find further important information about codec profiles in the chapter "Codec Profiles".

Call Direction

This dropdown list determines the default setting of the call direction. Options are Send-Receive (bi-directional), Send-Only, and Receive-Only.

Network Interface

This is the determination of the network interface over which all SIP communication takes place. This is the only instance where this setting can be made to SIP and affects both registration and audio streaming.

Base Streaming Port

This is the destination port for the audio stream at the remote address. This port setting has the same meaning as the destination port setting in the RTP Streams Table.

3.5.4.2 Peer-Mode Account Configurations

Username

The username can be freely defined in peer-to-peer mode, e.g., MyCodec_25.

Important: the username must not contain spaces!
Currently, this input field allows entering blanks.

Server Address

The server address is the current IP address of the codec. This address is determined by "localhost." If the IP address of the network interface used for SIP communication changes, the address of the peer mode account changes accordingly.

3.5.5 Codec Profiles

Introduction

The codec profiles described here are used for **Audio SureStream** connections and the **SIP connections**. Note the codec entries in the profile in Figure 3-68. The first entry is an RTP/SIP entry; each further entry is a SIP-only entry.

Unlike SIP, SureStream Audio cannot negotiate, so only the first entry in the profile can be used for this (RTP) connection. Take this into account when prioritizing the codecs in the profile!

For SIP, the Session Description (SDP) information is generated from the SIP Codec Profiles. This information is transmitted from the calling codec to the remote device during the session setup. Then, the remote device tries to respond in the same format to the sender's request.

This communication aims to negotiate a transmission format within the framework of the possibilities defined by the **caller profile**. It is irrelevant whether a profile of the same name is defined in the receiving codec. If the required audio algorithm and the mode (bit rate, mono or stereo) are supported by the called codec, the response is according to the request. The profiles only serve for categorization by the user. A caller profile can also request multiple formats alternatively. In this case, several algorithms are defined in the same profile. Negotiation begins with the first entry in the list.

ⓘ *Whether a Codec profile is used for a symmetrical or asymmetrical SIP connection is determined by the CALLER mode and not by a specific profile itself. Refer to chapter 3.3.4.1.*

Symmetrical use of Codec Profiles

As described above, the use of a profile is determined by the caller mode. The "Call With" mode with your profile selected in the dialer always leads to a symmetrical connection. The same can be achieved if the current SIP User Account is configured to "Receive the same as Transmit" (chapter 3.5.4.1 /9). In this case, the caller requests the same mode for reception in the direct dialer mode "Call."

Symmetrical connections are the recommended use of the profiles in unknown, public SIP infrastructures since no individual UDP port assignments are required at the gateway routers. However, this consideration is irrelevant in Peer-to-Peer mode as no foreign gateway has to be passed.

Asymmetric use of Codec Profiles

To force asymmetrical use of codec profiles, you must use the direct caller mode "Dial" (chapter 3.3.4.1), and the current SIP User Account must specify different profiles with different codecs for sending and receiving (see also chapter 3.5.4.1).

ⓘ *Asymmetrical use of SIP codec profiles is only recommended in your known network, where no port translation takes place, and the ports specified in the codecs are used.*

Default Profiles

Three Codec profiles are predefined, which can be edited but not deleted. Renaming is possible with the copy function "Save as."

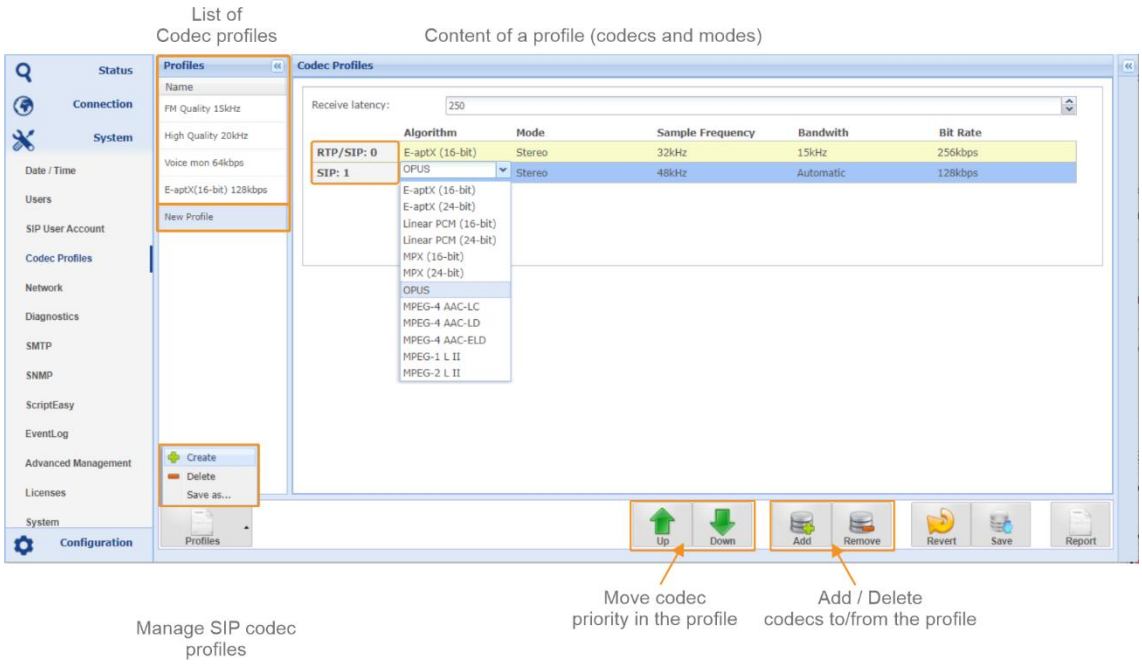


Figure 3-69: Shows the SIP Codec profile page with various options offered

Default Codec Profiles

- FM Quality 15 kHz (E-aptX, 16 Bit, 256 kbps)
- High Quality 22 kHz (E-aptX, 24 Bit 256 kbps)
- Voice mono 64 kbps (MPEG-4 AAC-LD)

3.5.6 Manage Codec Profiles

SIP Codec profiles are managed centrally via one page. This page is located in the System Menu. The profiles you have created are then available in the SIP Dialer, or you can define them as default profiles in the SIP User Account.

On the left side, you find the list of created profiles. The first three are the default profiles that you can customize. The fourth profile (currently selected) is the individual ("New Profile"). Finally, on the right side, you can see the codec configurations of the selected profile, which are similar to the representation in the RTP Streams Table.

Differences in the RTP-direct Mode

1. A selection of the audio algorithms available in the device is supported by SIP. Therefore, the MPEG 2/4 HE-AAC and the MPEG 2 AAC family do not appear in the list of codecs.
2. The assignment of the physical network interface is done in SIP Account Management and is defined there for all profiles used by the SIP User account.
3. For the UDP port assignment of a SIP codec profile, the same applies as for the physical ETH port; this is defined in the SIP User account.

3.5.6.1 Creation of a Codec Profile

In the toolbar on the left are the options: "Create," "Delete," and "Save as." Click "Create" to create a new profile, or select an existing one and save it with "Save as" under a new name.

Select the new profile with the mouse and edit the codec details. Finish the action by saving the changes by clicking on "Save" (right in the toolbar).

3.5.6.2 Multi Algorithm Codec Profiles

One profile can contain one codec configuration or several. If you want a profile to offer multiple formats, click "Add" to add more codec formats to this profile.

Negotiating the formats is always done from the first entry in the list. The top entry in the list has the highest priority. If the called codec does not support this format, then the caller offers the profile in the following line of the list and so on.

You can change the coded formats' priorities by activating the profile entry with the mouse and moving it up or down with the green arrows in the toolbar.

Finally, save these changes.

ⓘ *You can define up to **five** codec formats in one profile.*

⚠ Only the first entry in the list can be used for Audio SureStream Connections (RTP)

3.5.6.3 Embedded Aux Data in Codec Profiles

You can transmit the Aux **and** GPIO data embedded in the Enhanced aptX algorithm. For this algorithm, the data channels are opened by default. These do not have to be activated separately.

ⓘ *Note: Aux data and GPIO transfer is currently only supported for Enhanced aptX.*

3.5.7 Network Configurations

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

3.5.7.1 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.

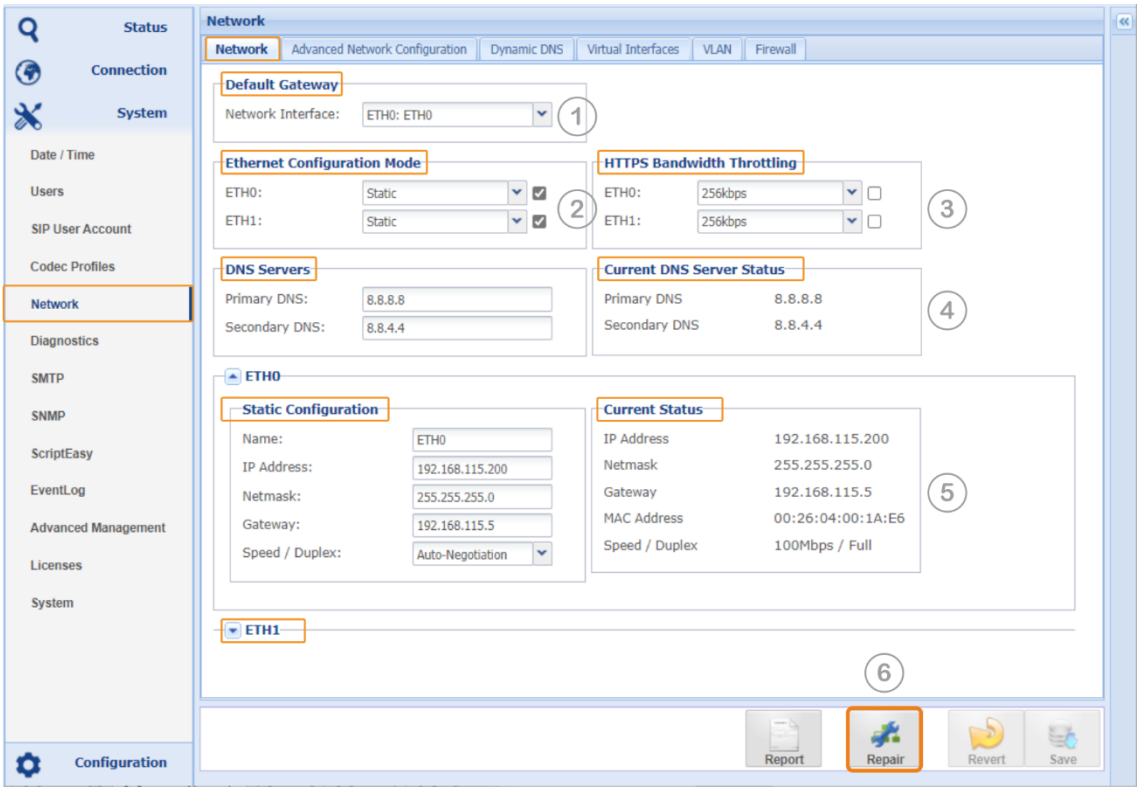


Figure 3-70 shows the options on the Network configuration page

(1) Default Gateway

This setting specifies that all data that cannot be configured as an audio or data stream should use the gateway of the physical interface selected here. These are, e.g., the NTP daemon, SNMP traffic, email notifications, etc.

(2) Ethernet Configuration Modes

- Static Mode for manual IP address assignment
- DHCP Mode 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)*

(3) HTTPS Bandwidth Throttling

Bandwidth Throttling allows you to limit HTTP traffic over the network and can be set from 16 kbps to 1000 kbps. With this setting enabled, the GUI's disproportionate use of the network capacity can be avoided, especially on the first start. Furthermore, 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. Network – Network (continued)

(4) 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 were 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 (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.

(5) Current Status and Static Configuration for ETH0 and ETH1

This section shows both interfaces' "Current Status" on the right-hand side (the ETH1 section is collapsed by default). The "Static Configuration" entry fields 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
- Ethernet port speed and duplex modes (must be selected manually in any case)

Each ETH interface MUST be configured on a **separate** sub-network. Therefore, assigning more than one ETH interface to the same subnet is impossible!

(6) 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 external to the system (routers or others).

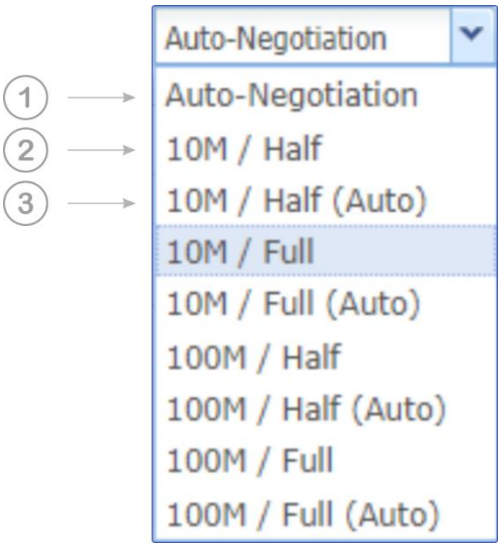
Network – Network *(continued)*

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 the same restricted negotiation mode.

The hard-coded inputs are not negotiated. The remote station (the switch) must be set similarly to establish a trouble-free connection.



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 the Interface advertises only this one value.

Note that the Restricted Auto Negotiation method is different from the hard-coded port speed setting. The corresponding ETH port must be set to the same method if supported or 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:

3.5.7.2 Advanced Network Configuration

Advanced Configuration provides UPnP settings for the management ports.

3.5.7.3 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 used in the Codec device.*

The UPnP section provides the controls for the management settings, as shown in the screenshot below.

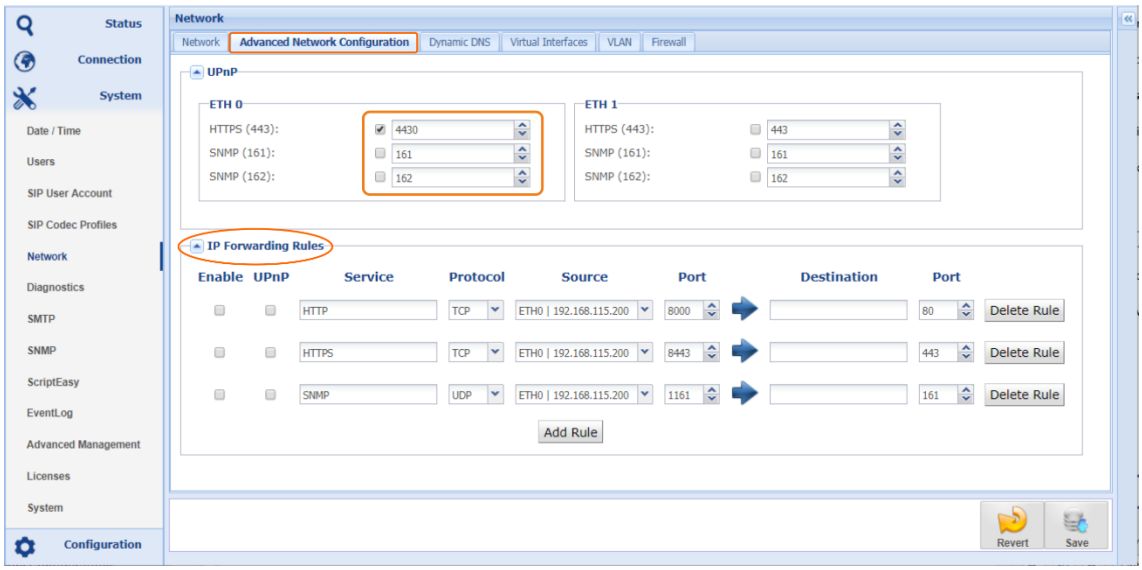


Figure 3-71 Shows the advanced network configuration page

This page allows specific port mapping of standard 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 this AoIP card identified by its MAC address (port forwarding rule in the router). Port mapping or port forwarding is possible on both ETH interfaces independently.

3.5.7.4 Advanced Forwarding Rules

The forwarding rules use the Layer 3 routing capability of the codec and allow the design of particular applications.

A typical application manages a device that is only connected to the codec and not directly to the network at a remote location. This can be an FM or DAB/HD radio transmitter, a sound processor, or others.

The rule shown here is configured on the local codec to which, e.g., a PC is connected, which should reach not only the remote codec but also the WEB GUI of another device that is not directly connected to the network.

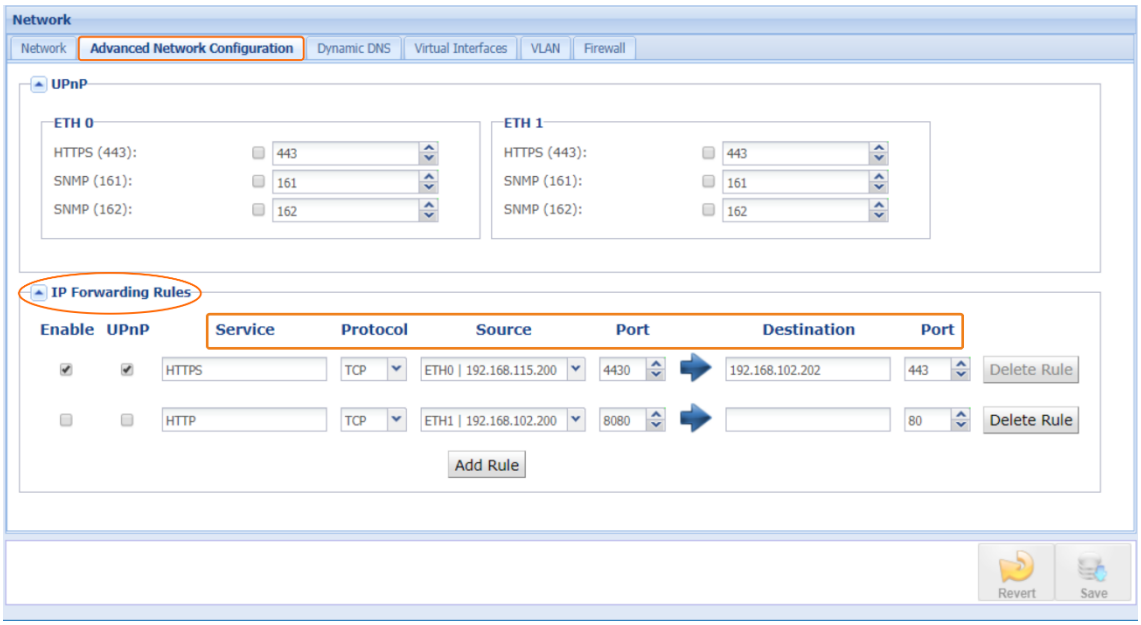


Figure 3-72: Describes the Advanced IP Forwarding Rules of a local codec

Service

Describes the required service that shall be forwarded from the local Codec to the remote device; any name is allowed.

Protocol

Determines the protocol that shall be forwarded; options are TCP and UDP.

Source

Defines the local Codec's ETH port from which this protocol is connected (e.g., the PC). The drop-down list offers ETH0 and ETH1 with their IP addresses.

(Source) Port

This port is the source port from the protocol that shall be forwarded. The example describes a rule allowing another device to reach the WEB GUI at the destination via HTTPS port 443. The port 443 (already assigned to the local AoIP codec module) must be replaced by an arbitrary port (e.g., 4430), which is again assigned at the destination to the standard port 443 of the destination address.

Destination

This is the destination address of the device to be managed that is connected to the remote codec. The device can be connected to any ETH port of the remote codec. However, the destination address must be in the same subnet as the selected ETH port of the remote codec.

(Destination) Port

The destination port in this example is the standard HTTPS port of the WEB GUI (443) and is determined by the device to be managed.

Enable

A rule can be configured but is inactive; "Enable" activates the rule.

UPnP

UPnP acts on the local router in this setting and configures a port forwarding rule to the destination port. Here, UPnP is only applicable if the public IP address of this router is addressed with the destination port extension from outside the local network. The router would then forward this port to the configured destination address (to the remote device).

Accessing the Remote Device

In this example configuration, the remote device would be addressed this way:

IP address on ETH0 of the local codec with port extension: **192.168.115.200:4430**

Notes:

_____

_____

_____

_____

_____

_____

3.5.7.5 Dynamic DNS

Dynamic DNS is a method that 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 AoIP card 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 AoIP card can be addressed, in a WAN environment, without using its allocated numeric IP address. Instead, each interface should be configured with a unique hostname that can be used instead of a numeric destination IP address for WAN-based audio streaming.

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

The screenshot 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. The stream finds this device automatically regardless of where the unit is (globally) connected.

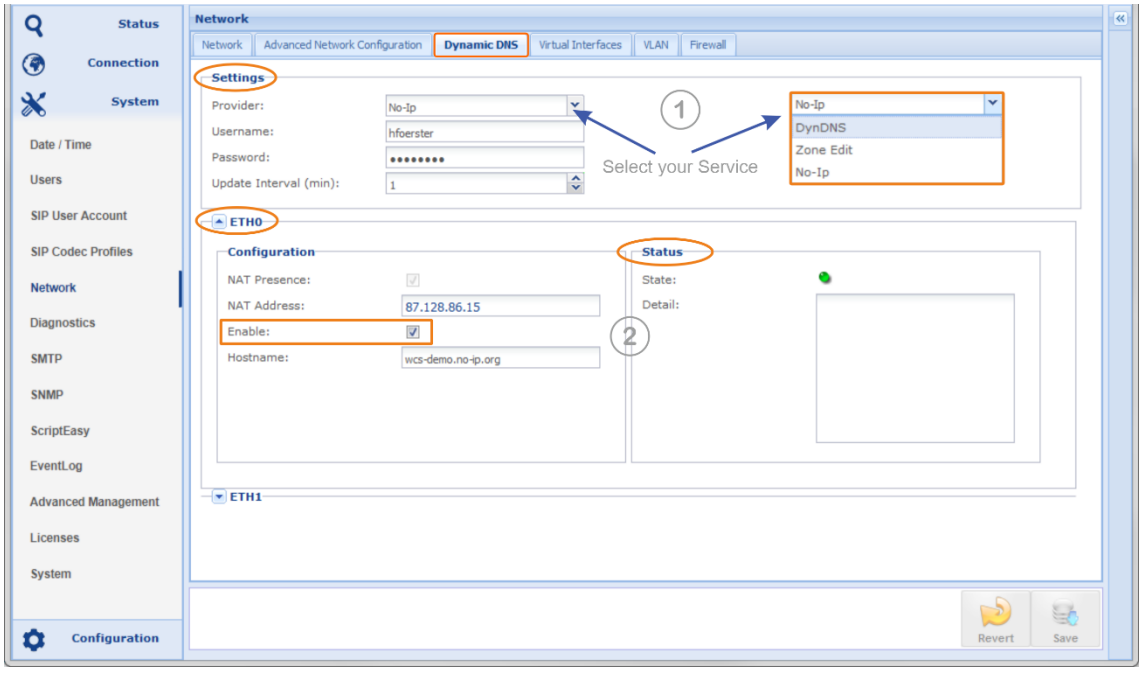


Figure 3-73 shows the Dynamic DNS client settings and status information

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.

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 an error message or another 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:

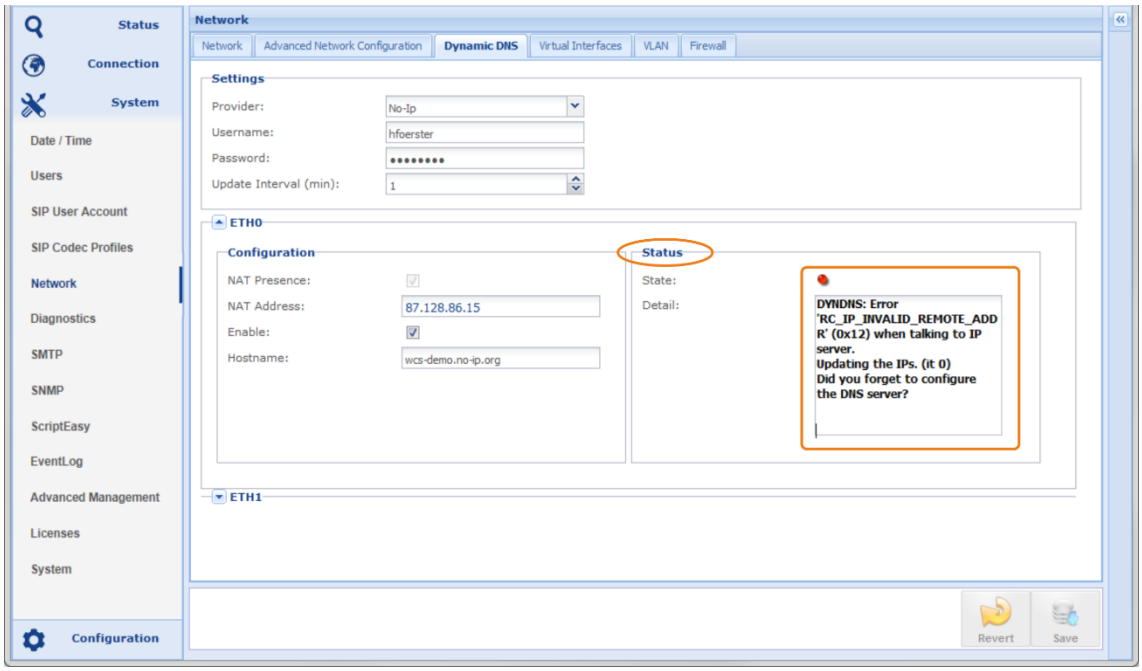


Figure 3-74 shows an error message of the DDNS status

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 indicate the current misconfiguration.

3.5.7.6 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 is to install Apple's implementation of Zeroconf for Windows (Bonjour Service). In the case that DHCP must be used to get a network access, the DNS lookup feature may help to identify the current IP address of the dynamically applied unit. With the DNS lookup you can access your unit 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 AoIP Codec Modules, the mDNS name is:

Wcs-SerialNumber.local – e.g., for an AoIP card with serial number N100109:

https://wcs-N100109.local

The serial number is available on a label on the solder side of the AoIP Codec Module. The "Local" domain is the standard domain of your PC.

3.5.7.7 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 without virtual LAN tagging.

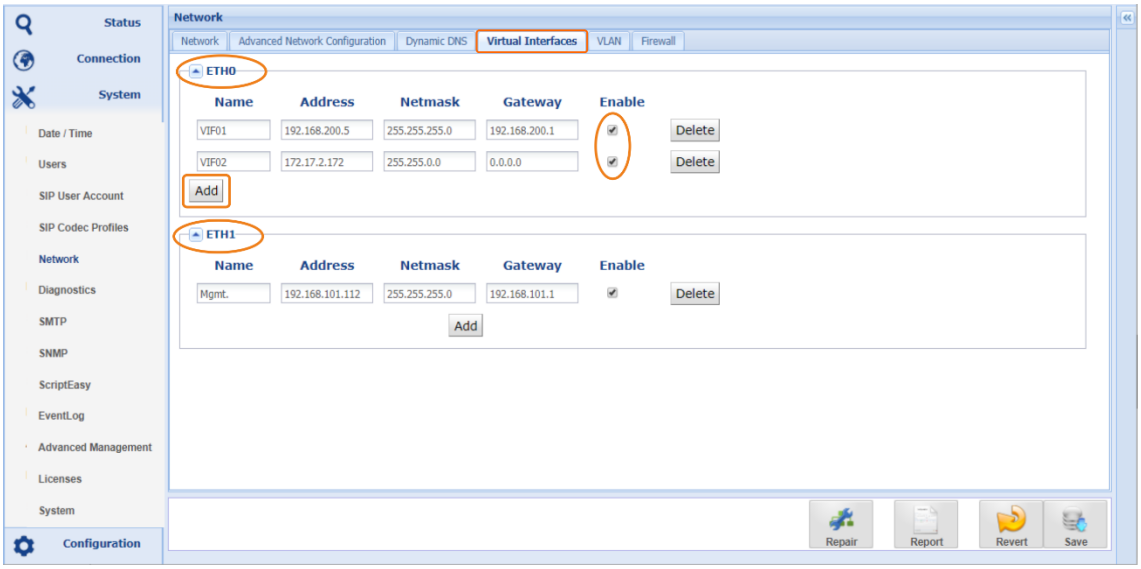
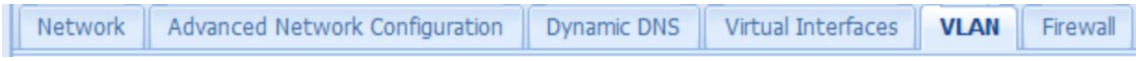


Figure 3-75 shows the management page of virtual interfaces

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. The new interface is available in the drop-down list in the stream configuration window (section 2.4.11 pos. 5).

3.5.7.8 VLAN Tagging – Virtual LAN



Applying VLAN IDs (VID) to the virtual interface allows integrating the AoIP card into a virtual LAN per 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.

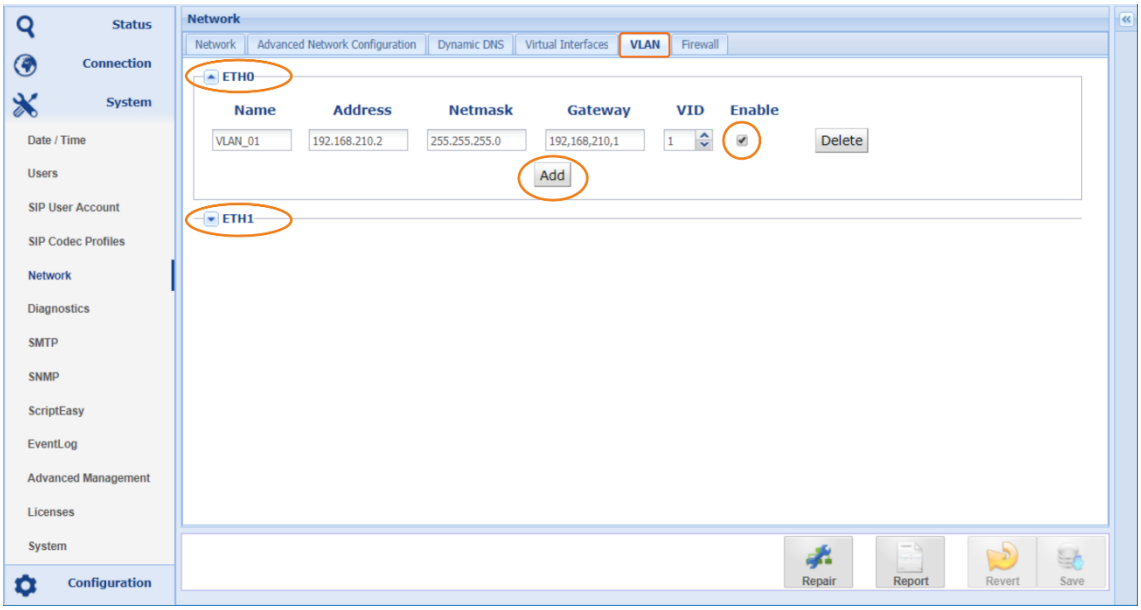


Figure 3-76 shows the management page of virtual LANs (VLAN)

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. The new VLAN interface is available in the drop-down list in the stream configuration window (section 2.4.11 pos. 5).

The VLAN tag protects the IP interface of a VLAN in the Ethernet frame (layer 2). Therefore, any stream to this MAC address without having the correct VLAN tag (VID) is rejected from this interface. There are 4094 VLANs selectable.

Notes:

3.5.7.9 Firewall

The AoIP card provides basic firewall features on the ETH ports as a network appliance. 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.*

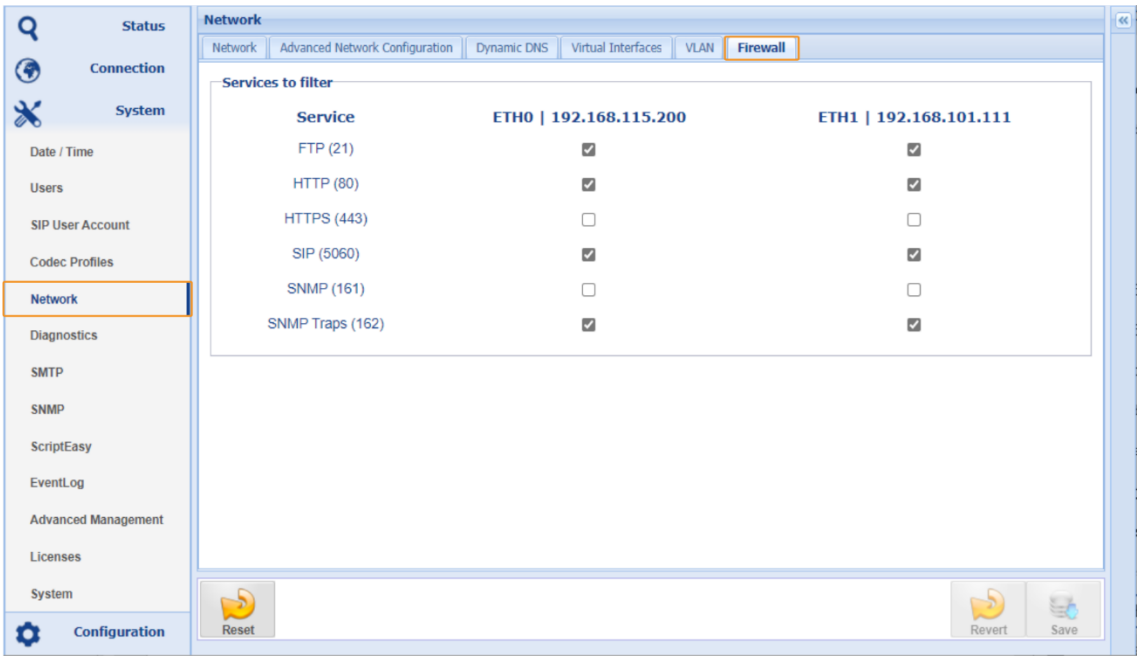


Figure 3-77 shows the filter options on the firewall page - HTTP service (port 80) is disabled on both interfaces

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

Section 1.9.1 presents a list of TCP/UDP ports protected internally or externally.

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!

3.5.8 Diagnostic Page

The Diagnostics page provides some utilities for device maintenance and the Ping Tool for network verification.

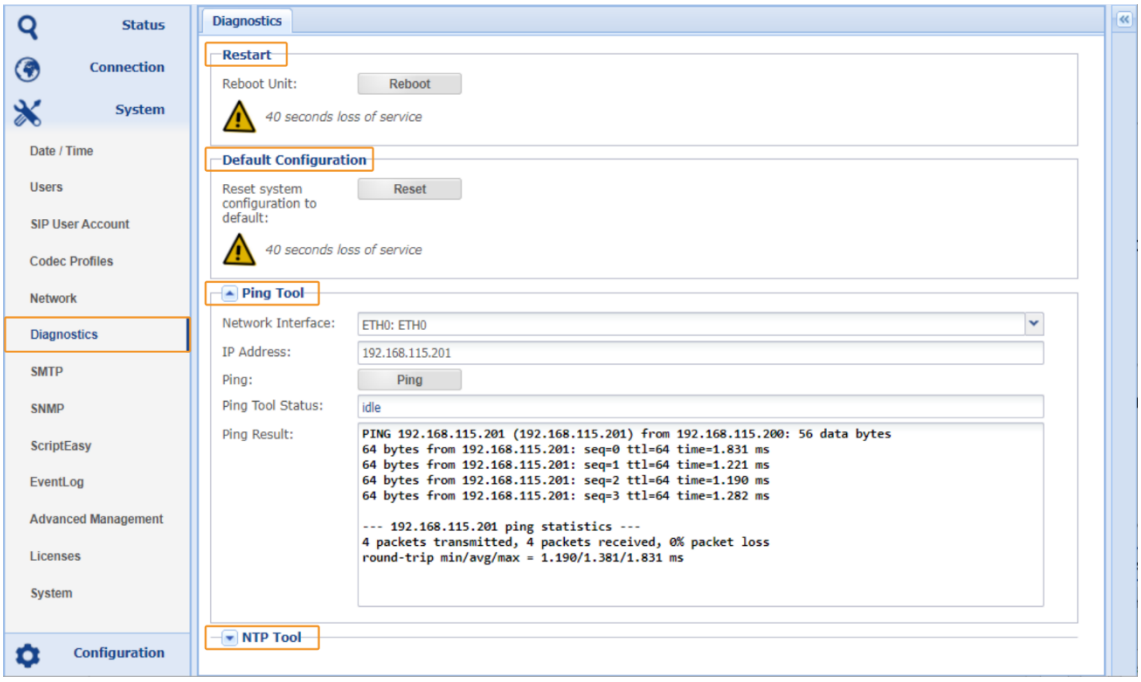


Figure 3-78: Shows the diagnosis page with the maintenance utilities

Restart

This forces a unit reboot – the unit reboots 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 connection profiles, ScriptEasy Scripts (save first!) and all other user configurations BUT NOT the network settings!*

3.5.8.1 Ping Tool

This ping tool works in the usual way and allows sending a ping directly from the selected ETH interface. This diagnostic tool facilitates the identification of possible connection problems. Host names can also be used instead of the IP address if a DNS server has been configured on the network page.

ⓘ *If the hostname could not be resolved or an invalid IP address was entered, the ping tool returns to idle mode without comment.*

3.5.8.2 NTP Tool (Status Monitor)

Below the ping tool, you find the NTP Tool. The Ping tool window can be minimized. Click the "NTP Status" button to see and update the current status of the previously entered NTP servers.

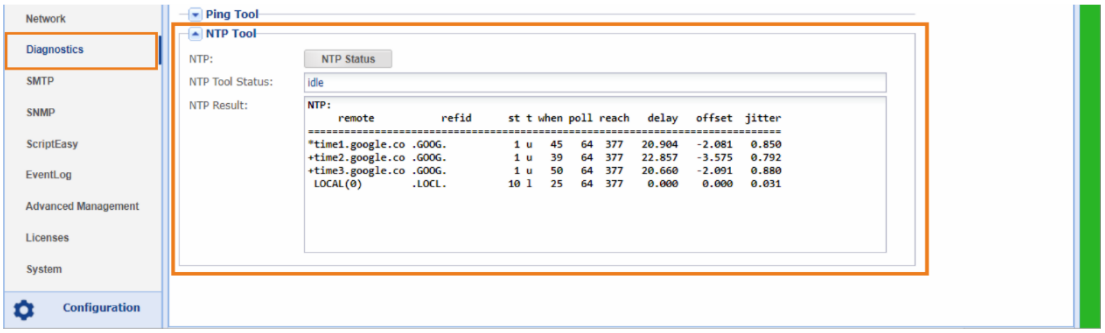


Figure 3-79 shows the NTP tool with the status information table of all registered NTP servers.

How to read the Table

If the first character of a line is not space, it contains an identifier of how the NTP daemon evaluates this time source. Immediately after the daemon starts, all lines contain a space at the beginning.

The NTP daemon needs several polling cycles to check the specified time sources and select one of them as the one it synchronizes with.

remote: Shows the list of IP addresses or the hostname of the connected NTP servers, including localhost (LOCAL), if no server can be reached. The currently used reference server is marked with a "*." The next best server is marked with "+."

refid: Reference ID is the ID of the time reference of the currently active NTP server.

st: Shows the stratum of the NTP-server.

t: type, u = unicast client, b = broadcast or multicast client, l = local reference clock

when: Shows the number of seconds since the last polling cycle. When this value reaches the value shown in the poll column, the NTP daemon performs a time comparison with the corresponding reference time source and sets the "when" value back to 0.

poll: Is the polling frequency in seconds, from 64 to 1024.

reach: This shows whether the reference time source was accessible during the last polling cycles. The number is an 8-bit register whose value is displayed in octal notation (for historical reasons). If the NTP client has just started, the reach-value for all time sources is 0. After each successful polling cycle, the values 0, 1, 3, 7, 17, 37, 77, 177, 377 are displayed one after the other. 377 is the highest possible value indicating that the last 8 polling cycles were successful. Successful means that data could be exchanged with the time source and that the reference time source itself was also synchronous with its own time source.

delay: This value is the time between the NTP client's request and the arrival of the response.

offset: This value shows the time difference between the reference time and the own system time.

jitter: This value indicates the degree of fluctuations between individual time comparisons.

3.5.9 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).

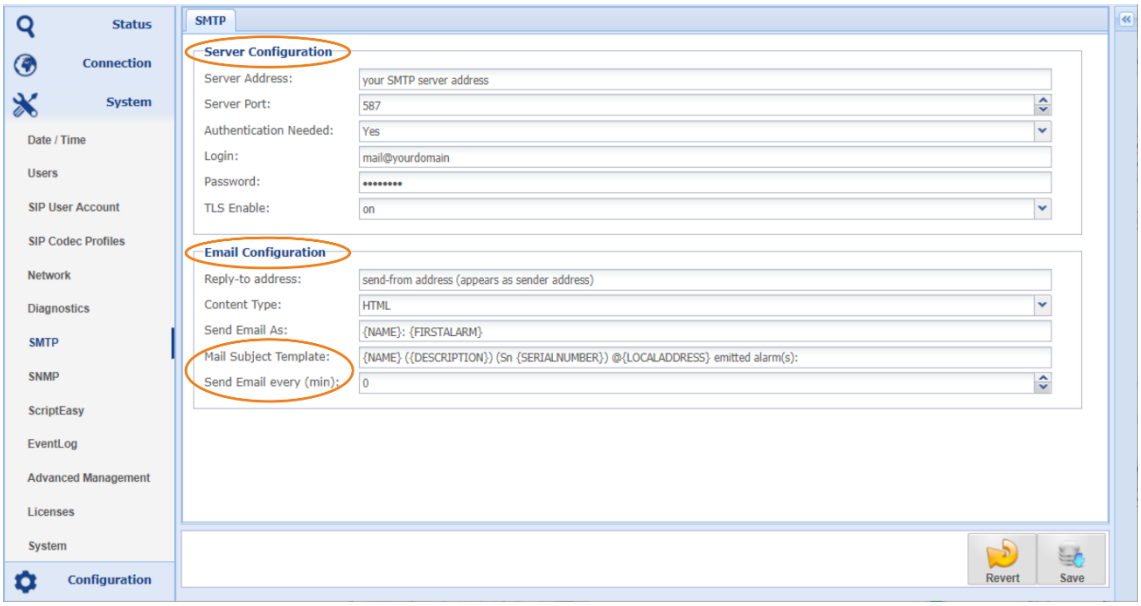


Figure 3-80 shows the SMTP (email) configuration page

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 Minute(s):

The number of minutes set here defines the interval to send an email. For example, with the value "0" minutes, the SMTP server sends the mail immediately when an alarm occurs.

Once this configuration is completed and tested, the mail alert feature can be used in the alarm settings. The User Account page provides an option for sending a test mail (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:

3. {NAME}: Unit name which was applied to the unit
4. {FIRSTALARM}: Alarm Status (Alarm active / Alarm cleared)
5. {DESCRIPTION}: Information about unit Type, i.e., AoIP Card
6. {SERIALNUMBER}: Serial number of alarming unit
7. {LOCALADDRESS}: IP address of port ETH0 of alarming unit

3.5.9.1 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:

3.5.10 SNMP

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

3.5.10.1 SNMP Agent

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

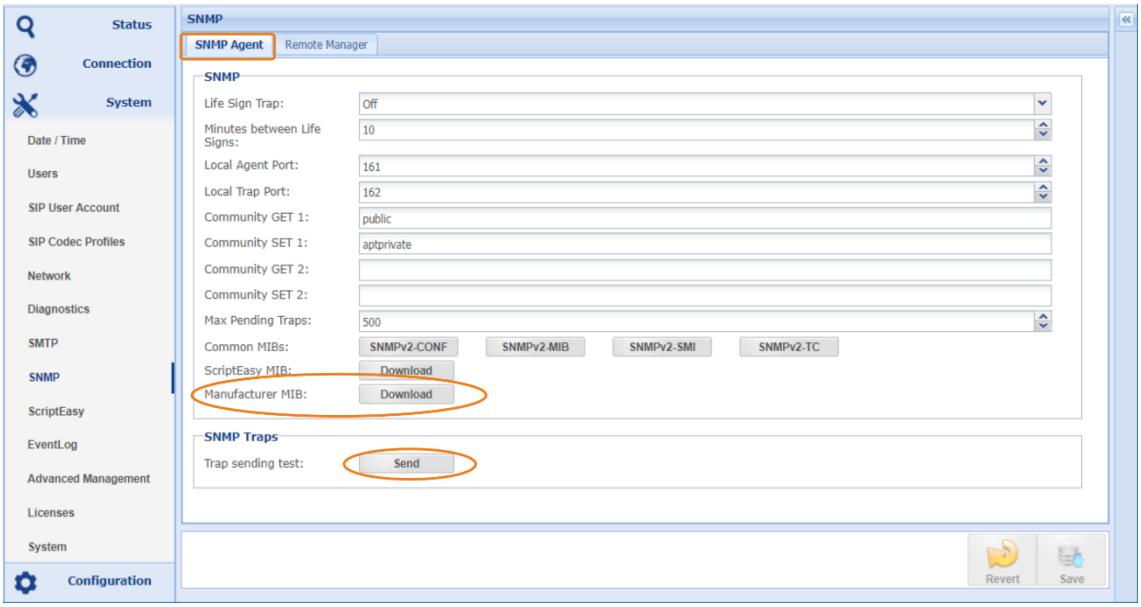


Figure 3-81 shows the SNMP-Agent configuration page

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

3.5.10.2 SNMP MIB Files

You can download the required MIB files from this page.

- The Manufacturer's 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 standard SNMP files. You can download the full set from this page if your SNMP Manager refers to these files. These are no device-specific files.

3.5.10.3 SNMP Remote Manager

The SNMP Manager configuration allows the setup of four SNMP remote manager instances. In addition, the general Trap management has been integrated into this page, allowing different Trap management for each remote manager.

A Remote Manager describes the SNMP Manager in the network.

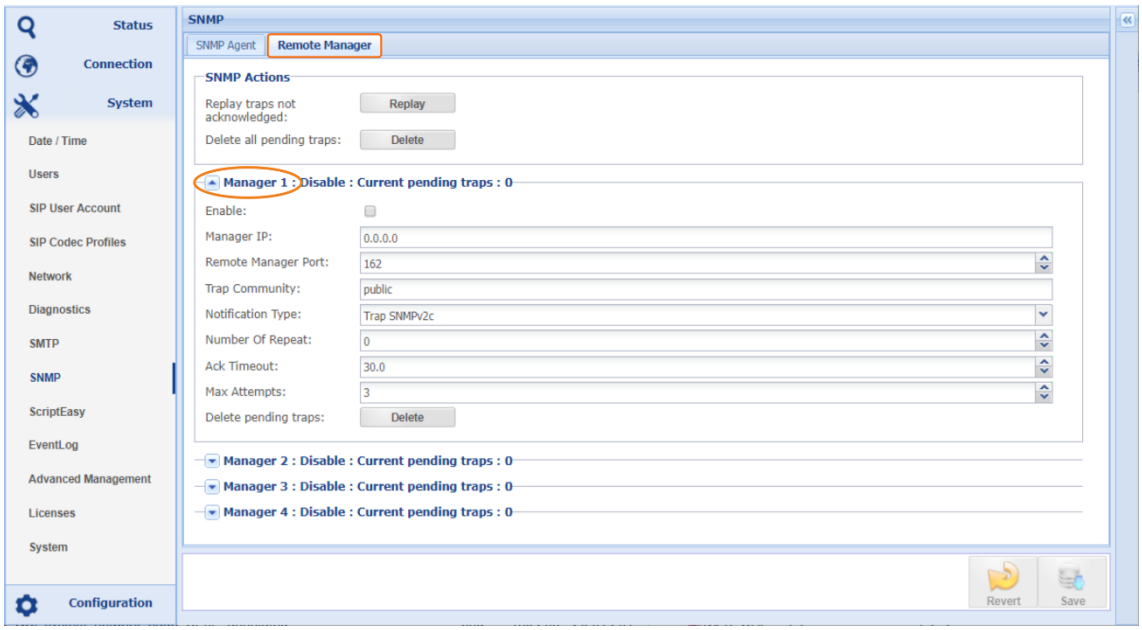


Figure 3-82 shows the configuration page for the SNMP Remote Managers

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 "Replay" re-sends the traps. Clicking on "Delete" deletes the pending traps from 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

3.5.11 ScriptEasy

A Script Application is a ScriptEasy script supplied by WorldCast Systems, which adds extra functions to your AoIP Codec. The requirement to use an application is activating 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 include breakout cables or other utilities.

A separate user/developer manual can be downloaded from the [WorldCast System] website (user account required).

3.5.11.1 Application Builder

The ScriptEasy IDE (Integrated Development Environment) is a separate PC application and consists of a graphical application designer (please get in touch with your APT representative). The IDE allows the creation of 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 screenshot shows an example of how an application can be used on an APT Codec.

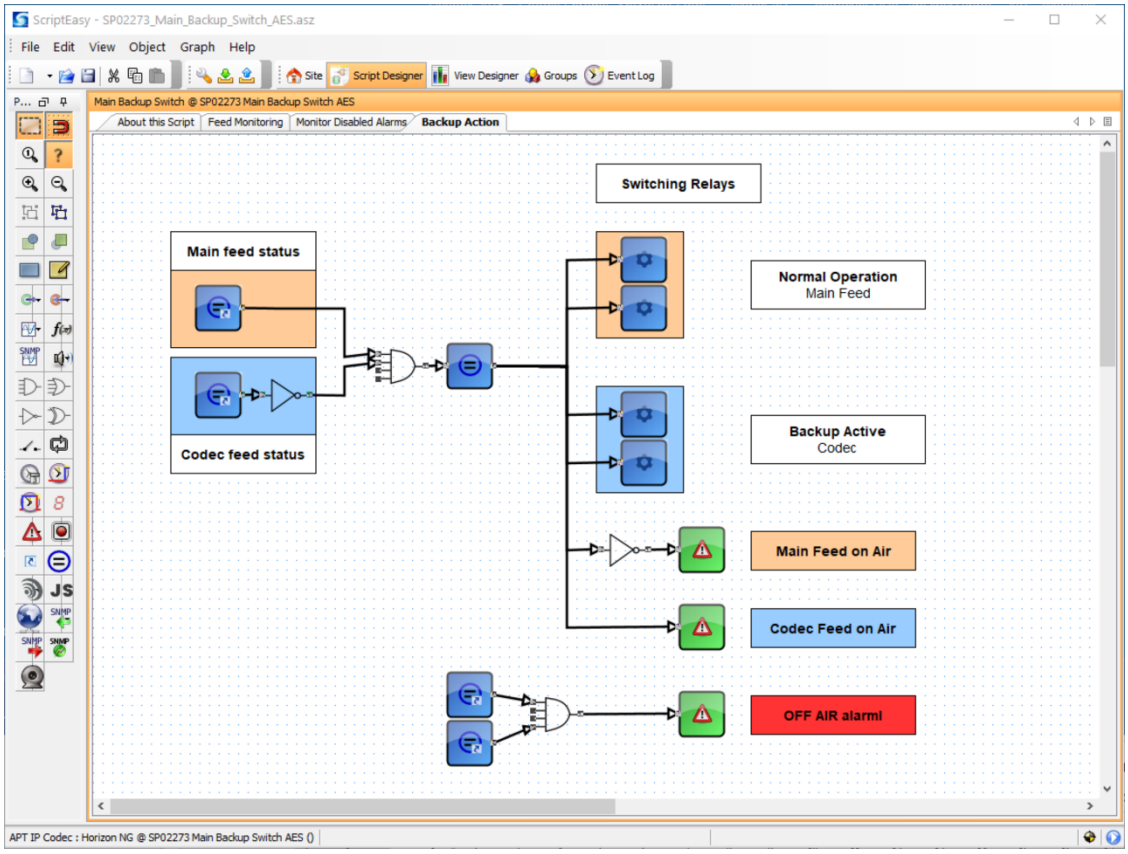


Figure 3-83: Shows the Script Application Designer IDE

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

3.5.11.2 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.

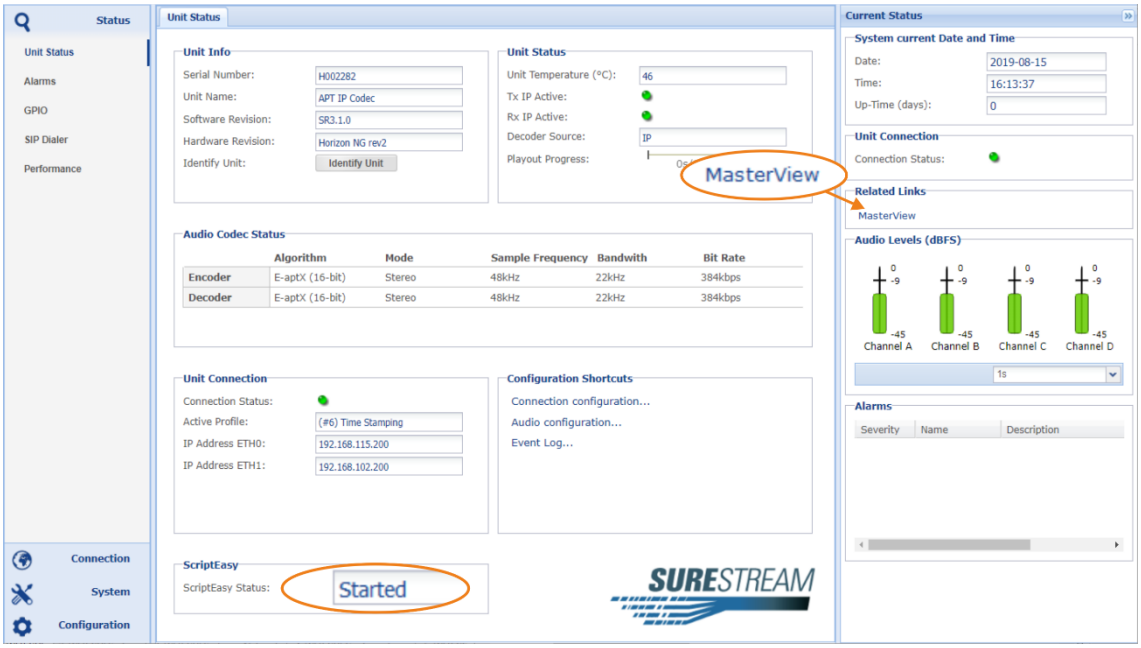


Figure 3-84: The status page showing the link to MasterView

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.

Notes:

3.5.11.3 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.

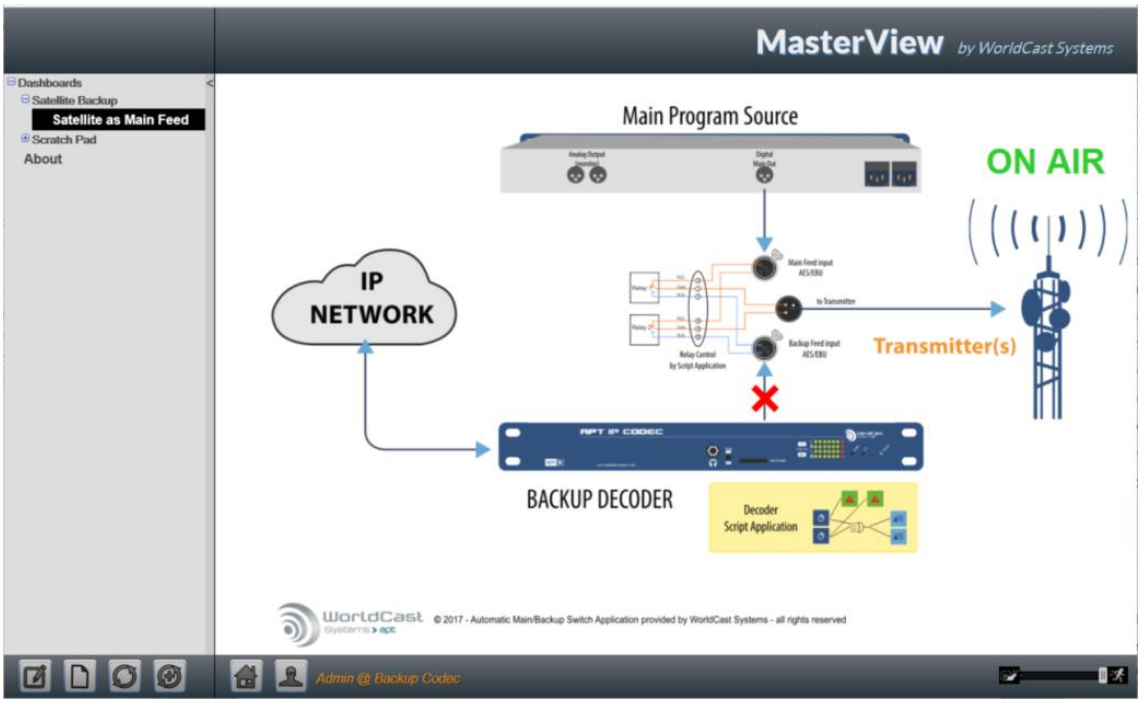


Figure 3-85: Shows the application status on the MasterView dashboard.

Note that the application and the dashboard shown above are examples of the APT Codec to host the script. The same application or any other design is the same way possible with your AoIP card.

Notes:

3.5.11.4 ScriptEasy Control

The ScriptEasy page is used to start and 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 restarts after a unit reboot! 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 does not appear again; this information is stored in a browser cookie.

A script may overwrite user actions on its own! Therefore, if you want to deactivate a script permanently, you must follow the procedure described in section 3.5.11.5.

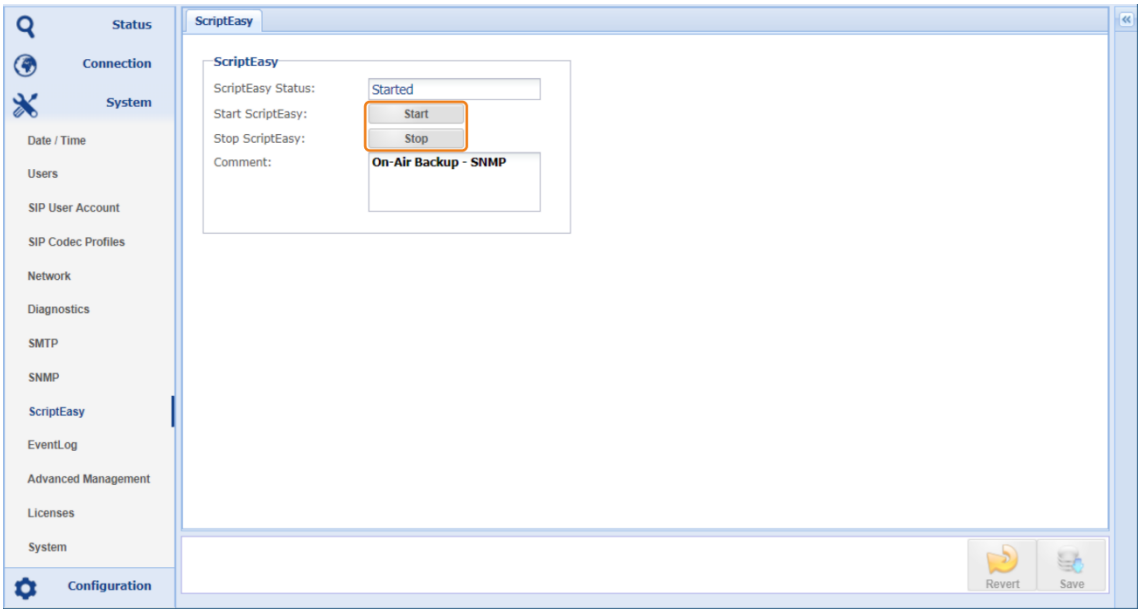


Figure 3-86 The ScriptEasy page in the system menu shows the script controls

ⓘ *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 3.5.7.9).

3.5.11.5 ScriptEasy Remove a Script

Once you have uploaded a script to the Codec device, it becomes active automatically. The GUI offers only limited control of the script. To permanently deactivate (deleting) a script, it must be overwritten by an **empty script** (a script without content).

3.5.12 Event Logging

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

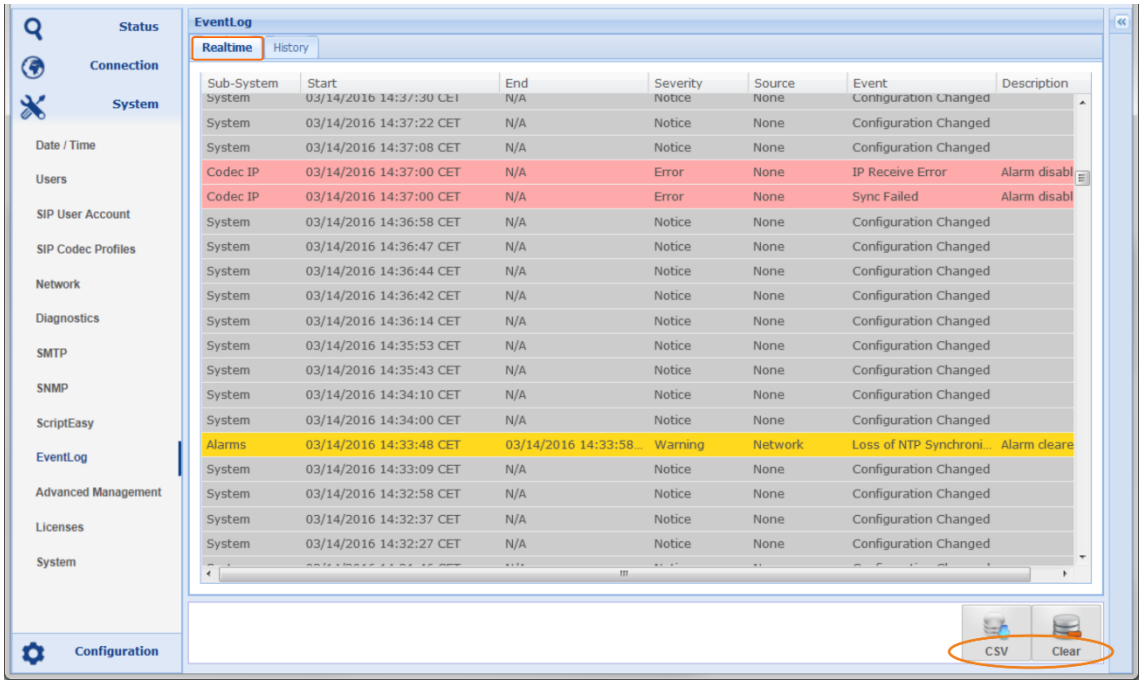


Figure 3-87 shows Event Logs in the real-time

3.5.12.1 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.

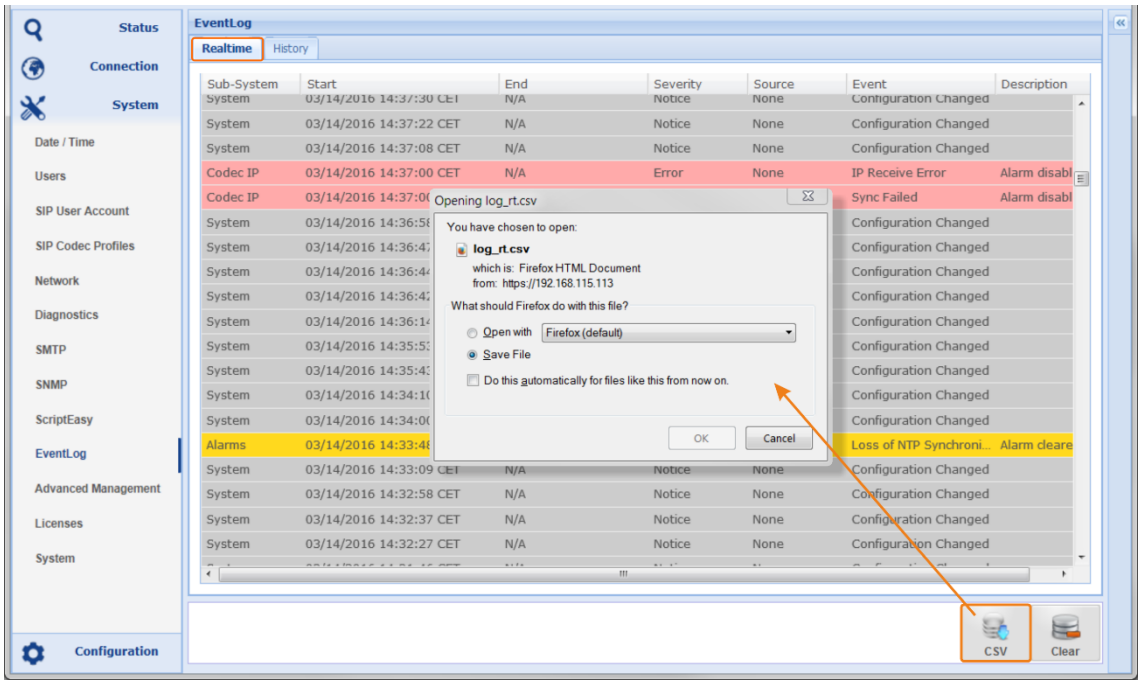


Figure 3-88 shows the browser popup for exporting the CSV formatted file

3.5.12.2 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 presents an empty page. Then, clicking the "Search" button starts the retrieval process following the selected search options.

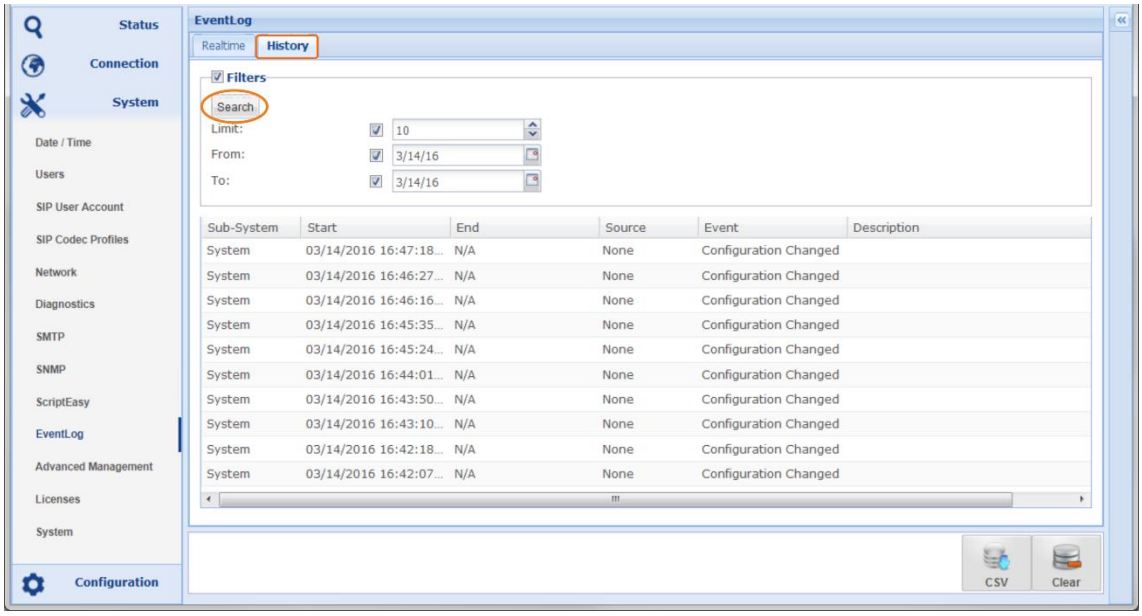


Figure 3-89 shows the history retrieval options

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

Notes:

3.5.13 Advanced Management

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

- SD Card Management
- SD Card System Backup
- Backup/Restore Configuration
- Firmware Update

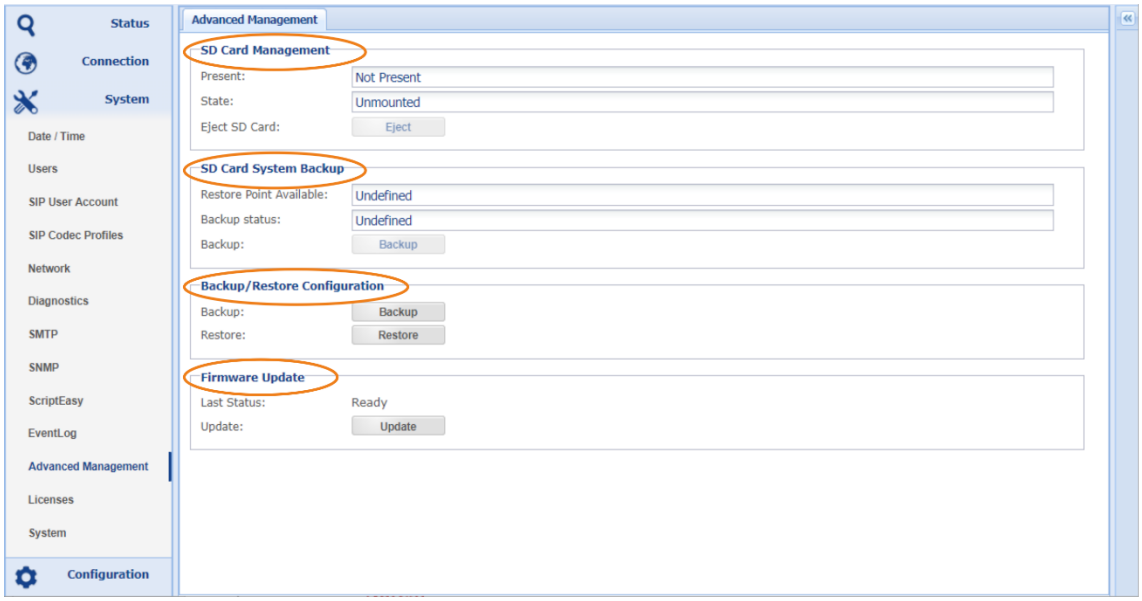


Figure 3-90 shows the advanced Management options

Notes:

3.5.13.1 Inserting an SD Card

- Pull the AoIP module out of the chassis slot
- Insert the Micro-SD card as shown below
- Re-insert the card into the chassis slot

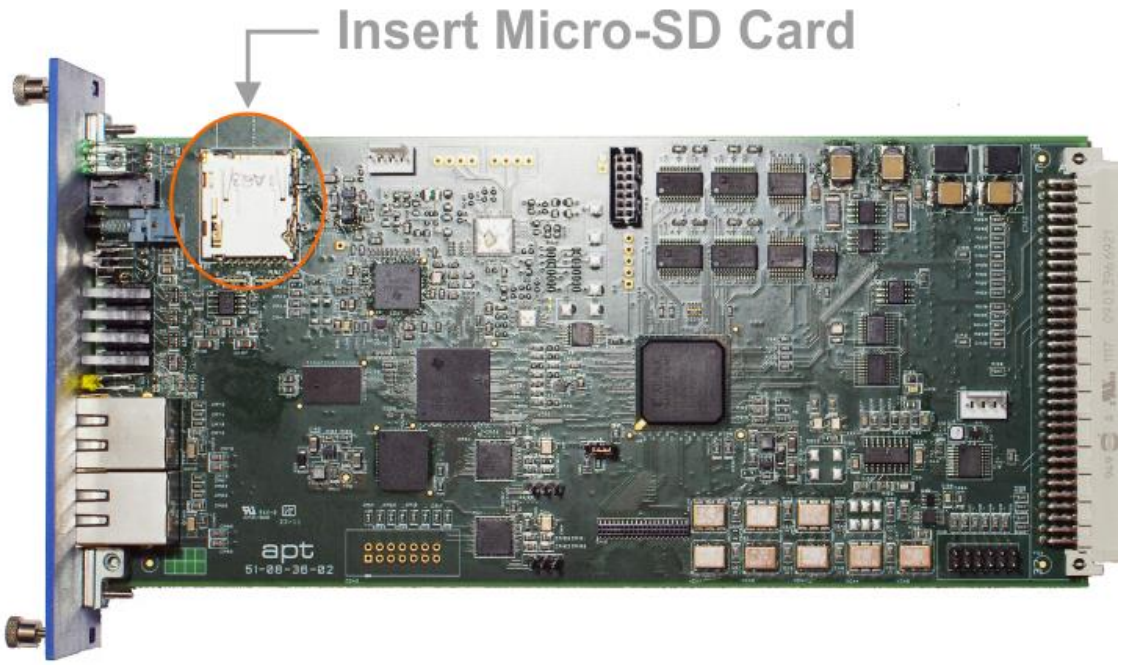


Figure 3-91 shows how to insert an SD card

3.5.13.2 SD Card Management

Once an SD card has been inserted, the system mounts the card (only **FAT 32** is supported). The SD Card status shows "Mounted." Clicking on the Eject button unmounts the card.

ⓘ *An SD Card is mounted when inserted – no manual mounting is required.*

Two system applications support and require the SD card to be mounted.

- SD Card System Backup
- Audio Backup on SD card

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

3.5.13.3 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 configurations, including network settings and all user settings

If you restore this backup file to a new module, the new unit appears as an exact clone of the origin AoIP card (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.

ⓘ *To only reload 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 backup file's status and creation date. 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 3-91).
- Remove the power lead(s) from the chassis
- Insert the AoIP card into the chassis
- On the AoIP module's front panel, there is a small hole where behind this hole sits a little Switch (refer to section 1.7.2). Press this button and connect the power supply to the unit. Hold the button during power-up until the status LED flashes (about 10-15 seconds). After that, the unit boots and loads the configuration from the SD card.

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

Notes:

3.5.13.4 Backup/Restore Unit Configuration

This option exports and restores the unit configuration to and from offline storage like your PC's hard drive. A backup consists of all unit parameters, including ScriptEasy applications, user-defined alarms and all parameters which may differ from the default values.

- 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, click on the backup file and upload the .dat file to the unit. A configuration file name consists of the unit's serial number, date, and time of creation, e.g., for IP Codec #N000105: backup-N000105-20160408-181525.dat.

⚠ You can edit the file name only behind the Serial number part, e.g., "backup-N000105-*My-AoIP-Card*.dat." You must keep the word "backup" and the serial number!

Confirming the restore action loads the backup configuration to the unit.

The management system restarts, and the GUI prompt you to reconnect (it takes approx. 15 sec.). All configurations from the backup are valid after reconnecting **except the settings from the main network page**. To apply the **network settings** from the backup configuration, open the network page and click on "Repair." This action applies the settings from the backup file **to** the network "Current Status." The procedure overwrites your old IP addresses and requires a reconnect from the browser on the **new IP addresses** derived from the backup file.

⚠ If you want **to keep the old network settings**, you MUST **manually** copy the values **from** the "Current Status" into the fields under "Static Configuration." Otherwise, the backup configuration data are automatically applied at the next unit bootup. This results in a loss of browser connection.
Also note: All other network-related configurations are automatically copied from the backup (Advanced Network Configuration, Dynamic DNS, Virtual Interfaces, VLAN and Firewall). You must always manually change them back to the old values if needed.

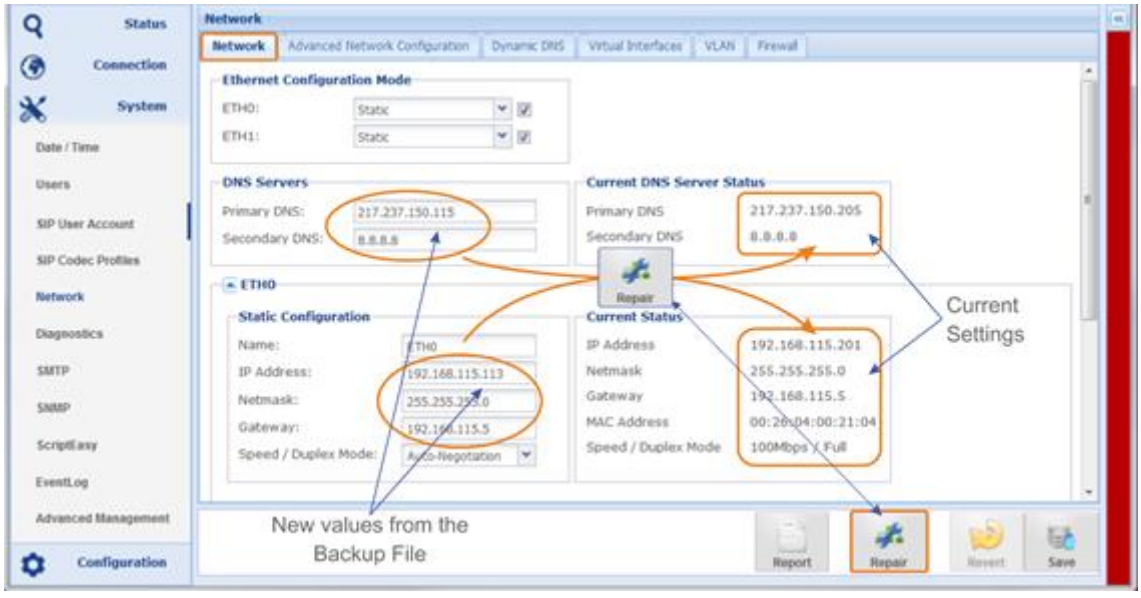


*Figure 3-92 shows the main network page after a backup file was loaded. The network values (Static Configuration) differ from the "Current Status." Clicking on "Repair" or **a reboot** applies the network settings to "Static Configuration" from the backup file to the unit (Current Status).*

3.5.13.5 Firmware Update

This section is the step-by-step instruction for performing a firmware update successfully. It is a straightforward 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

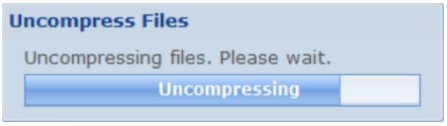
A Firmware release consists of a set of inter-compatible firmware files. These are the DSP, OS, and WEB GUI files. A system release is always delivered as a Zip-Archive.

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

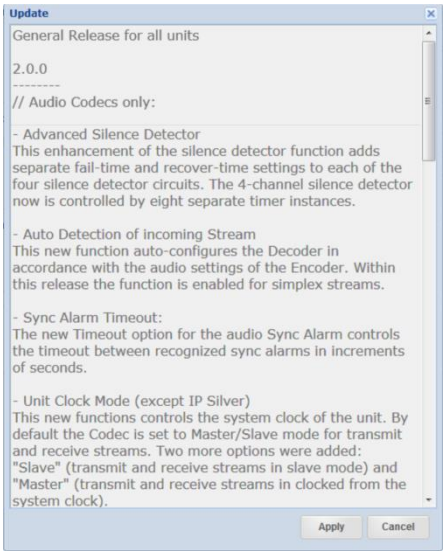
Clicking on the "Update" button opens the PC file browser. Navigate to the folder where the firmware file is stored and select the zip-archive (Oslo_AoIP_SR_x.x.x.zip). Confirm your selection and proceed with the firmware update.

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

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

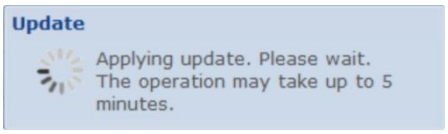


Once the firmware archive is successfully uncompressed and verified, the window with the release note appears. The release note contains the essential information about new features, bug fixes and other changes in the new firmware.



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.*

3.5.14 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 can no longer be used.
- **ScriptEasy**: With SR 2.0, the ScriptEasy license has been 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.

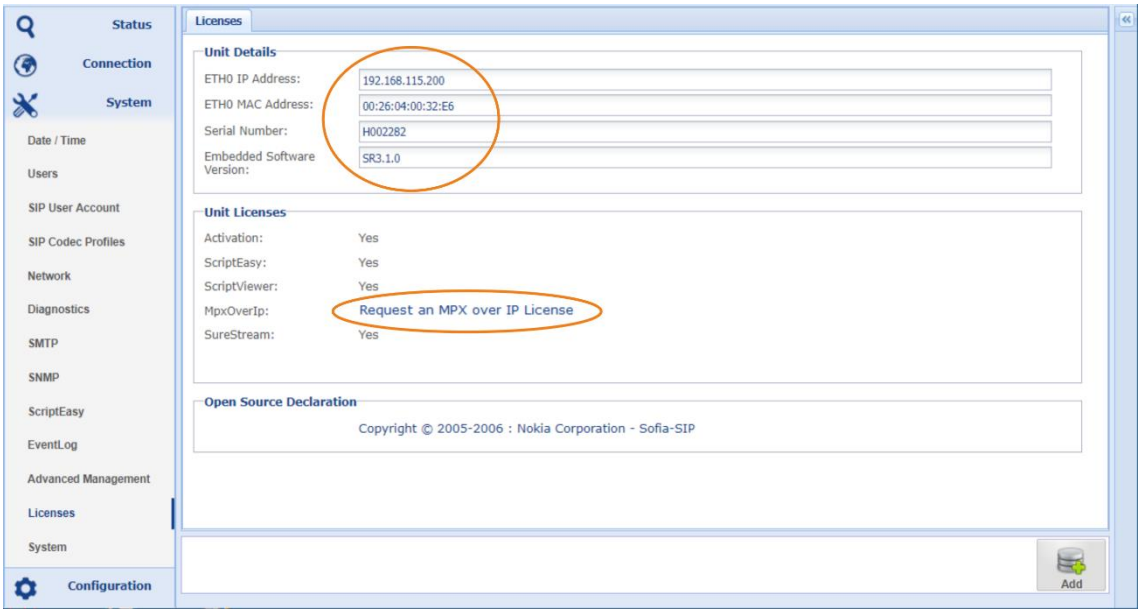


Figure 3-93 shows the unit parameter for getting an options license

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.

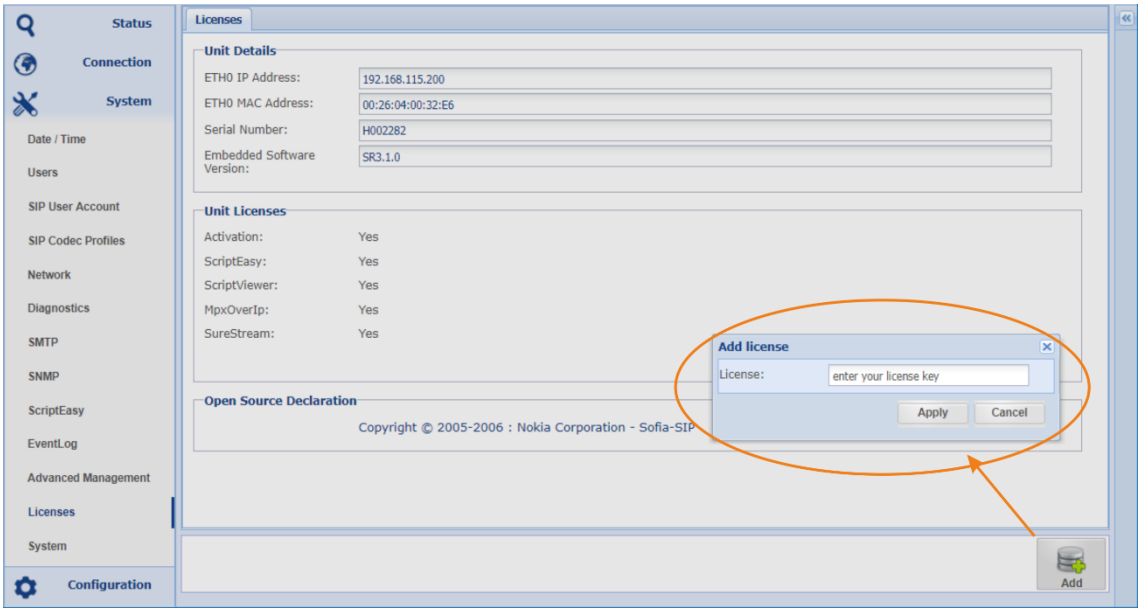


Figure 3-94 shows how to apply a new license key to the system

Notes:

3.5.15 System

This page displays the hardware and software versions 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 and 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.

Operational Mode

- This mode selection box allows the change of the AoIP card's operational modes: Simplex for dual Encoder/Decoder or Duplex mode. "Simplex Mode" (dual Encoder or dual Decoder) sets the unit to dual stereo operation. The AoIP card can send or receive two independent audio streams with different encoder or decoder settings (different algorithms and stream configurations).

⚠ Changing the Operational Mode deletes all current audio coding and streaming settings. It also deletes all profiles created with the previously selected mode! You can save these profiles to offline storage.

System Information

This section provides system information regarding current software versions.

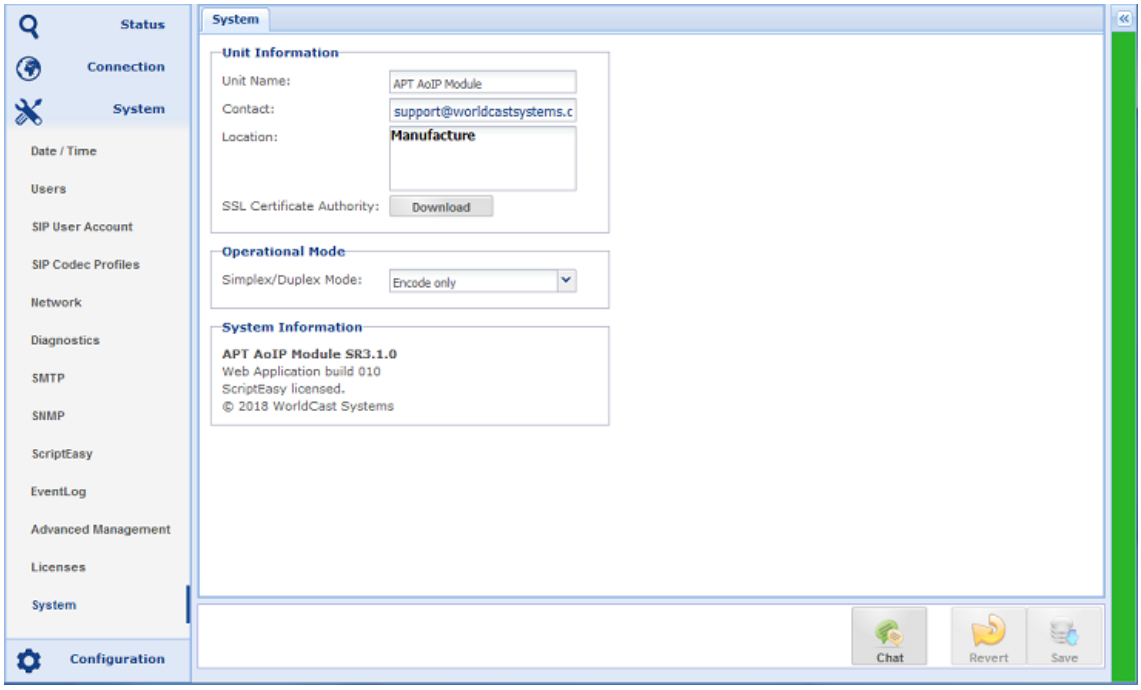


Figure 3-95 shows the "System" page of the System menu

3.5.15.1 SSL Certificate Authority

Download the SSL certificate shown in Figure 3-95 and store it on your computer. Next, 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 into "Certificate Authorities." It appears as a WorldCast Systems certificate.

You must install it only once; it is valid for all WorldCast Systems devices connected to this browser.

3.5.15.2 Chat Box

The System page also provides a little chat box to send short messages to other logged-in users. The "Screen Name" field on the user LogIn defines the user's name that appears in the chat box.

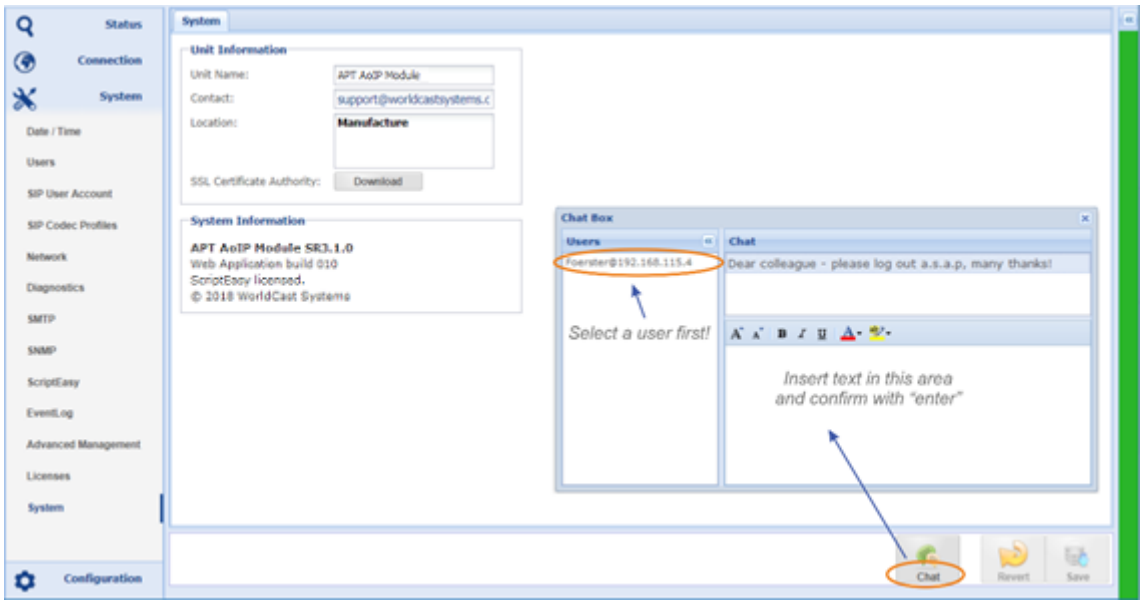


Figure 3-96 shows the "System" page of the System menu with Chat Box open

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 from which this message was sent (see next page).

The chat box uses UDP datagrams for sending these messages.

ⓘ *The username 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.

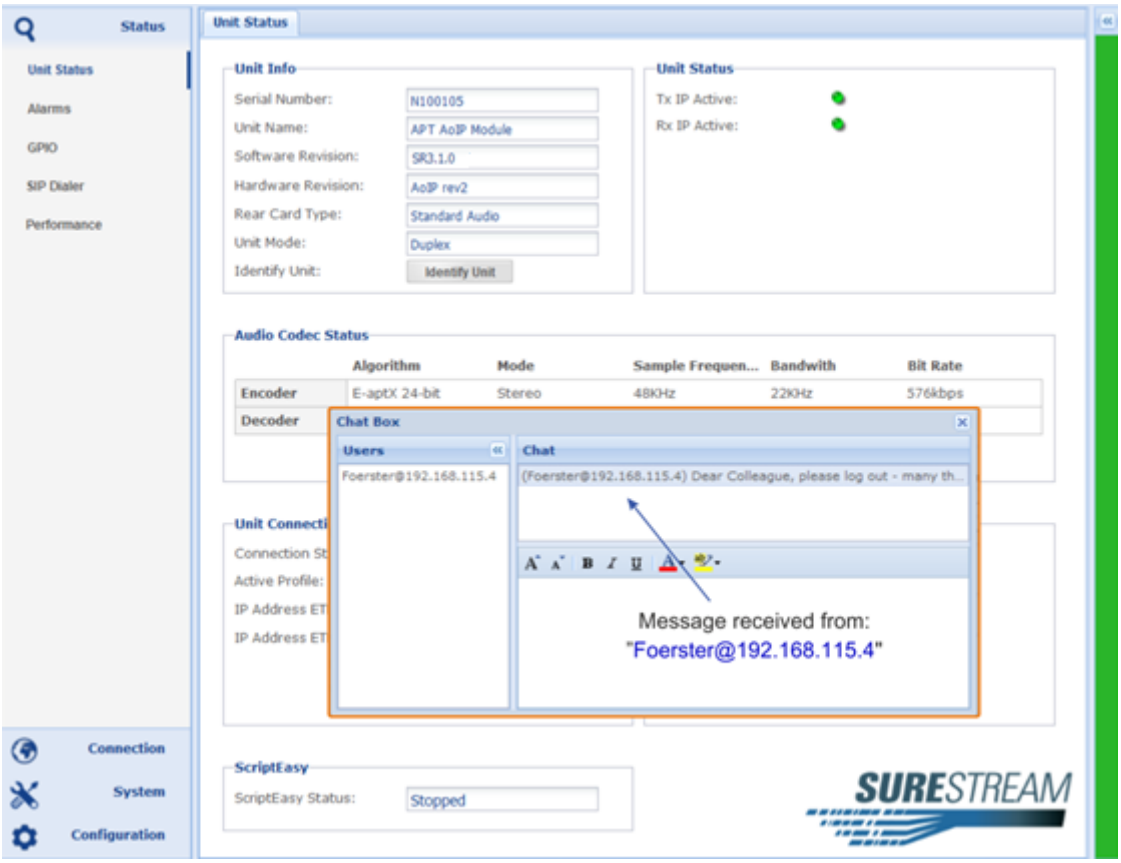


Figure 3-97 the chat box pops up when a message is received

3.6 Main Menu - Configuration

The configuration menu provides four submenu items, the Audio Configuration, 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

The options available on the audio setup page can differ depending on the selected operational mode (Simplex or Duplex).

Simplex or Duplex Mode

Selecting a different operational mode, simplex dual Encoder/Decoder or duplex, is a general system configuration that deletes all previously created profiles (refer to section 3.5.13.4 about saving the settings if desired).

For example, the screenshot below shows the options for the duplex mode.

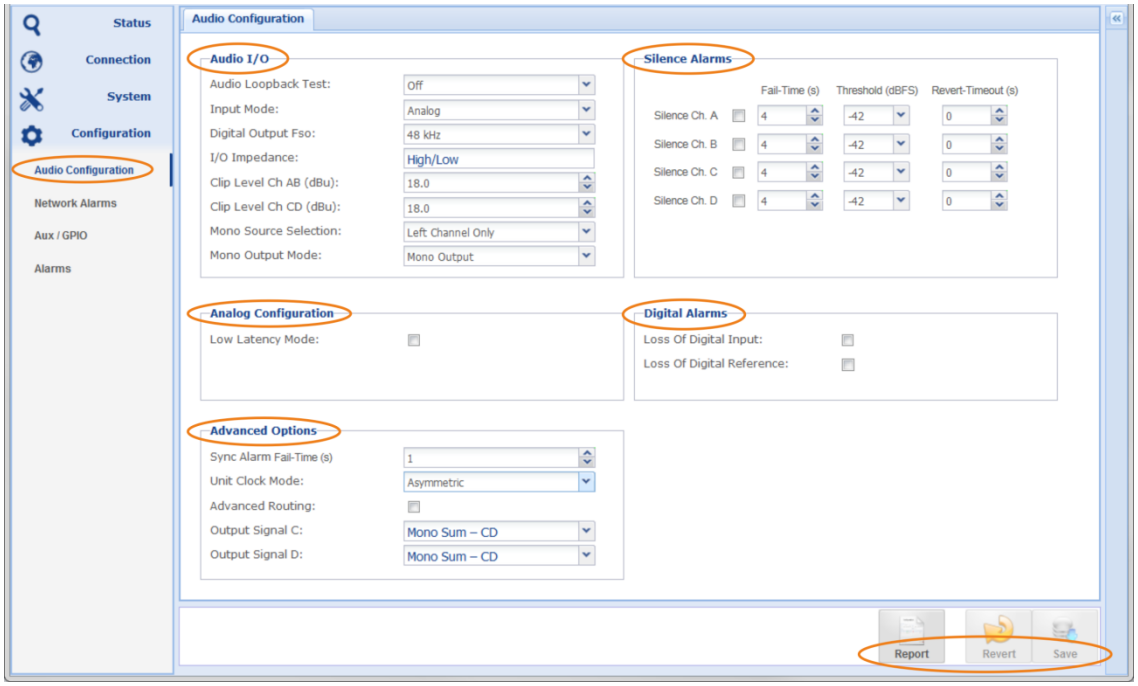


Figure 3-98 shows the Audio Configuration page for duplex mode

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

3.6.1.1 Audio Configuration in Duplex Mode

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 read only[2]	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 0-18 dBu	Adjusts the analog Input level in reference to the digital dBFS in increments of 0.1 dB
Output Clip Level (dBu)[3]	Values 0-18 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 them by 2 (-3 dB)
Mono Output Mode[4]	Mono Output MonoFill	Mono Output on the 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] Refer to the hardware manual to see how to change the impedance by jumper
[3] Analog Outputs are non-functional when 96 or 192 kHz is selected.
[4] MonoFill cannot be used together with the advanced routing option as the two features stay in a conflict

Audio Configurations duplex *(continued)*

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 = +18 dBu. For example, if an analog signal of +6 dBu shall equal -9 dBFS, then the **analog clip level** must be set to +15 dBu (0 dBFS = 15 dBu, hence -9 dBFS = +6 dBu).

3.6.1.3 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 occurs 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), 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

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 time. The system does not flag sync alarms shorter than the defined fail time.

3.6.1.5 Unit Clock Mode

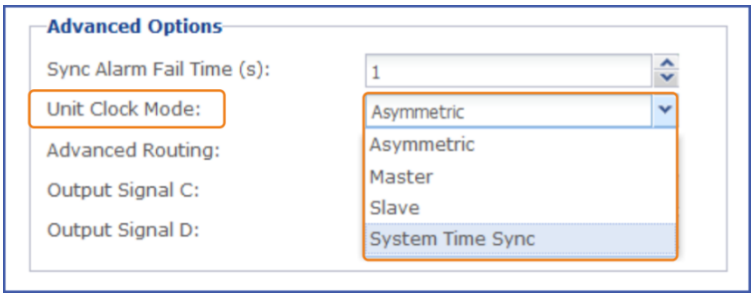


Figure 3-99 shows the Unit Clock Mode selection

- **Asymmetric**:
  By default, the Codec is clocked asymmetrical if it is set to duplex mode. Asymmetrical clocking guarantees 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 to send a stream (Tx) and receive a stream (Rx). This mode is only useful in a LAN environment or a network with no or extremely low delay jitter.
- **Slave**:
  This clock option is only available in the Duplex operational mode of the AoIP card and uses the internal VCXO for sending (Tx) and 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. Units configured to use this mechanism should have NTP enabled as the system time source (refer to section Date and Time 3.5.1). If NTP is not enabled, this mode equals the Master Mode.

ⓘ *You can use "System Time Sync" and the NTP system time source to adjust the overall link latency. This application is described in section 3.6.2.*

Notes:

3.6.1.6 Advanced Routing & Decoder Mono Mode

The complete description is available in section 3.6.1.9.

Advanced Routing must be enabled by the check box "Advanced Routing" and clicking on "Save" at the bottom of the page.

"Output Signal C" and "Output Signal D" describe the physical outputs on the rear of the codec. The drop-down list shows the available signals:

"Mono Sum CD" is the mono sum from the equation ((C+D)/2).

Signals "C" and "D" represent the signals L/R from the received stereo stream.

In duplex mode, the advanced routing and mono mode feature offer the mono sum signal on both outputs C and D. This takes effect on the digital and the analog outputs.

3.6.1.7 Digital Alarms

Digital Alarms 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 flags this alarm if the digital source at the digital input is lost
Loss of digital Reference	Enable/Disable	Enabling this checkbox flags this alarm if the digital reference signal at the reference input is lost

**Note, in simplex mode, this check box enables these alarms for both stereo paths (A/B and C/D).*

3.6.1.8 Silence Alarm Configurations

These alarms are Silence Detector alarms. These settings enable the alarm for each Input and Output channel (A/B/C/D). In addition, you can set the Fail Time, the threshold level and the Revert Time for each channel 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.

3.6.1.9 Advanced Routing & Decoder Mono Modes

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

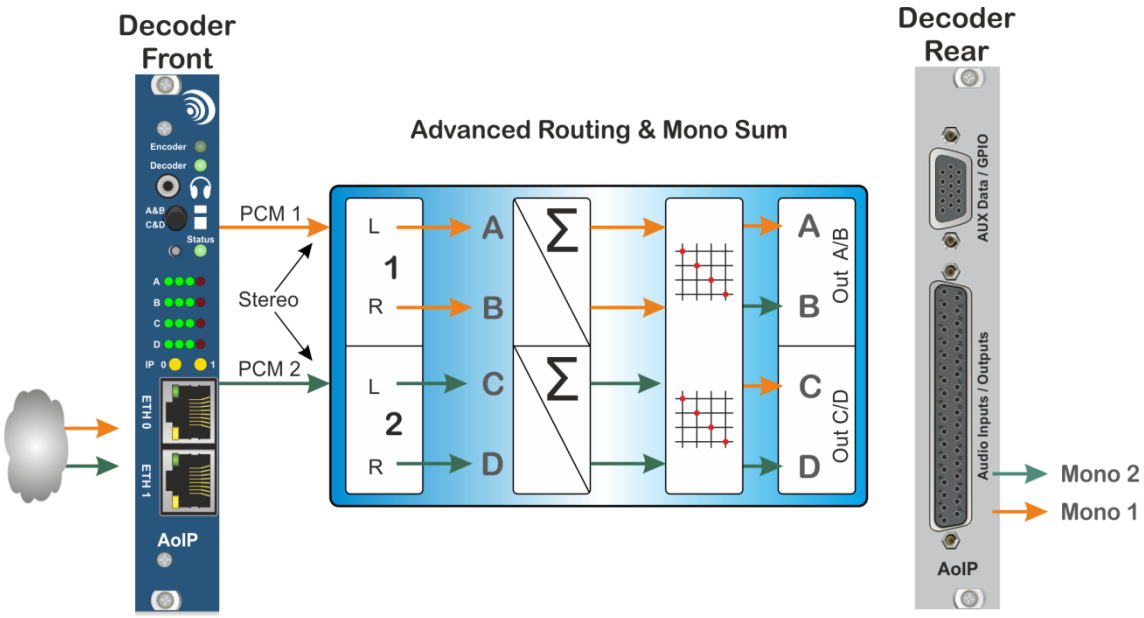


Figure 3-100 shows the principle of this feature in dual Decoder mode

Decoder Mono Modes

This feature creates 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. Besides 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 a stereo feed, e.g., an FM supply and a mono feed for an AM supply – the mono/stereo signal is generated from the same stereo stream.

Advanced Routing

This feature allows the flexible routing of decoded PCM streams from the DSP output to the physical output connectors on the rear panel of the decoder. By default, and if the advanced routing feature is disabled, the signals are routed 1:1. According to the operational modes (duplex or simplex decoding), the options are different.

ⓘ *In Encoder mode (simplex), the advanced routing option is unavailable – this is a Decoder option only.*

3.6.1.10 Simplex Mode

Other than on the duplex mode, the input and output configurations for simplex modes (Encoder and Decoder) are separated. The Encoder provides options for Input settings; the Decoder only allows settings for the outputs.

ⓘ *Selection of the signal domain (analog or digital) for inputs and outputs in Encoder mode is valid for both stereo signals (A&B and C&D).*

3.6.1.11 Dual Decoder Mode

The Decoder mode supports dual stereo decoding; hence, the Audio Configuration page provides only output settings. This page provides the same controls as the duplex mode and, in addition, the Advanced Routing options.

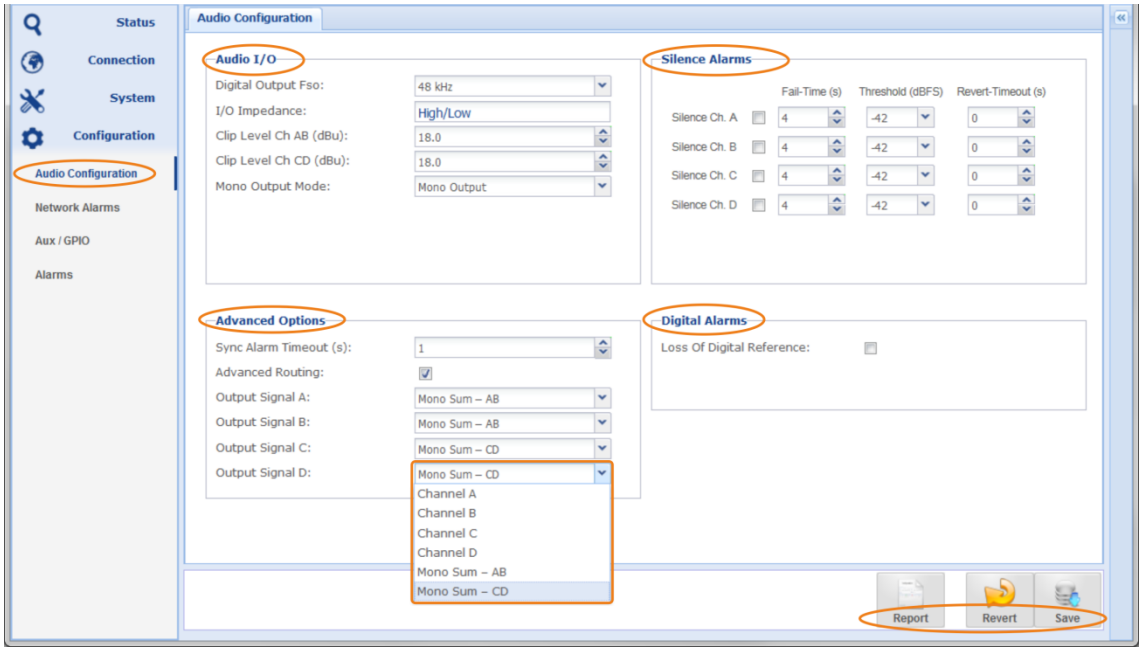


Figure 3-101 shows the Audio Configuration page for Simplex Decoder mode

Advanced Routing & Decoder Mono Mode

Advanced Routing must be enabled to become active by clicking the check box "Advanced Routing" and clicking on "Save" at the bottom of the page.

"Output Signal A" to "Output Signal D" describes the physical outputs on the rear of the codec.

For each output signal, the drop-down list shows the available signals:

- "Channel A to D"
- "Mono Sum AB"
- "Mono Sum CD"

Audio Configurations simplex Decoder Mode *(continued)*

The signal "Mono Sum AB" and "Mono Sum CD" represent the mono sum from the equation ((L+R)/2) for AB and CD. Signals "A" to "D" represent the input signals from the received stereo streams.

This routing matrix allows a combination of assignments of individual channels or mono-sum signals to the physical outputs. If the mono sum AB is assigned to any Output, then the individual channel A or B are not available even if the drop-down box still offers this option. A validation rule will reject saving a wrong combination. The same logic is valid for signals C and D.

The Validation Engine prevents unallowed combinations. Usually, the advanced routing options are configured after the decoder IP streams to get a direct response from the Validation Engine.

3.6.2 Program Time Alignment

This standard function is based on one or more NTP servers as a time base for transmitting time information utilizing timestamps. The transmitted packets get a timestamp from which the decoder determines the desired playout time of the packets.

All corresponding decoders must be configured in the same System Time mode.

Set your system time to NTP time (section 3.5.1) and select the "System Time Sync" clock mode (section 3.6.1.5).

Details on the configuration can be found in Appendix 8.0 of this manual.

Time Stamps derived from the NTP protocol allow stable time alignment in the millisecond range, which is more than sufficient in MFN applications.

Please note that NTP is unsuitable for carrier frequency synchronization (SFN).

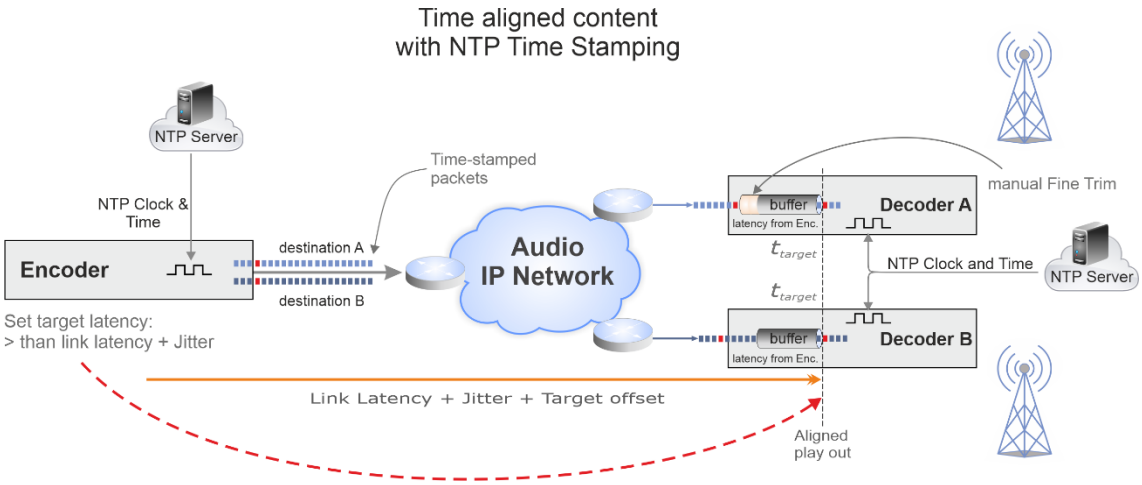


Figure 3-102 shows the principle of time aligned content playout in MFN networks

3.6.3 Network Alarms

This page provides the option to control the network-relevant alarms.

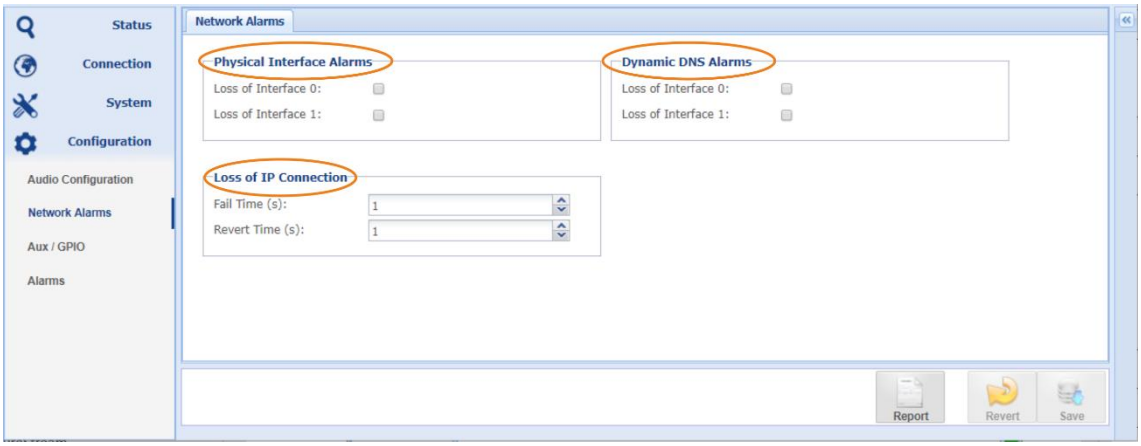


Figure 3-103: Configuration options of network alarms

Enable/Disable alarms for physical loss of connections.

Once both ETH ports have been connected to the network, this state is registered and stored as the default state until the next reboot. This alarm indicates the loss of a physical connection when activated here.

Enable/Disable alarms of Dynamic DNS connection

With this alarm, the connection to a DDNS server can be monitored, and the loss of DNS connection can be displayed; this option is disabled by default.

Loss of IP Connection

The alarm for the loss of an IP connection is managed in the general alarm configuration. The response behavior can be controlled here. Loss of IP Connection indicates that the de-jitter buffer is empty. This state can, under unfavorable conditions, be quickly intermittent and lead to a cascade of alarm messages. The adjustable delay of the repeat periods in seconds can suppress the cascading of the same message.

Notes:

3.6.4 AUX/GPIO Configuration

This page manages the Switch Inputs (GPI), the relay behavior (GPO) and the Aux data rate settings for AUX channel 1 ns AUX channel 2.

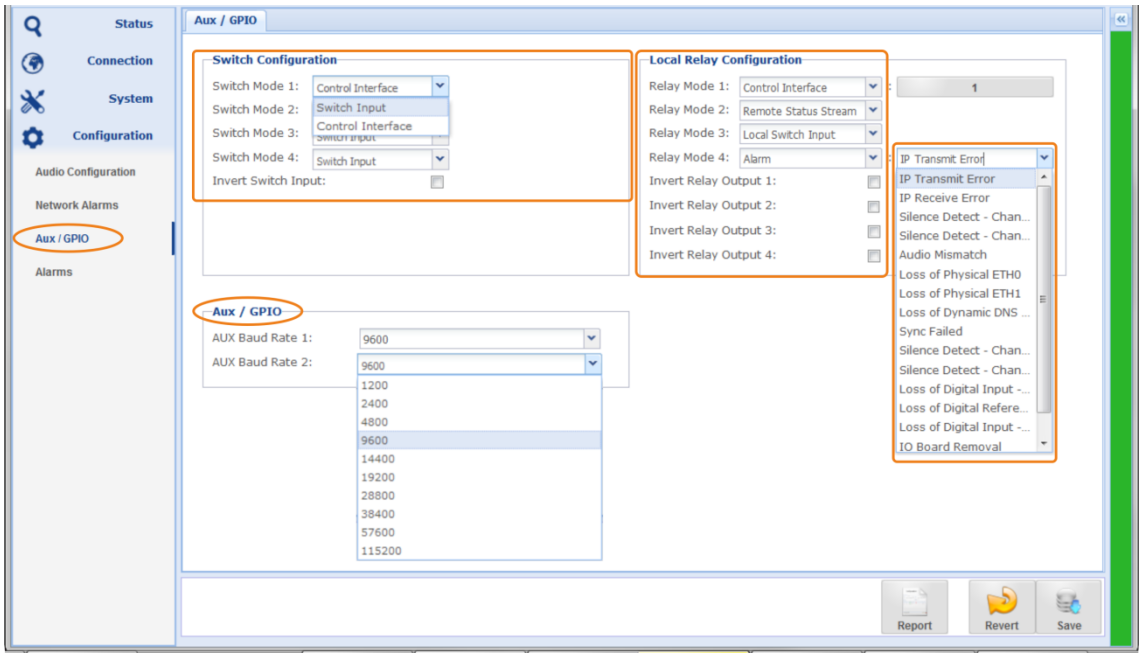


Figure 3-104 shows the AUX Data and GPIO configuration page with all options

The GPIO system consists of four relay contact closures and four opto-isolated switch inputs.

The input source for the opto-isolated switches can be selected to be either the D-Type connector on the rear panel of this unit or a button on this page. This is for each switch input selectable individually. A checkbox allows you to invert the switching behavior (all with one checkbox).

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.*

ⓘ *In embedded mode, the AUX data input 1 and 2 are assignable to stereo signals A/B or C/D. 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

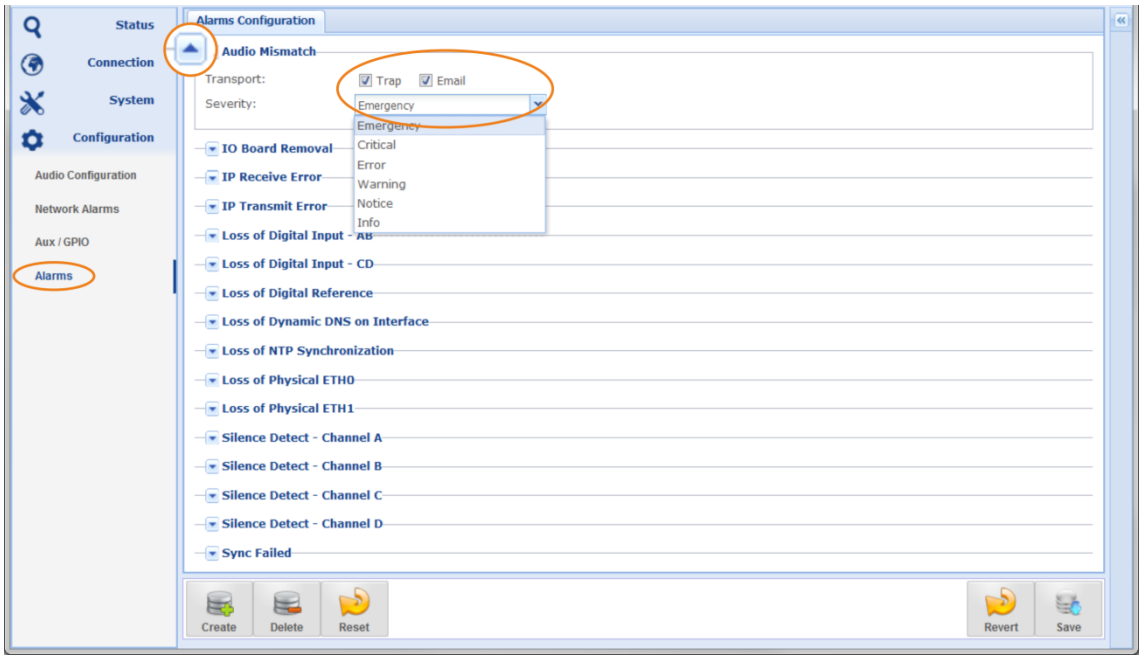


Figure 3-105 shows the Alarms Configuration page

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 3.5.9.

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.

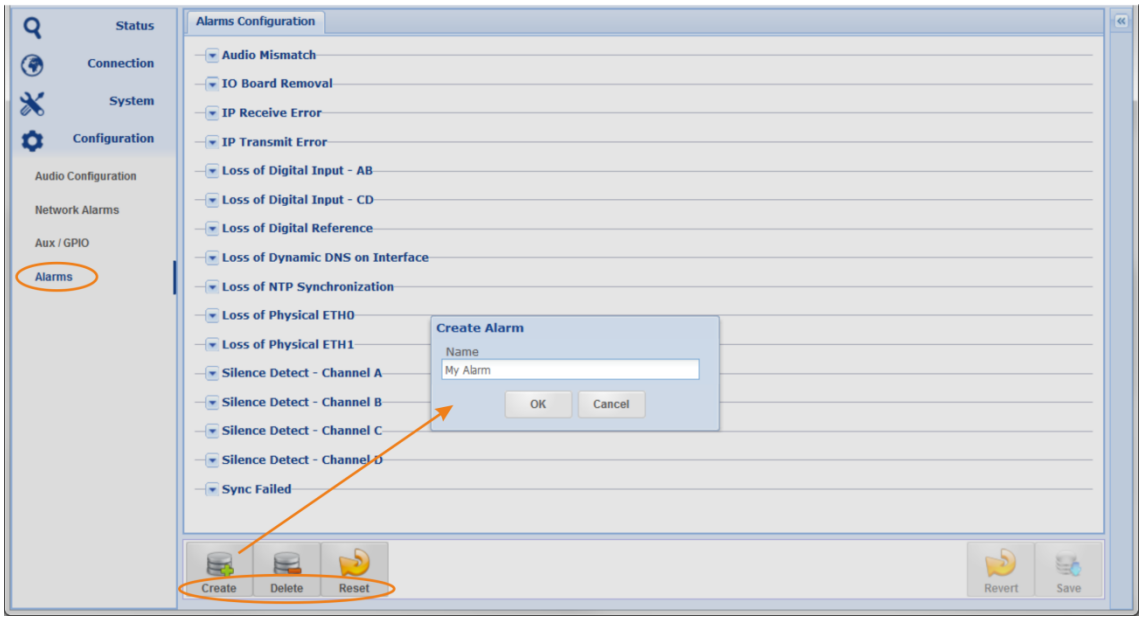


Figure 3-106 How to create a group of Alarms - apply a name to the new group and save it

- 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.

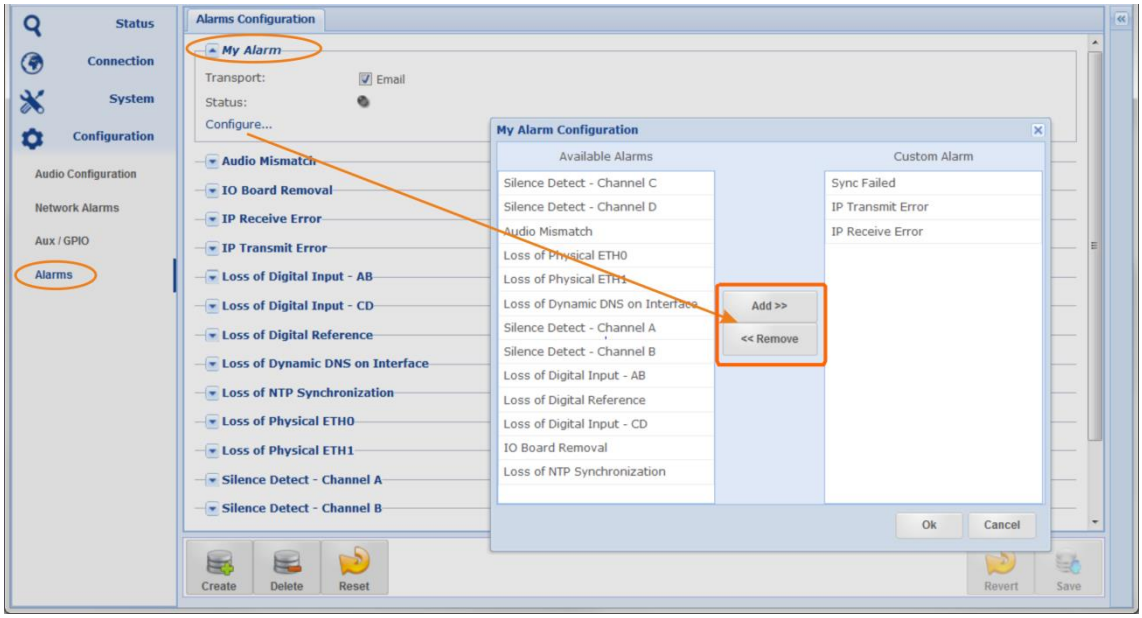


Figure 3-107 shows how to create an alarm group

- 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 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 AoIP Codec module when accessed from the NMS family tree view. The presentation of the GUI of the AoIP Codec Module is the same when opened in the family tree view (NMS) or directly from a WEB browser.

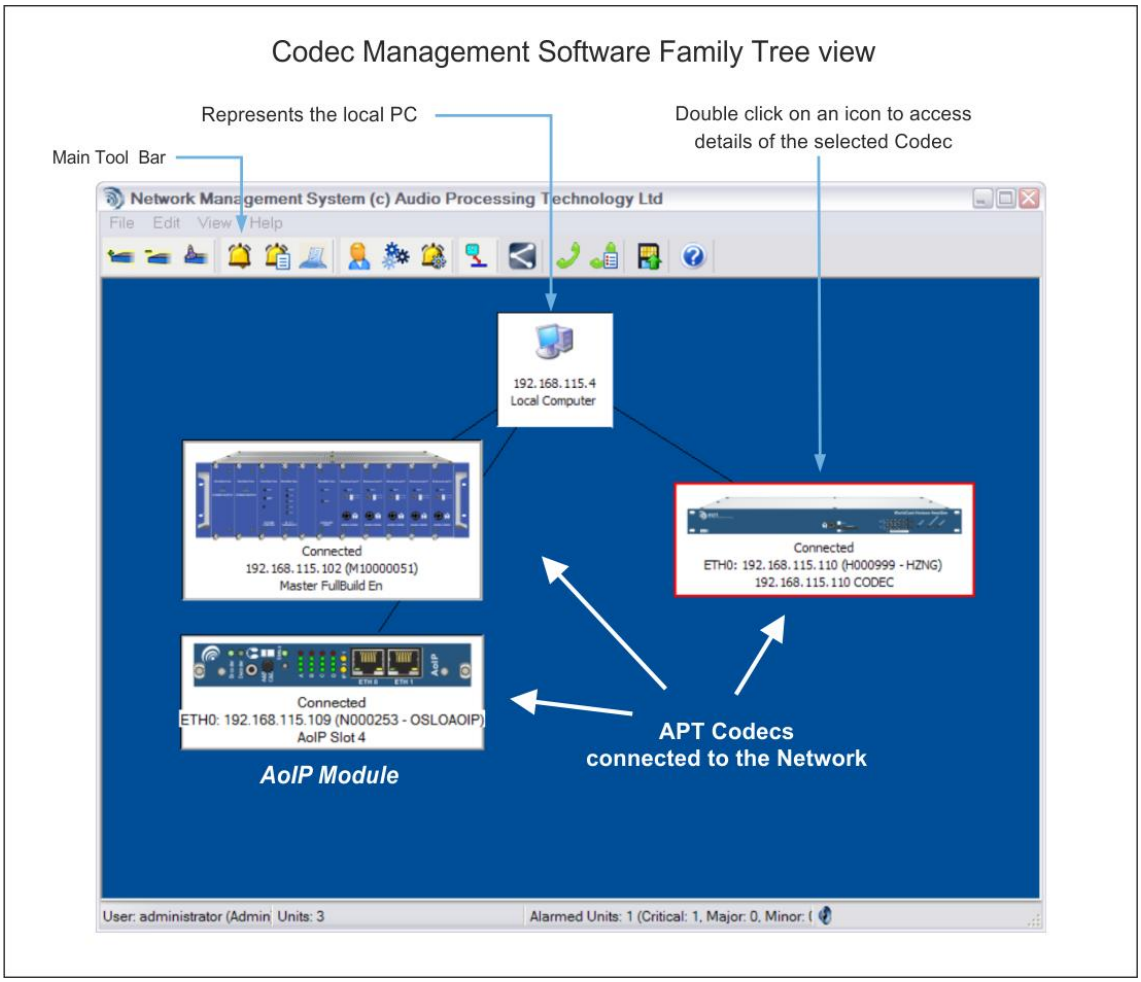


Figure 4-1 Family Tree of the Network Management System (NMS)

ⓘ *The presentation of the* AoIP Module *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:

4.1.1 Installing the Network Management System

Download the latest NMS from the WorldCast Systems Website. You need to logIn to your account: www.worldcastsystems.com/en/account/documents

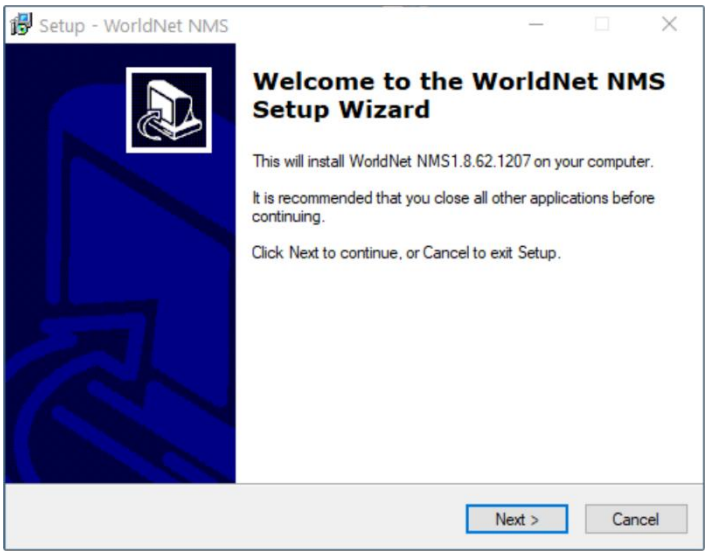
ⓘ Running any NextGen-Codec with the current system release on the NMS software requires the NMS build version **# 1212** or higher.

ⓘ ***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:

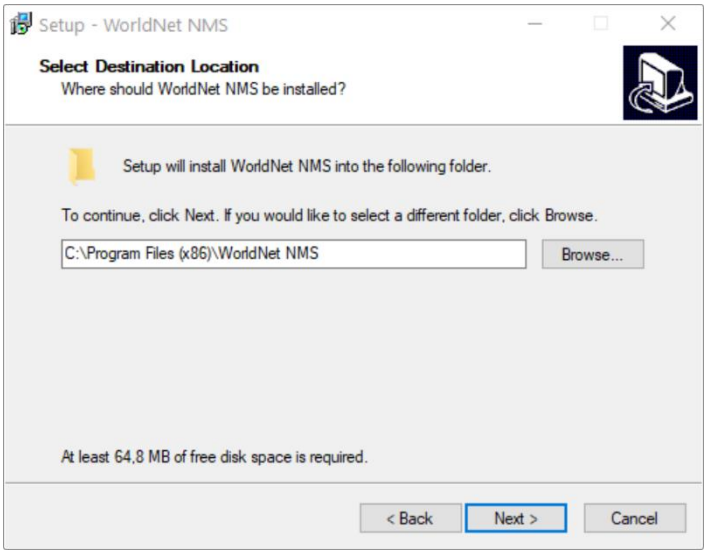
First Screen

It shows the NMS build version; please make sure that the NMS version is compatible with your current firmware.



Next Screen

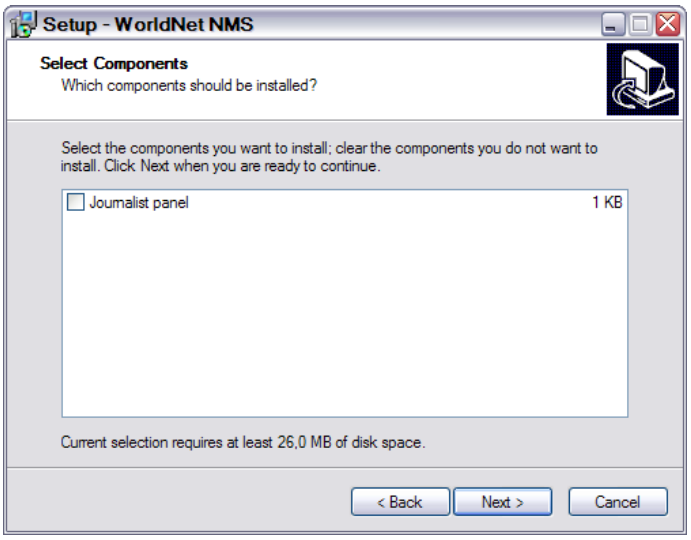
Please choose the folder where you like to install the NMS application.



Installing the Codec Management System *(continued)*

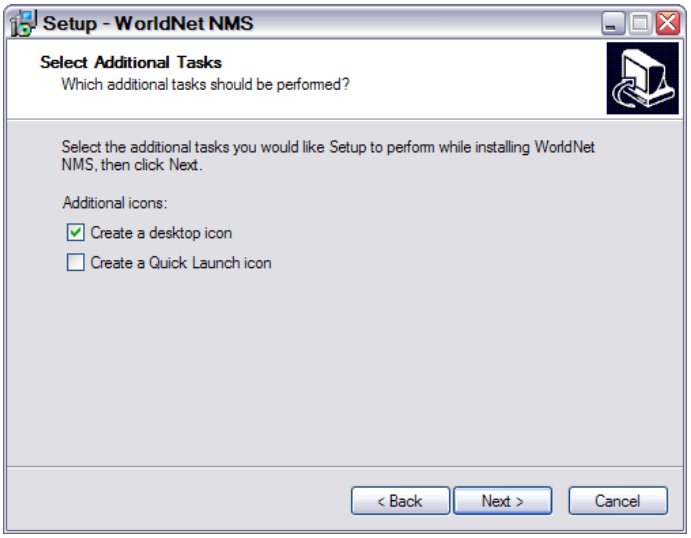
Next Screen

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



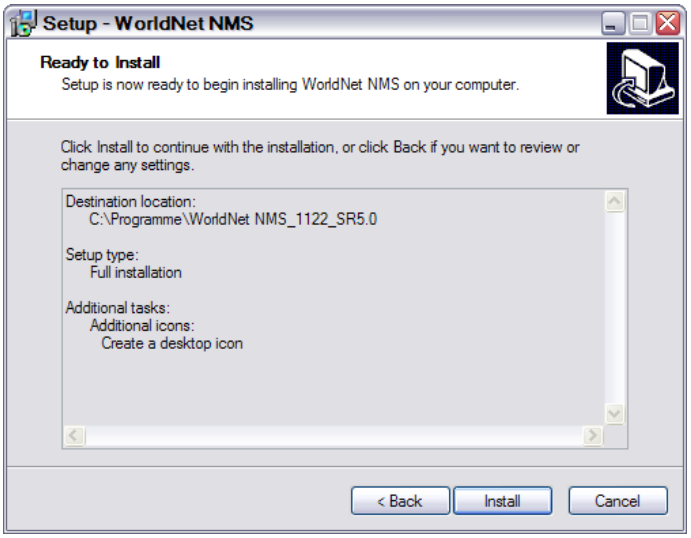
Next Screen

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".



4.1.2 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 WIN 10 Start-Menu in the folder "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 electronic 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."

5.0 Hardware Options

5.1 Analog MPX for AoIP Codec Module (MPXoIP)

The latest development of another input/output module for the AoIP main module now allows the transmission of analog MPX signals. The new interface card provides analog MPX inputs and/or outputs. The current version of firmware supports the duplex mode as well as the dual Encoder or Decoder modes.

ⓘ *The analog MPX input/output card requires firmware v2.0-MPX or higher.*

5.1.1 MPXoIP - Performance and Operational Modes

- Dual Encoder mode
- Dual Decoder mode
- Duplex mode
- Linear transmission with 16 Bit and 24 Bit resolution
- Sample frequency selectable 128 kbps (64 kHz) or 192 kbps (88 kHz)
- IP Packet time max: 3 ms at 16 bit, 2 ms at 24 Bit (max packet size 1152 bytes)
- Overmodulation Cancellation Algorithm for minimizing negative effects of packet losses on the FM deviation (protects against over-deviation)
- Fully compatible with existing protection mechanisms like SureStream and IP packet forwarding
- Headphone monitoring of L+R/2 (mono mix)
- AUX Data and GPIO support

More technical specifications are listed in the specification table in section 7.0 .

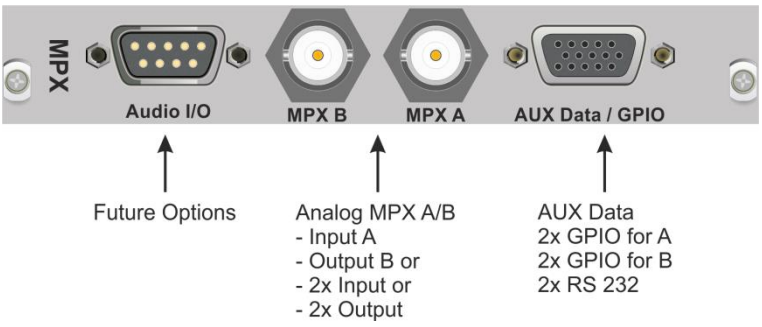


Figure 5-1 shows the rear panel components of the new analog MPX input/output module (with a future option of monitor return streams).

The signal flow on the BNC connectors is software controlled. BNC A and B can be configured as 2x inputs (dual Encoder), 2x outputs (dual Decoder) or 1x Input and 1x output (Codec).

5.2 Analog MPXoIP WEB GUI

The Codec main board supports the standard audio interface and the analog MPX input/output board; the WEB GUI is nearly the same for both variants. The main board automatically detects the type of interface that is connected to the main card. The current type is displayed on the status page, and the GUI provides only the MPXoIP configuration options to the user.

5.2.1 Main Menu – Status

In the previous chapters, all common functions have already been described; this part shows you how to use the analog MPX module.

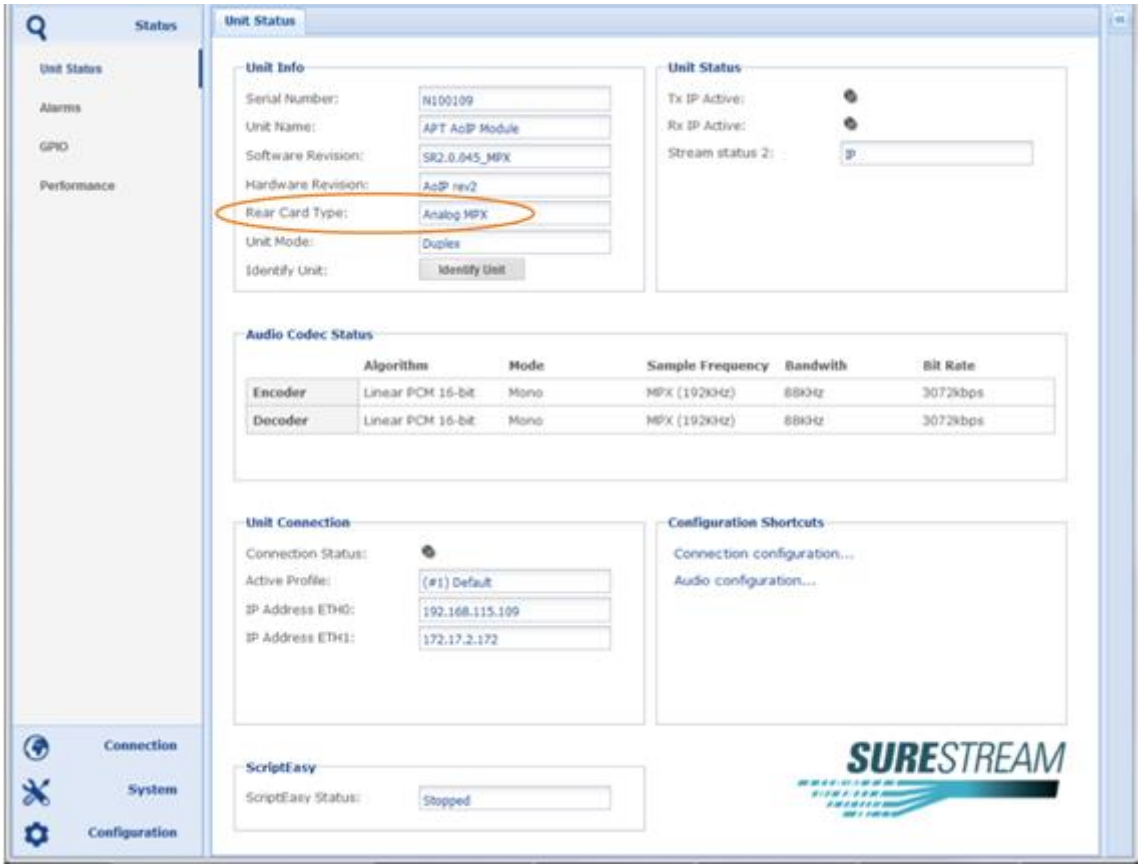


Figure 5-2 shows the status page of the unit with the analog MPX rear module detected.

The status page of the MPX version displays the detected Rear Card Type and the general status information.

5.2.2 MPXoIP Formats

On the stream configuration page, the MPX version of the firmware provides only the analog MPX modes. The configuration of the MPX formats is described in section 3.4.19.

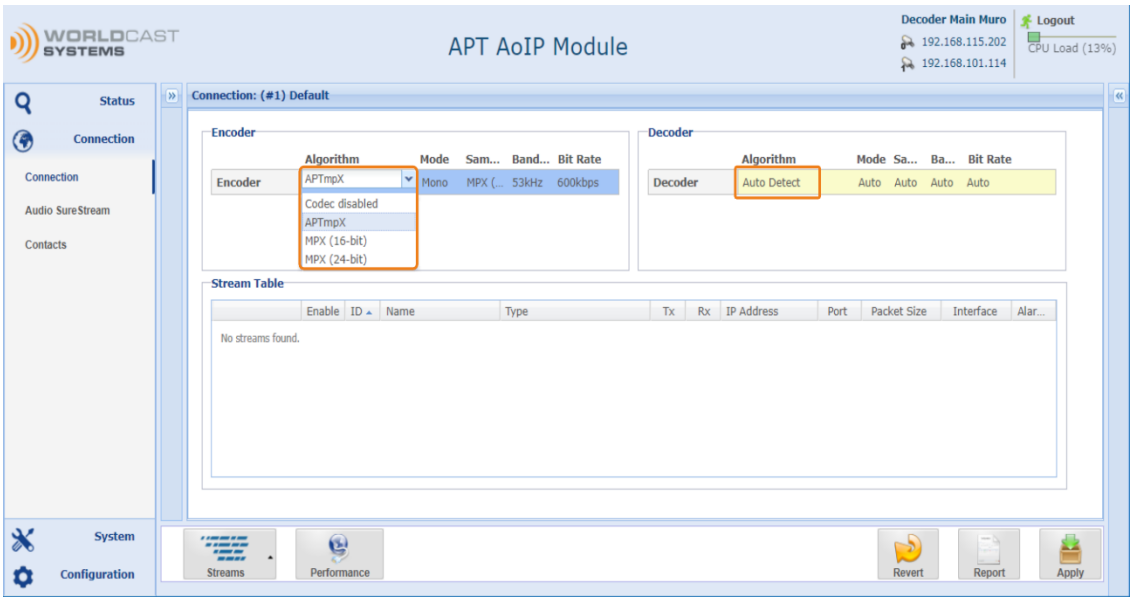


Figure 5-3 the algorithm list only provide the MPX options. This screenshot shows the duplex mode.

The analog MPX interface does not support embedded data; therefore, the option is not presented. The procedure of stream configuration follows exactly the instructions in section 3.4.11 and following.

The Encoder and the Decoder provide the same MPX formats, and, in addition, the Decoder supports the "Auto Detect" mode. Selecting this mode auto-configures the Decoder to the format of the incoming stream.

Notes:

5.3 MPXoIP Applications

5.3.1 Analog Input / Analog Output in duplex mode

The image below shows an application for analog MPX transmission for a single program. Configuring the MPX Codec in duplex mode supports a return path if required.

Effectively the analog MPX signal path works like a normal mono feed and could be used for baseband audio as well (confidence monitoring, etc.).

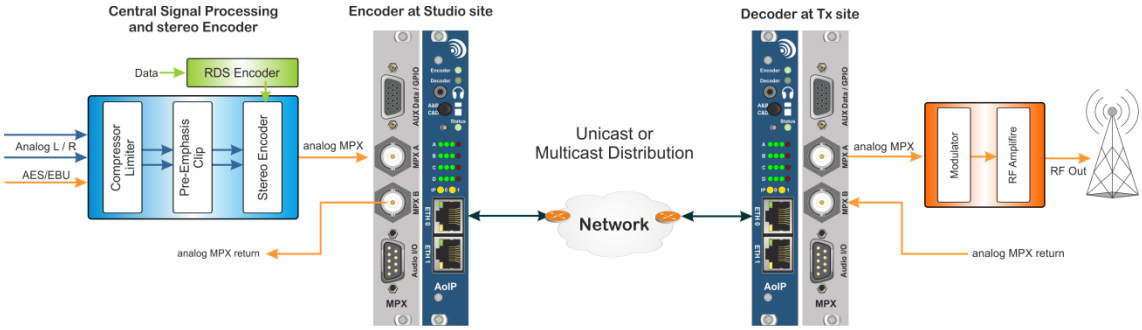


Figure 5-4 shows an analog MPX signal path for a single program - cards set to Mono Mode

5.3.2 Dual Analog Encoder / Decoder

This application utilizes the dual Encoder capacity of the analog MPX module by feeding two programs to a transmitter site.

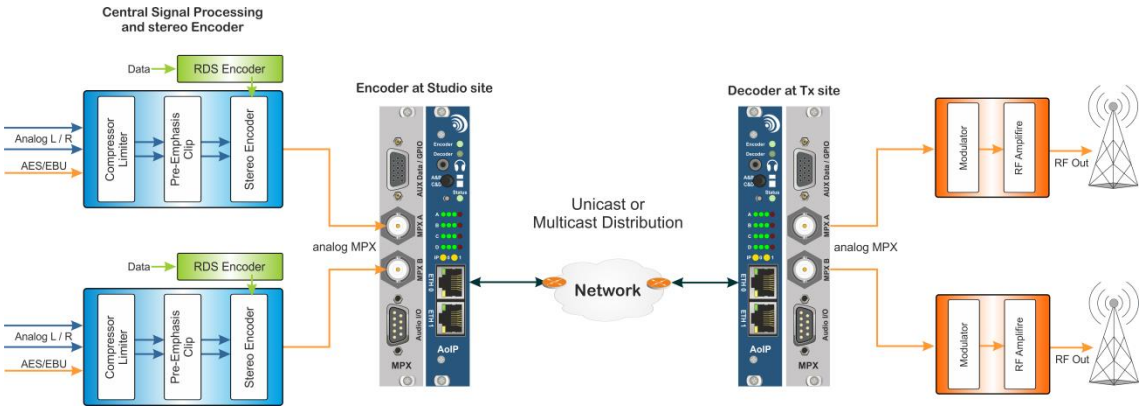


Figure 5-5 shows the analog MPX signal path for two programs - cards set to Simplex Mode

5.3.3 Analog Encoder - multiple Tx Sites

In this application, the Encoder transmits the same analog MPX signal to two transmitter sites utilizing multiple unicast or multicast mode.

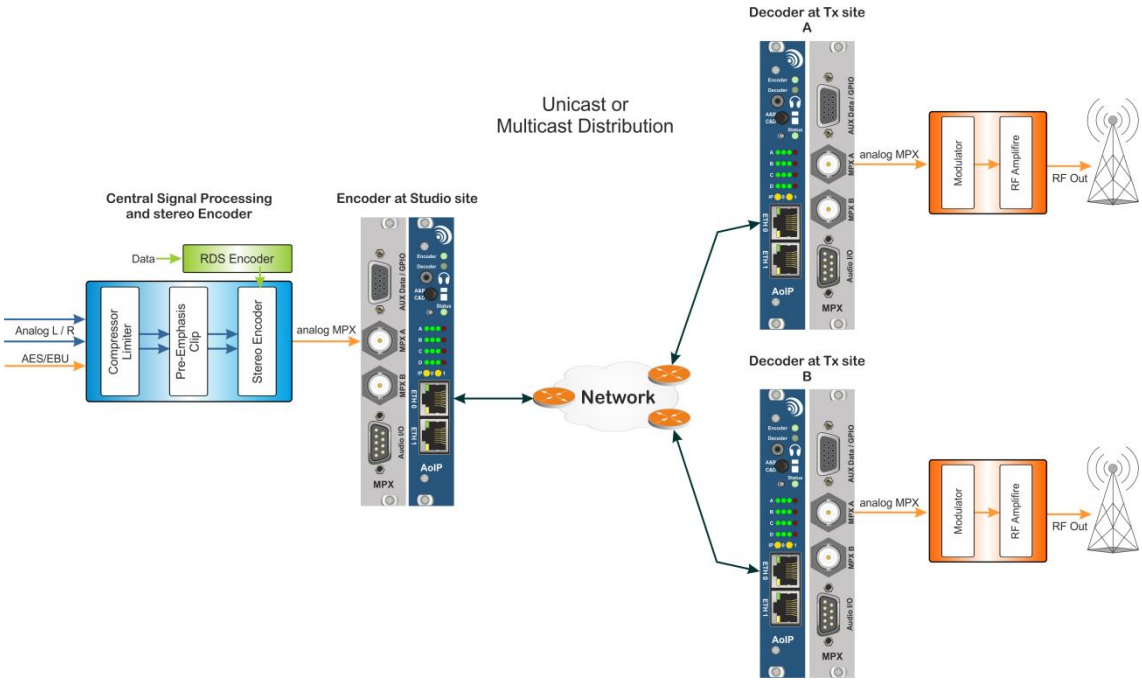


Figure 5-6 shows the typical analog MPX signal path of one program to multiple transmitter sites.

5.3.4 Digital Encoder – Analog Decoder

In this application, the Encoder receives digital MPX over AES at the input. At the transmitter site, an analog MPX interface feeds the signal to the analog transmitter.

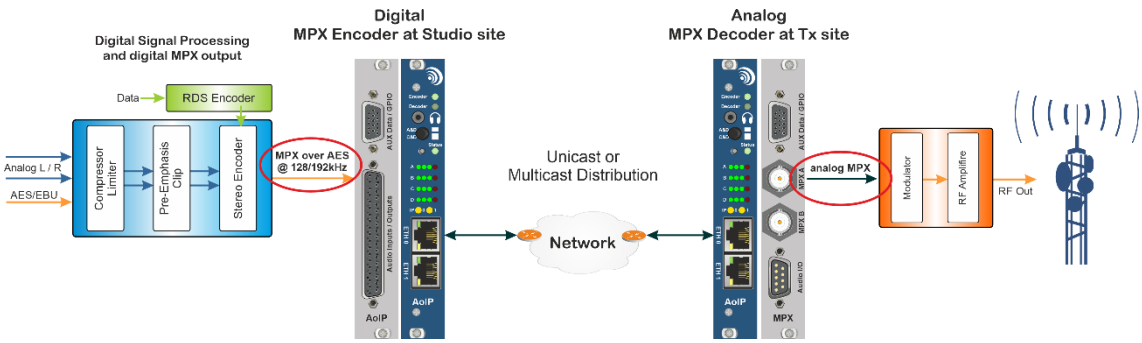


Figure 5-7 shows the digital MPX input at the studio and the analog MPX output transmitter sites

6.0 Specifications - AoIP and MPXoIP

Order Codes	
STP00034 (AoIP 4HP)	**4HP** kit of AoIP Main Board and AoIP Rear Panel – including XLR breakout cable (for 1U chassis)
STP00055 (AoIP 6HP)	**6HP** kit of AoIP Main Board and AoIP Rear Panel – including XLR breakout cable (for 3U chassis)
STP00050 (AoIP 8HP)	**8HP** kit of AoIP Main Board and AoIP Rear Panel – including XLR breakout cable (for 3U chassis)
STP00060 (MPXoIP 4HP)	**4HP** kit of AoIP Main Board and **analog MPX** Rear (for 1U chassis)
Physical	
Dimension	Euro PCB format, compliant with the EU ROHS directive; main board with Input/Output on the separate rear panel
Analog Interfaces	
Interface Type	electronically balanced, capacitive isolated physical: on 37-pin D-Type connector (via XLR breakout cable)
Audio channels	Simplex Mode: 2x Stereo-Input **or** 2x Stereo-Output Duplex Mode: 1x Stereo-Input **and** 1x Stereo-Output (analog and digital outputs are simultaneously available)
Analog I/O impedance	High >10 kΩ/Low <50 Ω or 600/600 Ω (by jumper settings)
Modes of operation	Stereo, Dual Stereo (simplex), Mono, Dual mono (simplex)
Audio characteristics	Analog Input to output: clip level: +18 dBu (0dBFs), 0 dBu to +18 dBu adjustable by 0.1 dB increments
Digital Interfaces (AES/EBU)	
Interface Type	AES 3: transformer balanced, or AES unbalanced (compatible with 75 Ω interfaces) physical: on 37-pin D-Type connector (via XLR breakout)
I/O impedance	AES 3: 110 Ω
Audio channels	Simplex Mode: 2x AES Input **or** 2x AES Output Duplex Mode: 1x AES Input **and** 1x AES Output
Modes of operation	Stereo, Dual Mono, Dual Stereo
Output sampling rates	32/44.1/48/96/192 kHz – software configurable
AES Reference	AES-11 reference input – per AoIP card or for the whole chassis
SRC	Sample Rate Converter at Inputs and Outputs

General	
Diagnostics	Local loop back Integrated Test tone generator Ping Tool for each ETH interface
Audio Modes	Mono, L&R/2 on encoder and decoder, MonoFill mode on decoder which copies a mono channel to both outputs; Stereo
Audio Bandwidth	10 Hz – 22.5 kHz and 88 kHz for digital MPX (optional)
Dynamic Range	Up to >110 dB @ 24 Bit
Signal Processing	24 Bit Audio processing
Silence Detection	Advanced Silence Detector on four channels, fail-time- threshold-level- and recover time settings for each channel.
SD Card Supported File formats	SDHC – no size limitation FAT 32 format .wav linear PCM .mp2 for MPEG 2 Layer II .mp3 for MPP3 files (VBR & CBR) .aac for AAC files with ADTS header (only)
ALARMS	
Silence Detectors (program loss) IP Alarms Power Supply	4 Alarms (L&R IN/Out) fail Time: 1 to ∞ sec. revert Time 0 to ∞ sec. Threshold level: -3 to -42dBFs Transmit and Receive error Alarms Failure on Power Alarm
DATA	
AUX Data Interface	RS 232, 2 channels per module parameter setting 8-N-1 (1 start/stop, no parity, 8 bits), no flow control
Aux data Mode	Embedded up to 9600 Baud Non-embedded up to 115200 Baud
Data Rates	embedded & non-embedded:1200/2400/4800/9600 non-emb.: 14400/19200/28800/38400/57600/115200 Baud
GPIO	Non-embedded: 4x opto-isolated switch inputs (2x per stereo) embedded: on aptX® Enhanced only
Relay contacts	4x relay contacts carried out as 2 pin switches, normally open to common – 2x per stereo signal

Audio Formats and Coding Algorithms	
Linear PCM	Fs = 32 kHz, 1024/1536 kbps (16/24Bit stereo) Fs = 48 kHz, 1536/2304 kbps (16/24 Bit stereo)
Optional: Digital Linear Composite/MPX	3072/4608 kbps, 16/24 Bit, MPX bandwidth 88 kHz 2048/3072 kbps, 16/24 Bit, MPX bandwidth 64 kHz (Audio/RDS)
Digital Compressed APTmpX	900 kbps, bandwidth 64 kHz (Audio/RDS) 600/400/300 kbps, bandwidth 53 kHz (Audio only)
apt-X® Enhanced	Sampling rates: 8/16/24/32/48kHz Bit Resolution: 16/24 Bit Bit Rates: 64 - 576 kbps
OPUS	Bit Rates: 64/96/128/256/384 kbps stereo Bit Rates: 32/48/56/64/96/128/256 kbps mono Fs 48 kHz
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-AACv1 HE-AACv2	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. 21.3ms	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
OPUS	20 ms	fixed

IP – Audio Streaming – IP Forwarding	
Casting Modes	Unicast, multiple unicast multicast, multi-multicast, source-specific multicast (SSM)
Stream Types	Audio (RTP/UDP): 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 Streams	Forwarding of any data, like EDI for DAB transmitter along audio streams with or without SureStream protection
Unit Clock Modes	Asymmetrical: Encoder/Decoder on separate audio modes/clocks/networks Master: System Clock Slave: Clock derived from VCXO System Time Sync: Metronome Clock from NTP source
De-Jitter Buffer Size	from 1 ms to 5000 ms independently per stream
Streaming	Tx Stereo audio, n number of IP-streams Rx Stereo audio
Asymmetrical audio Master/Slave System Time Sync	Encoder/Decoder on separate audio modes/clocks/networks Master/Slave Mode (Master clocks Slave) External System Time reference (NTP)
Auto-Detection, Auto-Configuration	Auto-detection of the incoming stream on receive-streams. Auto-Configuration of decoder settings
QoS, RFC 2474 	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) - SIP (port 5060) - SNMP (port 161) - SNMP Traps (port 162)
Secure HTTP	WEB GUI access via HTTPS as standard, TLS 1.1 and higher

IP – Interface and Protocols	
IP Interface Physical	Dual IP ports, 2x RJ 45 for streaming and/or management
IP Interface electrically	Separate PHY per interface 2x MAC addresses 2x network address settings Port speeds: 10/100 BaseT/Tx, Full Auto, 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
SIP/SDP	Session initiation protocol, Session description protocol
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, WorldCast Manager
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)

ANALOG MPX I/O Module (MPXoIP)	
Linear PCM for MPX	Fs = 192 kHz, 3072 /4608 kbps, 16/24 Bit mono, full MPX bandwidth 88 kHz Fs = 128 kHz, 2048 /3072 kbps, 16/24 Bit mono, MPX bandwidth 64 kHz (audio & RDS)
Coding Delay Link Delay	< 12ms variable (depends on network performance and de-jitter buffer)
Stream Types	Mono Audio (RTP): dual Encoder, dual Decoder or Duplex Mode
MPX Bandwidths	20 Hz to 88 kHz or 64 kHz suitable for audio &: RDS (57 kHz) SCA-1 (67 kHz) - 88 kHz mode only DARC (76 kHz) - 88 kHz mode only
Frequency Response	20 Hz to >60 kHz +/- 0.05 dBu
Stereo Separation	avg. 57 dB
THD+N	10 Hz to 40 kHz = -77 dBu 10 Hz to 80 kHz = -60 dBu
APTmpX (compressed)	900 kbps, bandwidth 64 kHz (Audio/RDS) 600/400/300 kbps, bandwidth 53 kHz (Audio)
MPX In/Out	2x BNC 75 Ω unbalanced (balanced – future option)
Input Level	+16 dBu clip level = 0 dB Fs, adjustable +10 to +16 dBu in increments of 0.025dBu
QoS, RFC 2474 SURESTREAM	DiffServ with distinct DSCP values per stream; Differentiated Services Code Point for packet classification purposes Overmodulation Cancellation of FM carrier due to packet losses SureStream Technology, based on redundant packet streaming (Statistical Stream Diversity) – license option
Management and Monitoring	
Management	Via WEB GUI, SNMP, NMS and API
Network Monitoring	Performance Monitor per Stream, displays: - Name of Stream - Rx/Tx Packet Interval – pkts/sec, p-time (packet time) - Rx/Tx Packet size in bytes - Rx/Tx bitrate in kb/s - Rx/Tx number of sent/received bytes - Source IP address of Rx stream - Source IP port on Rx stream - Number of dropped Rx packets - Duplicated packets - Re-sequenced packets count - Flooded buffer count - Loss of Connection events - De-Jitter buffer size and actual data level - RX port number - Physical port (ETH 0/1)
ScriptEasy	Allows customizing of features, e.g., backup scenarios with independent SNMP agent and manager for five connections

7.0 Appendix A - SureStream Option

7.1 Overview

⚠ 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 3.5.14 (System Licenses).

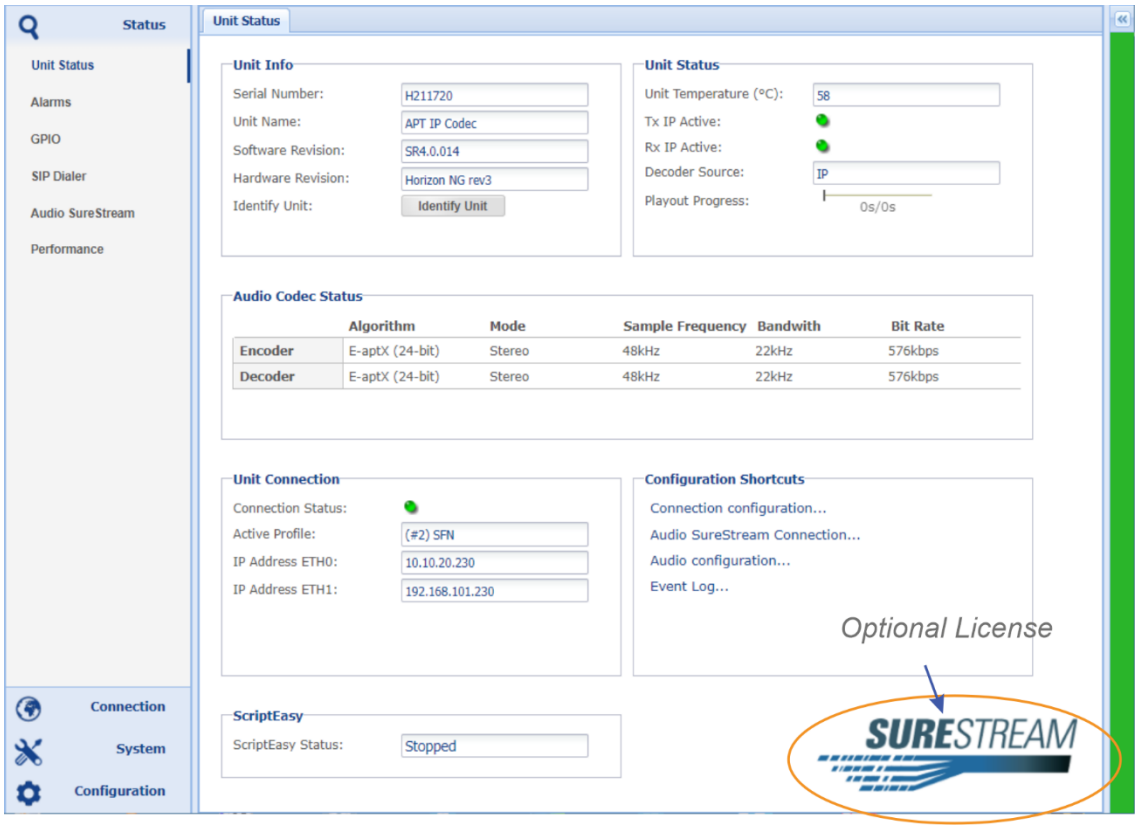


Figure 7-1: Shows the Status Page with SureStream license applied

7.1.1 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.

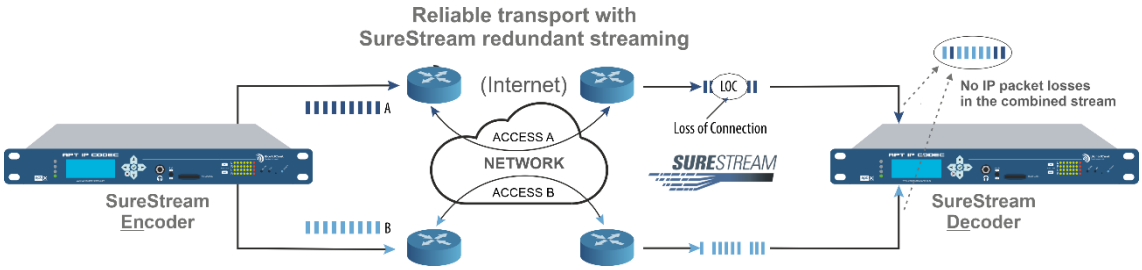


Figure 7-2: Shows a typical Dual Port Configuration with SureStream protection.

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.

7.1.2 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 7-2, the network as such maintains the stream diversity without adding diversity levels.

7.1.3 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 number 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.

7.1.4 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.

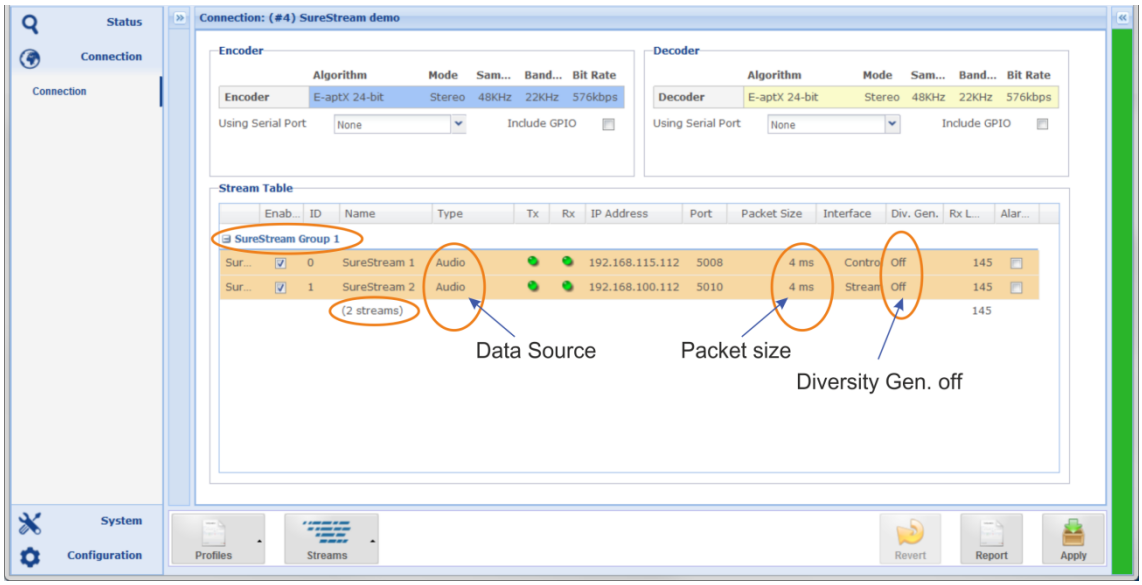


Figure 7-3: Shows a SureStream configuration on the Encoder

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.

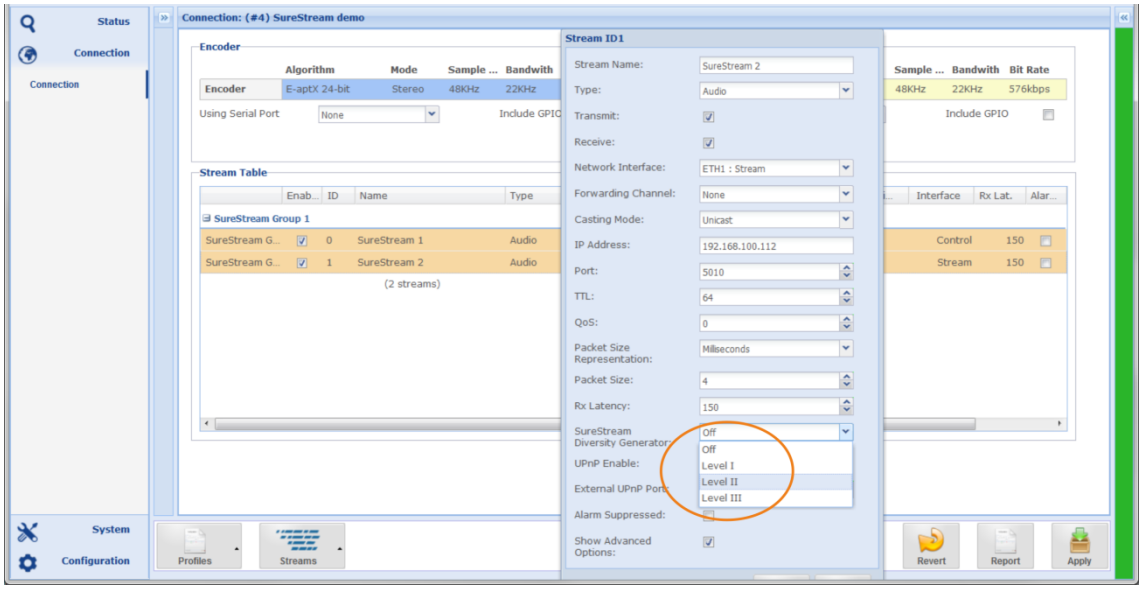


Figure 7-4: Shows the Diversity Generator options on the stream configuration window

7.1.5 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.*

7.1.6 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.

7.1.7 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.

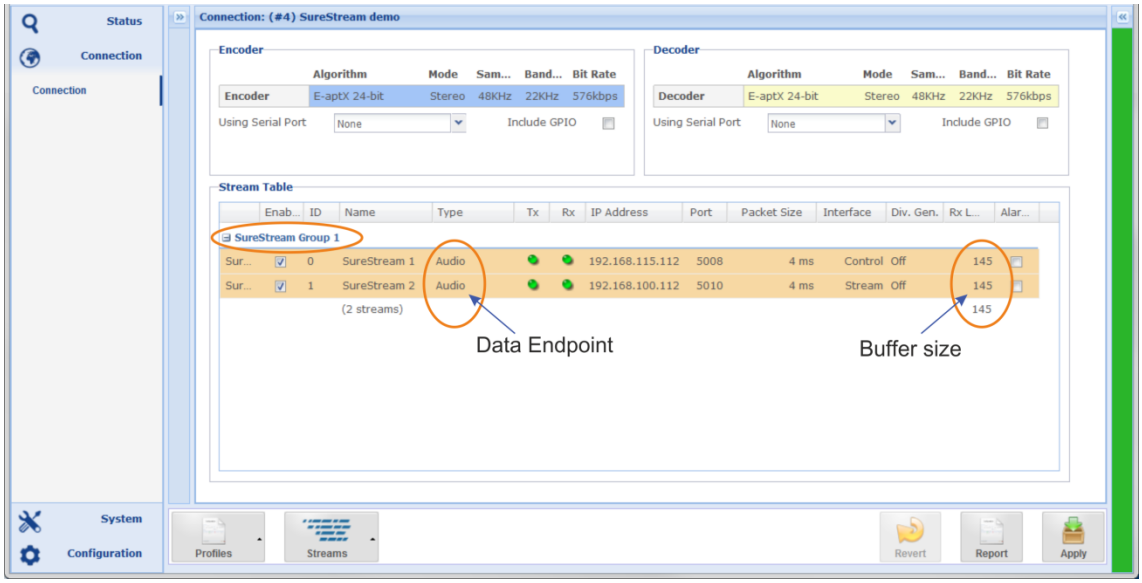


Figure 7-5: Shows a SureStream configuration on the Decoder with two streams received

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).

7.1.8 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 7.1.8.2).

7.1.8.1 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

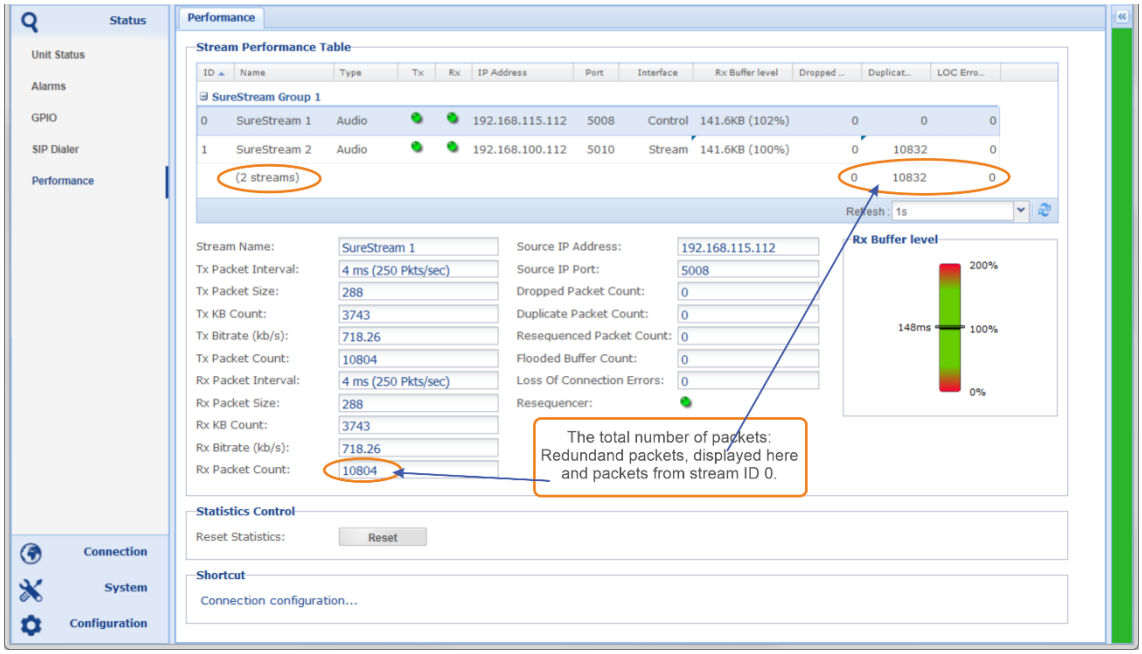


Figure 7-6: Shows the stream performance without a monitor stream

7.1.8.2 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.

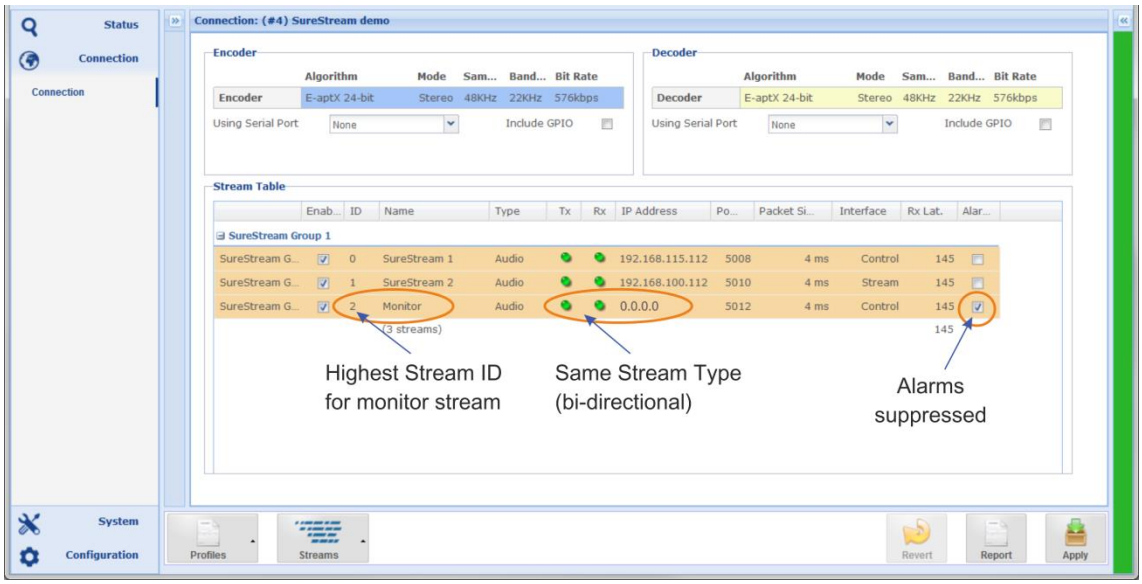


Figure 7-7: Shows a SureStream group with two component streams with a monitor stream

The stream table of the screen shot above is the same configuration as on Figure 7-5 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:

7.1.8.3 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.

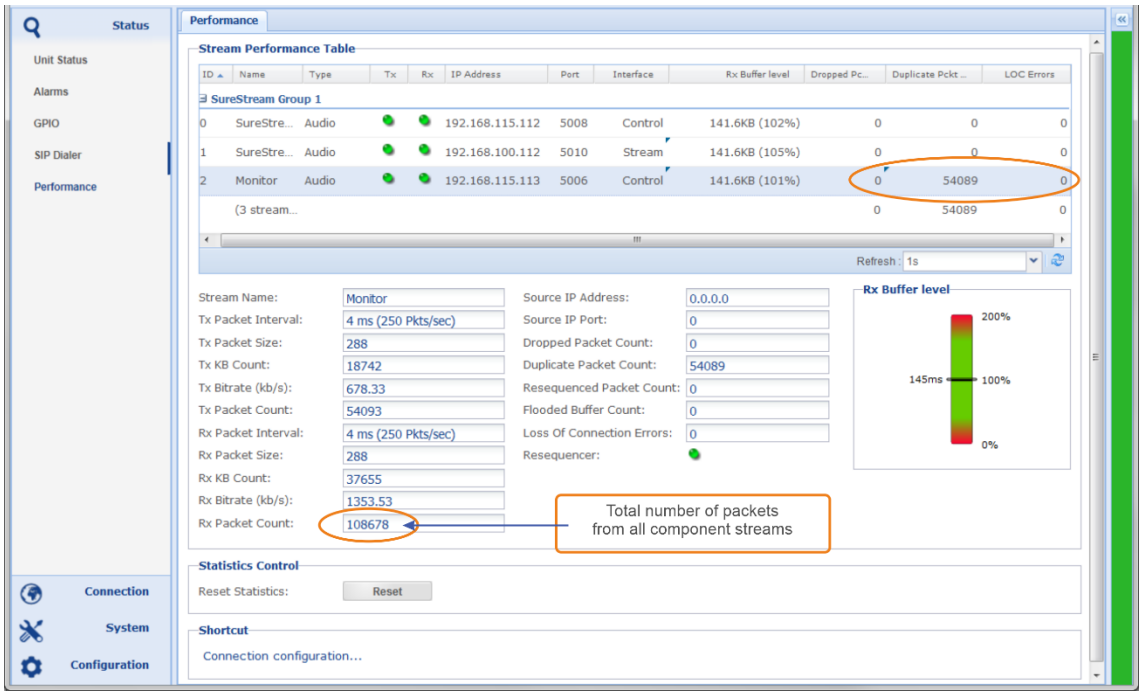


Figure 7-8: Shows the performance of the SureStream monitor stream

The performance figures of the monitor stream present the same IP statistics as described in section 3.3.5.

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:

8.0 Appendix B – FM MFN

8.1 Overview

8.1.1 System Clock with the NTP timing (for MFN)

This function synchronizes the Codec's system clock with the **NTP clock**, which enables the content synchronization of the transmitted programs on different FM frequencies (MFN). The playout time at the decoders is determined by setting a target latency at the encoder. This function can be activated on all generations of APT IP Codecs by a firmware update. A separate license is not required.

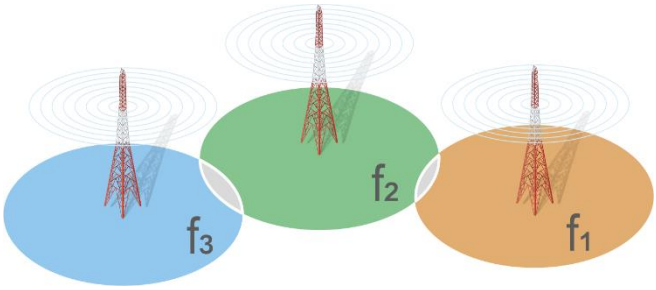


Figure 8-1: Multi Frequency transmitter arrangement

ⓘ ***Important**: The NTP's degree of precision allows an adjustment of the demodulated audio content in the millisecond range. This is sufficient for Multi-Frequency Network (MFN) applications.*

8.2 Application Settings

8.2.1 MFN Application with NTP Time Alignment

The target application is the program time alignment of **a Multi-Frequency FM Network**.

The aim is to adjust the programs' timing so that a transition from one transmitter coverage area to the next is without a noticeable time jump of the decoded audio. In an MFN, we only manipulate the audio time domain to enhance the listener experience.

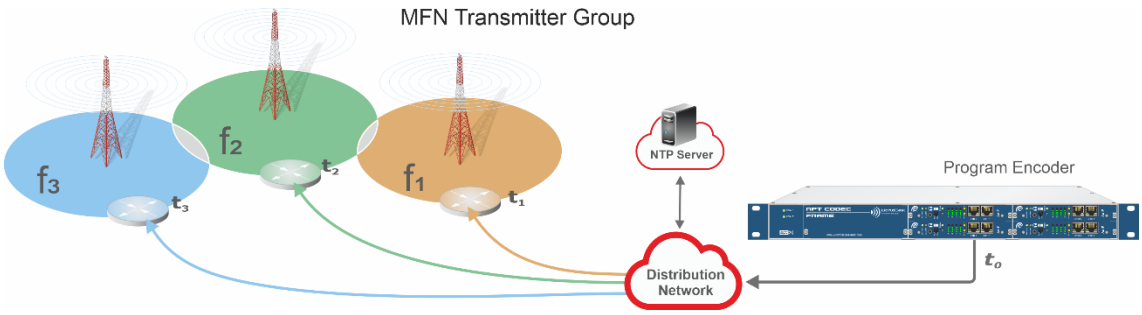


Figure 8-2 shows the different latencies of t1, t2, and t3 that need to be adjusted.

In this example, you must select the target latency higher than the latency of t3 (for f3). Also, you have to consider the value of a sufficient jitter buffer size.

8.2.2 NTP Server

In the System menu page "Date/Time," you must enter and activate an NTP server address. Enter a valid IP address or hostname of the NTP server and enable it ("Yes"). This setting must be configured in the Encoder and all Decoders.

After the NTP client has synchronized to its time reference (NTP server), the NTP LED turns green. It is essential to wait for time synchronization before you establish the IP streams.

You can **enter more than one NTP IP address** or hostname in this field separated by commas, e.g., "216.239.35.0,216.239.35.81", etc. (no blanks in between the entries).

Make sure that you use NTP servers with a stratum (layer) higher than "10", where "higher" is represented by a lower number in the stratum hierarchy. The highest stratum, therefore, is "1". A higher stratum result in higher NTP precision.

Google time servers, e.g., are on stratum "1" (time.google.com, time1.google.com, etc.). The internal clock of the codec is associated with stratum "10".

The Diagnostics page in the System menu offers an NTP monitoring tool, which allows you to see both the resolved IP address of a hostname and the stratum level, among other parameters.

ⓘ *Information about the **NTP Monitor tool** can be found in section 3.5.8.2.*

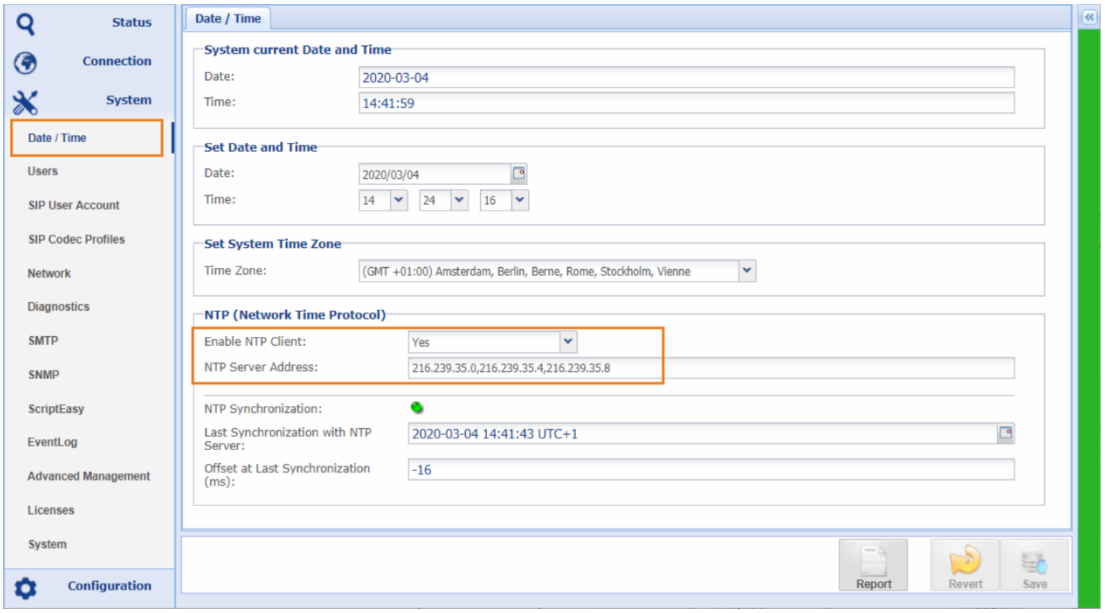


Figure 8-3 highlights the NTP server entries in the System Menu (Date / Time submenu).

8.3 Unit Clock Modes

Open the "Configuration Menu," navigate to the "Advanced Options," and select "Unit Clock Mode." Use this setting to define the clock and/or time reference for creating timestamps.

Use the "System Time Sync" option for NTP synchronization in **MFN** networks

*You must set the **Unit Clock the same** on all devices belonging to the same MFN network (Encoder and Decoder)!*

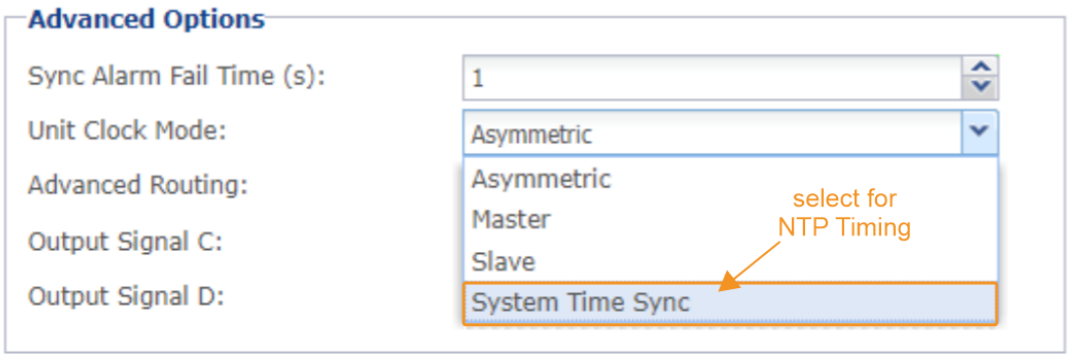


Figure 8-4: Shows the options of the unit clock mode

8.3.1 Codec Settings (all Clock Modes)

The configuration of the codecs (encoder and decoder) does not differ for the setup of an MFN network.

At the **encoder** you set the target latency **for all decoders**, which compensates for the dynamic latencies of the network.

The selected general target latency ensures that the audio is played out at all decoders simultaneously. You can add or subtract an individual trim offset at the decoder to match the transmitters to each other.

8.3.2 Configuration of the Encoder Streams

The stream configuration at the **Encoder** (Tx stream) offers new options to control the latency of the link, which effectively represents the total latency of the connection.

① First, enable the "**Link Latency Management**." After you have activated this box, the input field "Target Latency (ms)" appears. It allows setting increments of full milliseconds.

② The value entered here determines the **total** latency of the transmission path, **including the Decoder's jitter buffer**. You must set the target latency high enough to ensure an appropriately large jitter buffer on the link with the highest latency.

The application in Figure 8-2 indicates three latencies (t1, t2, t3). The reference point in this figure is t3 (highest link latency). The size of the required jitter buffer at t3 determines the minimum target latency.

Each stream in the MFN should be configured with the same target latency. Individual adjustments can also be made to the Decoder.

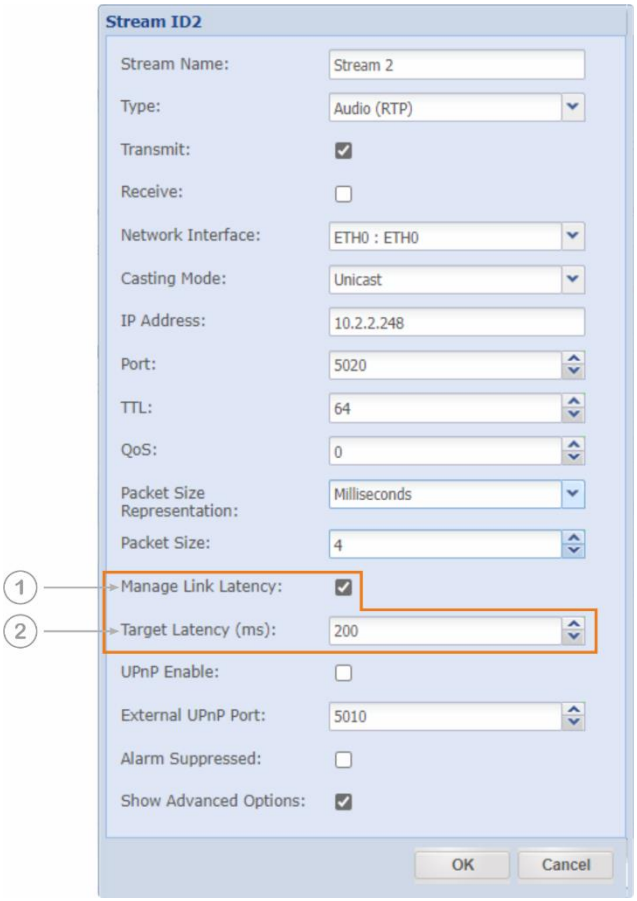


Figure 8-5 shows the latency controls on Tx streams

⚠ Note this:

The value set as Target Latency in milliseconds determines the Decoder's buffer size **minus** the link latency (can be checked with PING). For example, if the highest latency of a connection is 5ms and the Target Latency value is set to 100ms, then the buffer at this Decoder is automatically calculated to 95 ms.

Since the network's latency is not entirely static, the buffer automatically adapts to changed latency conditions to ensure the predetermined target latency.

8.3.3 Configuration of Decoder Streams (Buffer Mode)

The stream configuration at the **Decoder** (Rx stream) offers two new options to enable and control the individual link latency.

① On the option "**Buffer Mode,**" select "Link Latency from Encoder."

This enables the automatic mode of the buffer. In this mode, the buffer calculates and maintains its size dynamically depending on the link latency to reach the predetermined target latency:
Target latency minus link latency = buffer size.

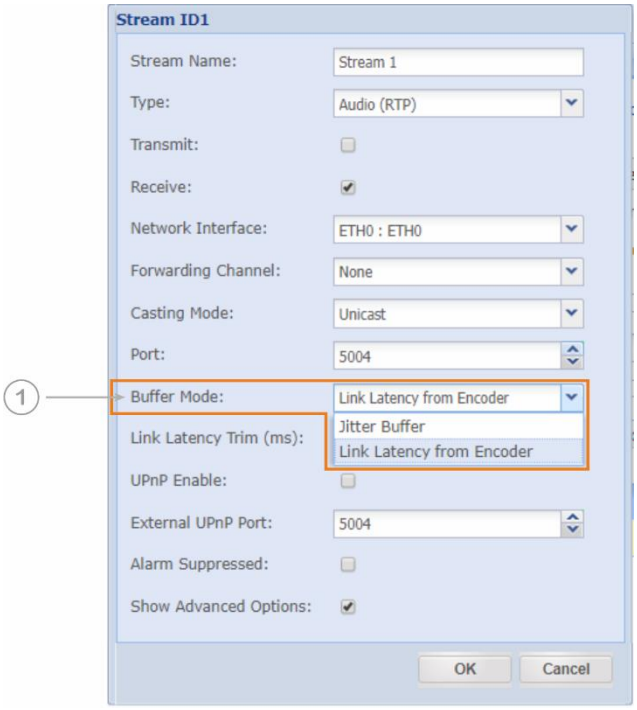


Figure 8-6 shows the latency controls on Tx streams

8.3.4 Configuration of Decoder Streams (Latency Trim)

The Decoder allows an individual adjustment of the target latency using a trim value. The trim value can be positive or negative and adds/subtracts a delay to/from the predetermined target latency.

② If the buffer is set to "Link Latency from Encoder," the input field "**Link Latency Trim (ms)**" appears. You can insert an individual value for this Decoder, which is added or subtracted to/from the target latency. The trim latency allows setting increments of 1ms for NTP timing. In this example, a value of +3 ms has been entered. The total target latency is 203 ms for this Decoder (200ms set from the Encoder).

③ **Minimum Buffer Alarm**, if activated, an alarm is triggered when the buffer size falls below the subsequently entered value (warning in yellow).

Minimum Buffer describes the threshold value of the jitter buffer alarm. If the value falls below the entered value, an alarm is triggered if activated.

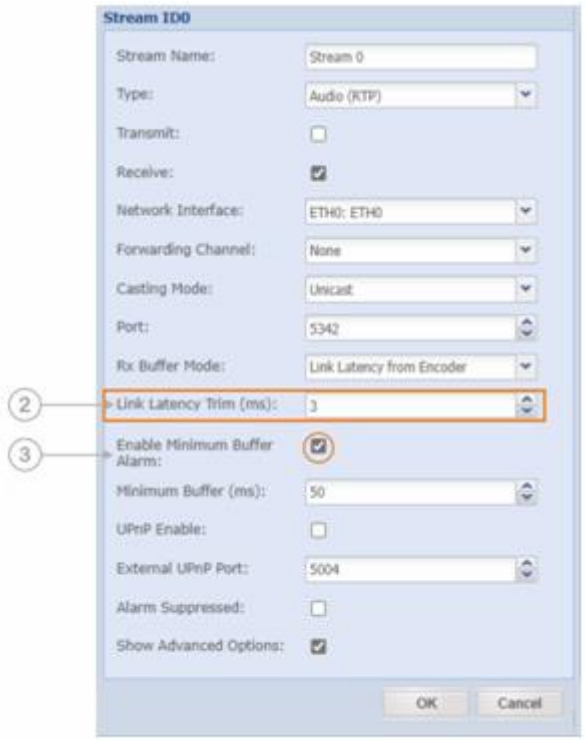


Figure 8-7 shows the latency controls on Tx streams for NTP and high-precision timing

⚠ Note this: Any change to the target latency by changing the Encoder or by individual settings at the decoder results in a buffer reset with a short interruption of the transmission!

8.3.5 Decoder Performance Page

The performance page presents the results of the configuration. In this example, a **target latency of 200 ms** is set by the Encoder. The latency of the **transmission link is 0.687 ms**, and the trim **offset value is 3.0005 ms,** so the buffer size results in 202 ms (rounded), and the desired **playout time is 203.0005 ms**, displayed as (rounded) 203 ms.

The resulting **buffer headroom is 202.313** ms (displayed as 202 ms).

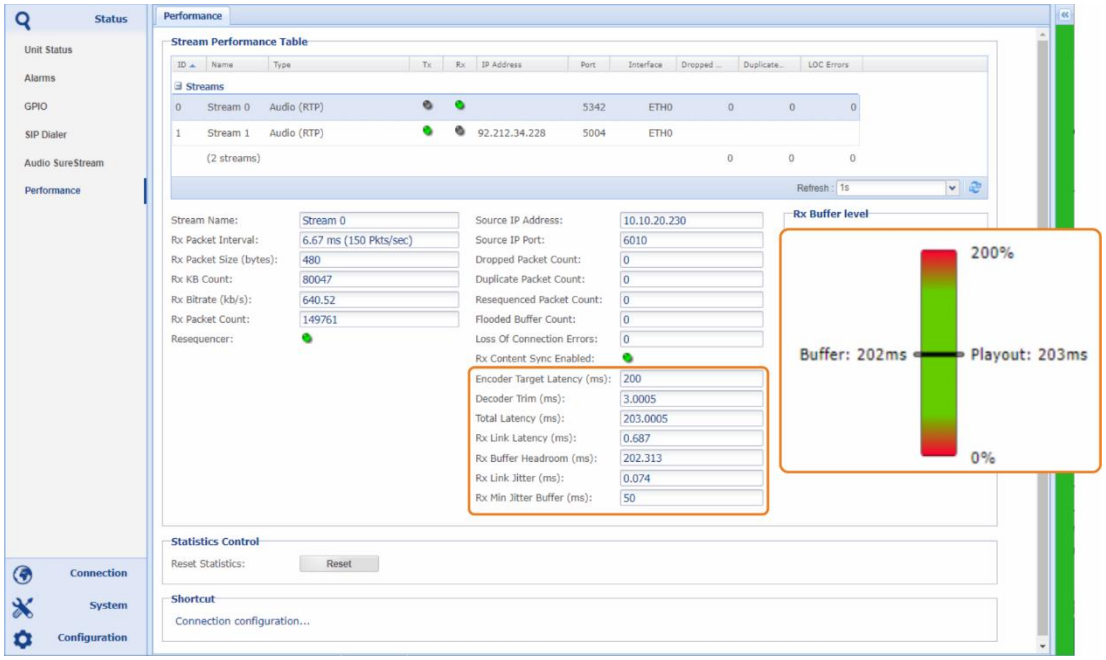


Figure 8-8 shows the timing components, the resulting playout time, and the buffer headroom.

Notes:

8.4 Some general Information on the use of External Clocks

8.4.1 NTP Time Alignment

In case the actual system time differs from the NTP time by more than 20ms, which can happen, e.g., due to NTP wander, the decoder re-synchronizes with the system clock in normal asymmetrical mode.

Switching to asymmetrical timing and switching back to NTP mode results in audible glitches of the modulation.

This can also happen in the first minutes of operation when the NTP client synchronizes with an NTP server for the first time.

9.0 Appendix C - SIP

9.1 Overview

SIP is an alternative connection mode and replaces when enabled the RTP/UDP direct mode in an Apt Codec. Once you have created a SIP Server account (chapter 3.5.4), the advantages of the SIP connection lie in the connection mode, which is similar to the dialing method of ISDN, whereby the remote codec receives stream configuration information via the SDP.

9.1.1 Implementation and Use

You select a contact from the phonebook (SIP dialer), choose a profile ("Dial with") and the connection can be established. If the SIP mode is enabled, the SIP dialer will appear as the first page when you open the codec's WEB GUI and replaces the standard Unit Status Page. The Unit Status Page is still available, it is just not the GUI's home page until you disable the SIP mode.

SIP in an audio codec is a product of the VoIP world and allows to dial different partners from a contact list, but syntactically similar to the email format. This is the SIP URI assigned by the SIP Server; it is unique and exists globally only once.

The SIP partner URIs are organized in the contact list (SIP Dialer/Phonebook) as a simple entry (SIP URI and name). The SIP codec profiles are centrally created once and are then available for connections to each contact (refer to chapter 3.5.5).

SIP is defined in various RFCs and has been implemented accordingly. There are some restrictions associated with this that do not apply to an APT codec in RTP/UDP direct mode.

- SIP in the APT audio codec can establish audio connections with Aux data and GPIO embedded in Eapt-X algorithms
- SIP mode works globally with a SIP server account, which is registered with the SIP provider, or in peer mode, which requires knowledge of the current destination address.
- SIP does not support redundant streaming.
- SIP connections should always be bi-directional (symmetrical use of codec profiles), as otherwise essential advantages of this mode will become invalid (e.g., port management via SIP Proxy).

9.1.2 Principle of a SIP/SDP Call Connection

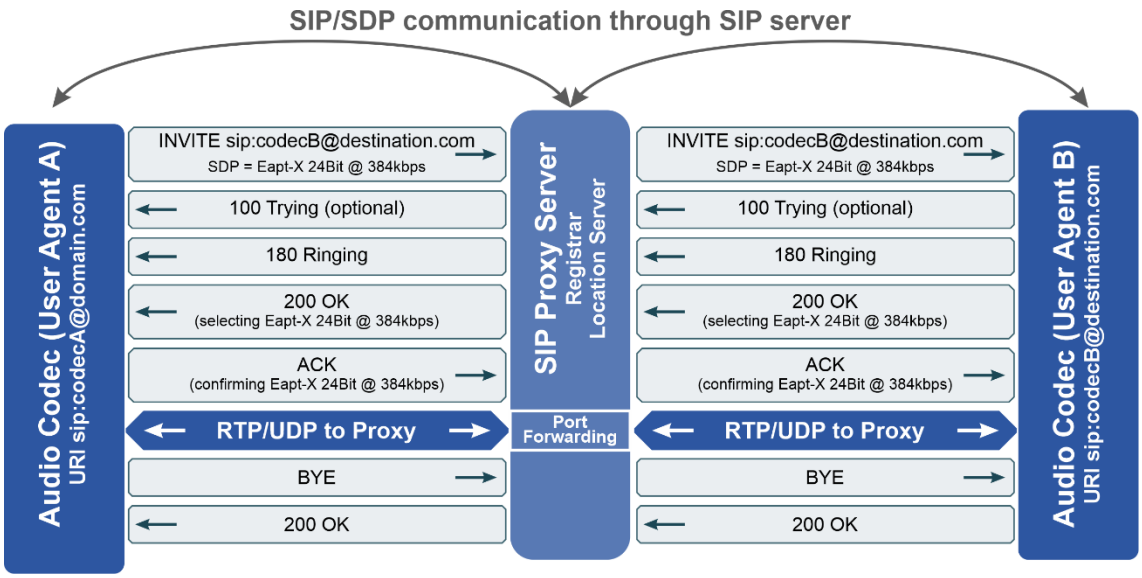


Figure 9-1: Shows a typical SIP infrastructure with registration and proxy server