Virtuoso Media Node
User's Manual

Revision: 2.8.44 (5409)

2019-02-15

Valid for SW version 2.8.44.

Contents

1 History

Revision	Date	Comments
2.8.44	2019-02-15	– Updated for version 2.8.44
2.8.30	2018-10-16	– Updated for version 2.8.30
2.6.24	2018-03-12	– Updated for version 2.6.12
2.4.14	2017-11-23	– Updated for version 2.4.14
2.0.16	2017-04-21	– Initial release version

2 Introduction

2.1 Scope

This manual is written for operators and users of the Virtuoso Media Node and provides necessary information for installation, operation and day-to-day maintenance of the unit. The manual covers the functionality of the software version 2.8.44 or later, and continues to be relevant to subsequent software versions where the functionality of the equipment has not been changed. When a new software version changes the functionality of the product, an updated version of this manual will be provided.

The manual covers the following topics:

- Getting started
- Equipment installation
- Operating instructions
- WEB interface description
- Preventive maintenance and fault finding
- Alarm listing
- Technical specifications

2.2 Warnings, cautions and notes

Throughout this manual warnings, cautions and notes are highlighted as shown below:

Warning: This is a warning. Warnings give information, which if strictly observed, will prevent personal injury and death, or damage to personal property or the environment.

Caution: This is a caution. Cautions give information, which if strictly followed, will prevent damage to equipment or other goods.

Note: Notes provide supplementary information. They are highlighted for emphasis, as in this example, and are placed immediately after the relevant text.

2.3 Heed warnings

- **All warnings marked on the product and in this manual should be adhered to. The manufacturer cannot be held responsible for injury or damage resulting from negligence of warnings and cautions given.**
- **All the safety and operating instructions should be read before this product is installed and operated.**
- **All operating and usage instructions should be followed.**
- **The safety and operating instructions should be retained for future reference.**

2.4 Contact information

Our primary goal is to provide first class customer care tailored to your specific business and operational requirements.

Please contact us at:

Telephone	+47 22 88 97 50
Fax	+47 22 88 97 51
E-mail	support@nevion.com
WEB	http://www.nevion.com
Mail and visiting address	Nevion Lysaker Torg 5 NO-1366 Lysaker Norway

3 Short Product Description

The Virtuoso is part of the Nevion cProcessor product family for processing and handling of MPEG transport streams. The cProcessor family represents a line of compact and powerful, yet cost-effective, products designed for advanced modification of MPEG Transport Streams.

Virtuoso includes Nevion's trademark advanced protection mechanisms that enables real-time transport of professional media over IP networks, as well as built-in monitoring that helps anticipate and correct any issues with the network or transport should they arise. Virtuoso can be configured via an easy-to-use web interface and interact with overlaying service and network management systems. Service scheduling and provisioning is performed via Nevion's Media Service Management and Orchestration solution: Video IPath.

The Virtuoso M4 consists of a 1RU (Rack Unit) server chassis with an integrated processor board for management and control, TS monitoring and processing, and IP/Ethernet network trunking up to 10 Gb/s. In addition, it holds up to four field installable modules, each offering a number of advanced input/output, processing and networking functions at present and in the future covering:

- H.264/AVC 3G/HD/SD 4:2:2 10-bit encoder/decoder (1 channel)
- TICO UHD encoder/decoder (2 channels)
- JPEG 2000 3G/HD/SD encoder/decoder (4 channels)
- DVB-ASI input/output module (4 channels)
- Uncompressed Media Processing and Adaptation (up to max 6 in any direction)

It's our goal to offer products that are reliable and easy to use. Therefore, the Virtuoso offers an intuitive and dynamic web interface that offers built-in Transport Stream monitoring of both encoder outputs and decoder inputs, as well as SDI and RTP/IP monitoring - all of which helps anticipate and correct any issues with input signals or networks should they arise.

Salient features of the Virtuoso are:

- PSI/SI table decoding
  - Repetition rate monitoring
  - Full decoding of all standard PSI/SI tables and descriptors
  - Monitoring of ASI and IP encapsulated transport streams
  - TR 101 290 Priority 1 monitoring: Sync loss, CC error
  - TR 101 290 Priority 2 monitoring: PCR jitter, PTS error
  - TR 101 290 Priority 3 monitoring: SI repetition rates
  - Monitoring of min/max bitrate for individual PIDs

- Flexible alarm configuration options
  - Alarm levels freely configurable individually for each channel
  - Individual setting of alarm levels based on PID values
- User-friendly configuration and control
  - WEB/XML based remote control
  - Easy access to unit from any WEB browser
  - Easy integration to NMS systems with SNMP Trap support
  - SNMPv2c agent
- Reception of transport stream over Gigabit Ethernet

3.1 Software options

The Virtuoso functionality depends on the software licences installed. The following table describes the features available as software options. Please refer to **Section 8.4.9.3** for more information how to obtain and enable feature upgrades.

Table 3.1.a Functionality enabled through software licences

Code	Max value	Description	Key features
OS	-	Enables usage of Virtuoso operating system.	
AMMX	50	Enables advanced monitoring on multi-program transport stream (MPTS)	ETR 290 Pri 2 and 3, PCR, Table decoding, Packet dump
BISSX	8	Enables BISS descrambling of Transport Streams	BISS-1
TSOX	80	Enables TS Gateway functionality output of Transport Streams over IP	IP outputs
ISWX	50	Enables TS Input switching functionality	TS Input Switching
TSPROTX	160	Enables FEC or LDO on TS over IP output, or FEC or SIPS on TS over IP Input.	FEC, SIPS, LDO
CCPX	4	Enables DVB-CISSA Encryption/Decryption	DVB-CISSA
J2KHDX	16	Enables JPEG2000 encoding or decoding	JPEG2000
J2KHDFILMX	16	Enables JPEG2000 encoding or decoding of film formats (2k, psf)	JPEG2000,2k,Film
UNCMONHDX	32	Enables monitoring of video (and embedded audio)	

Table 3.1.b Functionality enabled through software licences

Code	Max value	Description	Key features
MLSX	16	Number of outputs that can be synchronized by Multilink Synchronization	4K, 3D,HFR
UNCAUDX	2048	Number of audio channels that can be sent or received over IP	AES67
UNCAUDPROTX	2048	Number of audio channels that can be received with SIPS	AES67,SIPS
UNCAUDMONX	4096	Number of audio channels that can monitored	AES67
UNCHDX	32	Number of video channels that can be sent or received over IP	SMPTE2022-6
UNCHDFILMX	32	Enables film formats for IP transport (requires UNCHDX)	SMPTE2022-6, 2k, PSF
UNCHDPROTX	32	Enables SIPS protection for UNCHDX	SIPS
UNCHDCONTX	32	Enables contribution grade IP transport for UNCHDX	
UNCISW	32	Number of alarm based video input switches	Video changeover

3.2 Hardware options

The Virtuoso comes with a variety of hardware options. The product can be ordered with up to four daughter boards in order to tailor to specific needs in terms of inputs to monitor.

Currently, the four slots on the Virtuoso can be populated with any combination of the daughter boards listed below.

- ASI board (4xASI BNC inputs/outputs)
- H.264/AVC Encoder/Decoder Boards
- High Bitrate Accelerator Boards

4 Installing the Equipment

Caution: The Virtuoso must be handled carefully to prevent safety hazards and equipment damage. Ensure that the personnel designated to install the unit have the required skill and knowledge. Follow the instructions for installation and use only installation accessories recommended by the manufacturers.

4.1 Inspect the package content

- Inspect the shipping container for damage. Keep the shipping container and cushioning material until you have inspected the contents of the shipment for completeness and have checked that the Virtuoso is mechanically and electrically in order.
- Verify that you received the following items:
  - Virtuoso with correct power supply option
  - Power cord(s)
  - CD-ROM containing documentation and Flash Player installation files
  - Any optional accessories you have ordered

4.2 Installation Environment

As with any electronic device, the Virtuoso should be placed where it will not be subjected to extreme temperatures, humidity, or electromagnetic interference. Specifically, the selected site should meet the following requirements:

- The ambient temperature should be between 0 and 50 °C (32 and 122 °F).
- The relative humidity should be less than 95 %, non-condensing. Do not install the unit in areas of high humidity or where there is danger of water ingress.
- Surrounding electric devices should comply with the electromagnetic field (EMC) standard IEC 801-3, Level 2 (less than 3 V/m field strength).
- The AC power outlet (when applicable) should be within 1.8 meters (6 feet) of the Virtuoso.
- Where appropriate, ensure that this product has an adequate level of lightning protection. Alternatively, during a lightning storm or if it is left unused and unattended for long periods of time, unplug it from the power supply and disconnect signal cables. This prevents damage to the product due to lightning and power-line surges.

Warning: If the Virtuoso has been subject to a lightning strike or a power surge which has stopped it working, disconnect the power immediately. Do not re-apply power until it has been checked for safety. If in doubt contact Nevion.

4.3 Equipment installation

The Virtuoso is designed for stationary use in a standard 19" rack. When installing please observe the following points:

- Route cables safely to avoid them being pinched, crushed or otherwise interfered with. Do not run AC power cables and signal cables in the same duct or conduit.
- The Virtuoso has all connectors at the rear. When mounting the unit, ensure that the installation allows easy access to the rear of the unit.
- The fans contained in this unit are not fitted with dust/insect filters. Pay particular attention to this when considering the environment in which it shall be used.
- Make sure that the equipment is adequately ventilated. Do not block the ventilation holes on each side of the Virtuoso.

4.4 Ventilation

Openings in the cabinet are provided for ventilation to protect it from overheating and ensure reliable operation. The openings must not be blocked or covered. Allow at least 50 mm free airspace each side of the unit.

Warning: Never insert objects of any kind into this equipment through openings as they may touch dangerous voltage points or create shorts that could result in a fire or electric shock. Never spill liquid of any kind on or into the product.

- This product should never be placed near or over a radiator or heat register. Do not place in a built-in installation (e.g. a rack) unless proper ventilation is provided in accordance with the device airflow design as depicted in **Figure 4.1** .
- The Virtuoso may be vertically stacked in 19" racks without intermediate ventilation panels. In systems with stacked units forced-air cooling may be required to reduce the operating ambient temperature.

Figure 4.1 shows the air path through the unit, where cool air is taken from the front of the unit.

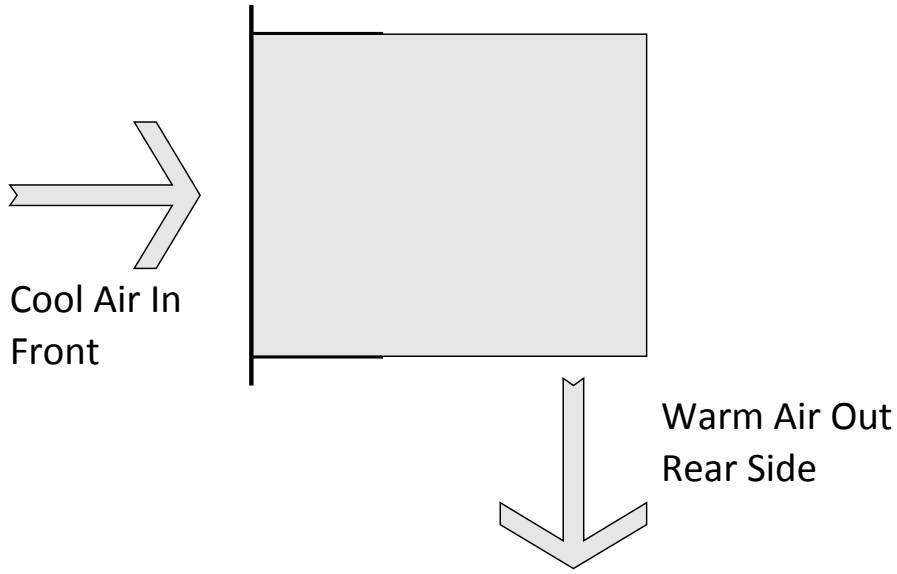


Figure 4.1 Air path through the unit

4.5 Power supply

The Virtuoso is delivered rated for AC operation.

Warning: This product should be operated only from the type of power source indicated on the marking label. Please consult a qualified electrical engineer or your local power company if you are not sure of the power supplied at your premises.

4.5.1 AC power supply

The Virtuoso has a wide-range power supply accepting the voltage range 100-240 VAC, 50/60 Hz. Please refer to **Appendix B** for a detailed specification of the AC power supply.

4.5.1.1 Dual AC power supplies

Alternatively, the Virtuoso may be fitted with dual internal wide-range AC power supplies. The power supplies cover the voltage range 100-240 VAC, 50/60 Hz.

During normal operation, load-sharing is used between the internal supplies. In case of a single power supply failure alarms will be raised and the unit will continue operating off the second power supply. To guard against failure in the external power circuitry it is imperative to connect each power supply to separate AC mains circuits.

Please refer to **Appendix B** for a detailed specification of the AC power supply.

4.5.1.2 AC power cable

Ensure that the AC power cable is suitable for the country in which the unit is to be operated.

Caution: Power supply cords should be routed so that they are not likely to be trod on or pinched by items placed upon or against them. Pay particular attention to cords at plugs and convenience receptacles.

The unit is supplied with a two meter detachable mains supply cable equipped with a moulded plug suitable for Europe, UK or USA, as appropriate. The wires in the mains cable are coloured in accordance with the wire colour code shown in **Table 4.1**.

Table 4.1 Supply cable wiring colours

Wire	UK (BS 1363)	EUROPE (CEE 7/7)	USA (NEMA 5-15P)
Earth	Green-and yellow	Green-and yellow	Green
Neutral	Blue	Blue	White
Live	Brown	Brown	Black

4.5.1.3 Protective Earth/technical Earth

To achieve protection against earth faults in the installation introduced by connecting signal cables etc., the equipment should always be connected to protective earth. If the mains supply cable is disconnected while signal cables are connected to the equipment, an earth connection should be ensured using the Technical Earth connection terminal on the rear panel of the unit.

Warning: This unit must be correctly earthed through the moulded plug supplied. If the local mains supply does not provide an earth connection do not connect the unit.

Caution: Consult the supply requirements in **Appendix B** prior to connecting the unit to the supply.

The unit has a Technical Earth terminal located in the rear panel. Its use is recommended. This is not a protective earth for electrical shock protection; the terminal is provided in order to:

1. Ensure that all equipment chassis fixed in the rack are at the same technical earth potential. To achieve this, connect a wire between the Technical Earth terminal and a suitable point in the rack. To be effective all interconnected units should be earthed this way.

2. Eliminate the migration of stray charges when interconnecting equipment.

Warning: If the terminal screw has to be replaced, use an M4x12mm long pozidrive pan head. Using a longer screw may imply a safety hazard.

4.5.1.4 Connecting to the AC power supply

Warning: Do not overload wall outlets and extension cords as this can result in fire hazard or electrical shock. The unit is not equipped with an on/off switch. Ensure that the outlet socket is installed near the equipment so that it is easily accessible. Failure to isolate the equipment properly may cause a safety hazard.

To connect the unit to the local AC power supply, connect the AC power lead to the Virtuoso mains input connector(s) and then to the local mains supply.

4.5.2 Powering up/down

Before powering-up the unit, please ensure that:

- The unit is installed in a suitable location
- The unit has been connected to external equipment as required

Power up the unit by inserting the power cable connected to the power source. When the unit has finished the start-up procedure, the fans will run at normal speed. Please check that all cooling fans are rotating. If they are not, power down the unit immediately.

Power down the unit by removing the power supply connector at the rear of the unit.

5 Functional Description

The Virtuoso provides advanced adaptation, processing, compression and networking capabilities. There are four (4) expansion slots for accelerator modules, providing highly flexible deployments for transport, encoding/decoding, processing, and monitoring applications in a small form factor.

Figure 5.1 shows a functional block diagram of the Virtuoso for a low/medium bitrate transport stream applications application.

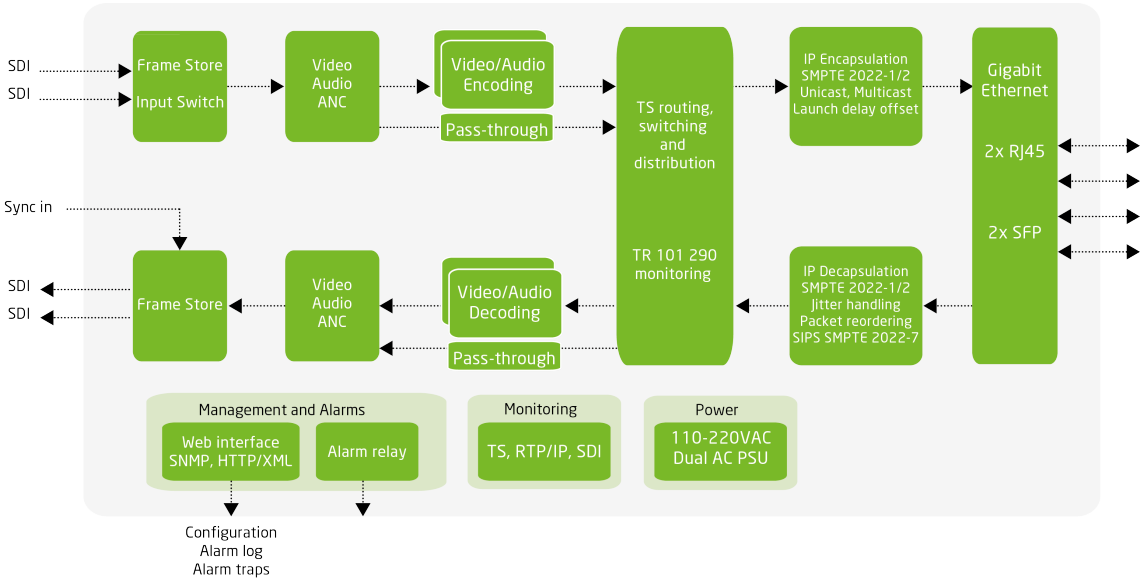


Figure 5.1 Functional Diagram for H.264/AVC, JPEG 2000 and ASI over IP

Figure 5.2 shows a functional block diagram of the Virtuoso for a high bitrate uncompressed media application.

5.1 Inputs

The input interfaces include up to twenty ASI inputs (BNC connectors) , up to 3 SDI inputs per H.264 Board , 4 SFP cages per HBR Board (used for Video or Data depending on SW version) ,and four Ethernet inputs .

5.2 Monitoring

The *Monitoring* section provides monitoring of up to hundreds of transport streams on-the-fly. Parameters of the selected transport streams will be monitored and compared against specifications and specific requirements. The values of critical components can be displayed graphically. An extensive set of alarms may be programmed, with different severity levels. The content of selected packets, or groups of packets, may be recorded for examination and/or documentation.

Measurements are made according to the DVB ETR 290 specifications.

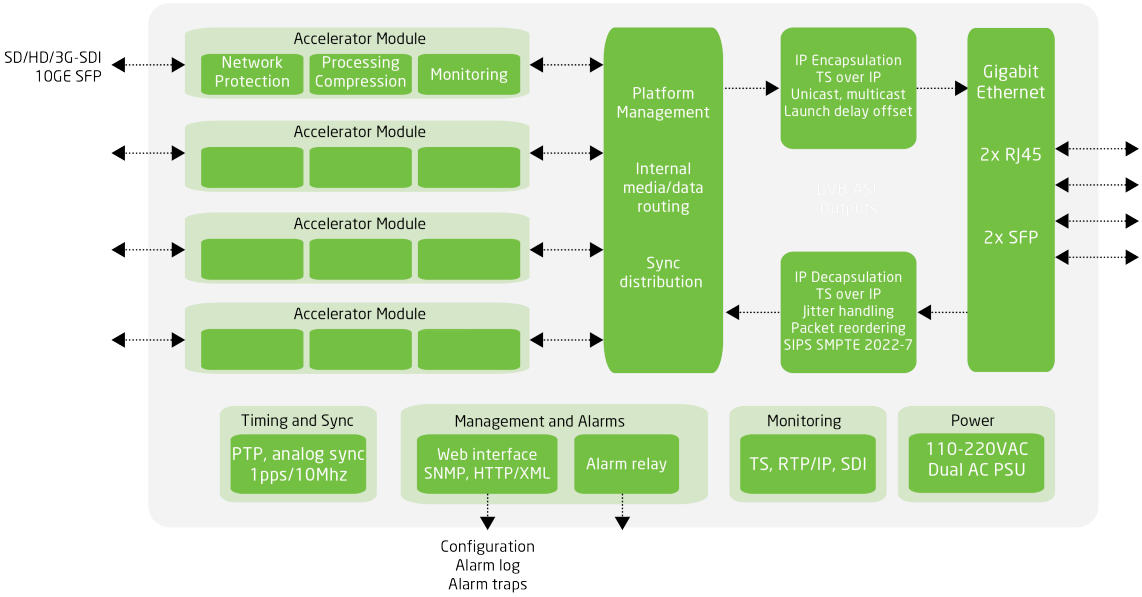


Figure 5.2 Functional Diagram for High Bit Rate Uncompressed Media Applications

5.3 Seamless IP Protection Switching

Seamless IP Protection Switching (SIPS) provides redundancy by protecting the media stream against errors in the IP network, but in a different manner compared to Forward Error Correction (FEC). FEC is designed to protect the stream against single or short burst packet losses, whereas SIPS provides protection against loss of complete data input, for example, due to link or equipment failure.

The main idea of SIPS is to transmit two identical copies of the media stream over separate network paths. At the receiver side, the data from the two incoming streams are combined at packet level to form an error free output data stream.

The combination of diverse path routing and perfect switching provides for the highest possible Quality of Service, effectively minimizing the effects of random packet losses, burst packet losses, losses due to fast reroutes, and link failures.

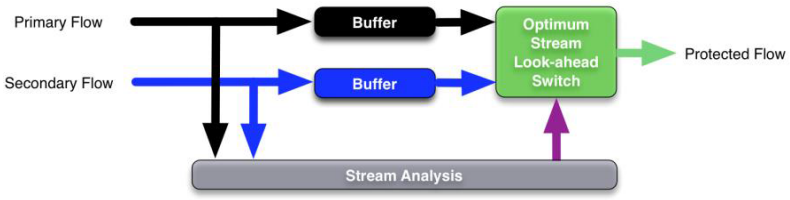


Figure 5.3 SIPS functional overview

Functional description

SIPS operates on the RTP packet level. The receive module buffers both incoming streams, mediating and selecting the most appropriate packets in what is termed active-active merging for use in de-encapsulation. In this way, if one stream is impaired, good packets are delivered via the other stream and a good output stream can always be reconstructed.

There will be packet loss at the combined stream only when the packet is received on neither of the two IP sources. The data stream resulting from combining the two incoming data streams will then be processed as one RTP packet stream.

Setup

At the transmitter side, the Virtuoso allows sending identical copies of the data flow to a user defined list of destinations. When several destinations have been configured for transmission, media streams are sent to different IP addresses but the streams are identical down to the RTP layer and are tagged with the same, randomly generated Synchronization Source ID (SSRC). For each destination, the physical or logical VLAN network interface, and IP unicast or multicast destination addresses are configured. This enables the two data streams to be routed to their respective network paths directly at the Virtuoso or at the first subsequent network node. See **Section 8.10.2.3** for more information on configuring redundant transmission/IP destinations.

At the receiver side SIPS must be enabled and the IP source parameters for IP flow A and B must be configured to receive the media streams from the two diverse network paths. For any fully seamless protection system to function, the dual media feeds presented at the receiver needs to be essentially coherent i.e. the exact same media feed down to the RTP transport layer. When the data streams have an identical SSRC value and data format, they are assumed to be identical and are used for Seamless IP Protection Switching. See **Section 8.6.2.3.2** for more info on configuration of SIPS on the receiver.

Delay compensation

As the A and B flows will typically be routed across network links with different delays, it is necessary for the SIPS module to wait for a period after the first signal is received before it starts outputting data, to ensure that the second signal that is received does not need to be written to the buffer after it is read out.

The SIPS Pre-buffer configuration parameter allows this period to be configured to allow the system to be able to compensate for the maximum expected differential latency between the A and B flows, while minimizing the additional delay added to the system.

Launch Delay Offset

If dual redundant network paths for some reason is not available, the Nevion patented technology Launch Delay Offset (LDO) may be employed on the transmitter side.

This feature makes it possible to introduce a delay to one of the transmitted media streams, and thereby introducing a temporal redundancy in the transmission. In this situation burst losses approaching the time delay configured for LDO can be handled by the receiving SIPS engine, even when only one network path is available.

Note that this setup will give protection against long burst losses, but not against complete network failure. If there is a need to protect against link failures, LDO should be used together with redundant network paths (routing flow A and B through different network paths).

For information on how to configure LDO, see **Section 8.10.2.3.1**.

Licensing

The SIPS feature requires a TSPROT licence at the receiving node. No licence is required to configure multiple IP destinations for an output channel on the transmit side.

The LDO feature requires the TSPROT licence at the transmitting node.

Compatibility

The SIPS feature is fully compatible with and extends the functionality of the SMPTE 2022-7 “Seamless Protection Switching of SMPTE ST 2022 IP Datagrams” standard.

5.4 Management subsystem

The management subsystem is a set of modules that handles all the interfaces to monitor and control the operation of the Virtuoso.

The management subsystem communicates with the users, both humans and machines, via the following interfaces:

- Front panel and back panel LEDs for status
- Graphical user interface via Flash application in WEB browser
- SNMP traps on alarms
- SNMPv2c Agent
- TXP (XML Protocol) to retrieve and set configuration and status
- Alarm relays on alarms
- Terminal interface either over Telnet or USB interface for debugging
- FTP server for direct file system access

The management subsystem communicates with other internal modules to make the unit perform the wanted operations.

5.4.1 Graphical user interface

Operators monitor and control the Virtuoso mainly via the Adobe Flash GUI application served from the device’s WEB server. The GUI application is accessed via a WEB browser that communicates with the configuration framework through an HTTP/XML based protocol.

The device exposes extensive status information to the web GUI providing detailed reports and real-time monitoring displays to the device administrator.

All the device configuration parameters available on the Virtuoso can be controlled from the web GUI.

5.4.2 Configuration database

The management subsystem processes configuration changes as transactions. All configuration changes made to the device are validated against the current running configuration before committing them to the device. This limits the risks of the administrator implementing changes that may cause down-time on the unit due to incompatible configuration settings.

Configurations can be imported and exported via the GUI. It is possible to clone the entire configuration of one device to another by exporting the configuration of one device and importing it to another.

Configurations exported via the web GUI are formatted as human readable/modifiable XML files. These files can be viewed or altered using any standard text or XML editor such as Windows Notepad.

To simplify cloning of devices, certain exported parameters within the XML file are tagged as device specific and therefore will be ignored when imported to either the same device or another. These parameters are as follows:

- Device Name and Inventory ID
- IP network parameters
- ASI Port mappings

5.4.3 Alarm manager

The Virtuoso contains an integrated alarm manager responsible for consistently displaying the alarm status of each individual interface.

"Port Alarms" are alarms bound to a specific input or output port via a port indexing system. The alarm severity for port related alarms can be configured per port level. "Device Alarms" are global to the device and are not bound to any specific port. They do not follow the indexing scheme. These are classified as "System Alarms".

Alarms are graphically represented in a tree structure optimized for simplified individual viewing and configuration. The "Device Alarm" tree is available from the "Device Info" page. The alarm tree for each port is available on the "Alarms" page for each port.

The alarm manager presents the alarm of highest severity upon the external interfaces of the device. The severity level of each individual alarm can be defined by the administrator. Alarm configuration is covered in greater detail in the "Alarm configuration" section.

SNMP traps are dispatched to registered receivers whenever there is an alarm status change.

The alarm manager keeps a log in non-volatile memory of the latest 100000 alarms that have occurred.

5.5 Time synchronisation

The Virtuoso contains an internal real-time clock that is used for all internal timestamps. The internal clock is battery backed up in order to continue operating while the unit has no power.

The internal time can be synchronised as follows:

- Manual setting.
- From NTP server using SNTP protocol.

6 Physical Description

Figure 6.1 Front panel of Virtuoso

The front panel, figure 6.1, provides two LEDs per Virtuoso. The meaning of the LED indicators is shown in table 6.1.

Table 6.1 Front panel LED descriptions

Indicator	Colour	Description
Power	Green	Indicates power ON and initialisation completed
Alarm	Red	Lit during reboot and when a critical alarm is active. The alarm severity level to activate the red LED is configurable

6.1 Slot and port numbering scheme

Figure 6.2 shows the rear panel of the Virtuoso, with no I/O daughter boards connected in the slots which are numbered 1-4. These slots can contain up to four daughter boards in any combination available from Nevion.

Figure 6.3 show the left half of the backplane as examples of one daughter board inserted in slot number 1. These figures illustrate the port numbering scheme used consistently for the Virtuoso. The numbering scheme contains two numbers, where the first is the slot number. The main board has slot number M (for Main board) and the rest are as shown in figure 6.2. The second number is an incrementing number, starting at 1, that increments for each extra addition of the same connector. As an example, the ASI daughter board in slot number 1 would have numbered the four BNC connectors as 1.1-1.4 as shown in figure 6.3.

Figure 6.2 Rear panel showing slot numbering for Virtuoso.

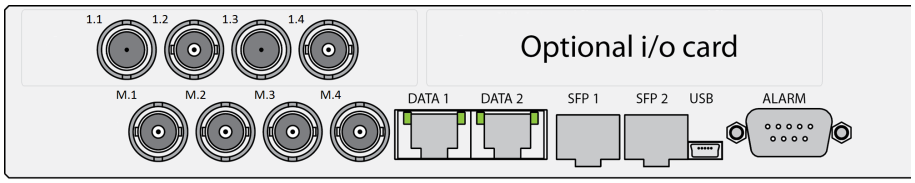


Figure 6.3 Example of numbering scheme using an ASI daughter board for Virtuoso.

6.2 ASI inputs

BNC connectors 1 through 4, as shown in figure 6.2 are input ports. Connect the transport stream input signals to be monitored to any of these connectors. The signals connected to the these input ports should be valid DVB or ATSC compliant transport streams according to the operational mode of the unit.

Note: that the four slots, numbered 1-4 in figure 6.2 and the cards contained in them (or the lack of card in them) may vary depending on the product configuration ordered from Nevion.

6.3 1PPS input

This coaxial connector (labelled 1PPS/10MHz) is provided in order to enable locking the internal system clock to a universal reference. A standard 1 pulse per second reference signal should be applied, e.g. from a GPS receiver. 1PPS is used for more accurate PCR measurements, and is required for SFN delay monitoring.

6.4 Alarm/Reset interface

The unit is equipped with a 9-pin male D-sub connector to provide alarm information. Two programmable relays are provided. The first relay is always activated on a critical alarm or when the unit is not powered.

The pin-out of the connector is shown in table 6.2.

Table 6.2 Alarm/Reset connector pin out

Pin	Function
1.	Relay 2 - Closed on alarm (NC)
2.	Relay 2 Common
3.	Relay 2 - Open on alarm (NO)
4.	Prepared for +5V Output
5.	Ground
6.	Alarm Relay - Closed on alarm (NC)
7.	Alarm Relay Common
8.	Alarm Relay - Open on alarm (NO)
9.	Optional Reset Input / GPI

Note: The Optional Reset Input / GPI is not currently not yet supported in software, but will be supported in a later release.

If a *critical* (level 6) alarm has been raised, if the unit is not powered or any other programmed condition for relay 1 is satisfied, there will be a connection between pin 6 and pin 7; otherwise, there will be a connection between pin 7 and pin 8.

The optional (additional) relay will follow the same behaviour, except that it can also be programmed to be *not* activated for a *critical* (level 6) alarm.

A connection between pin 9 and 5 (or a TTL low on pin 9) will hold the unit in reset if this function has been enabled. The connection must be held for 0.5 seconds in order to activate the reset. This can be used to force a hard reset of the unit from an external control system. This pin can also be used as a general purpose input (GPI).

For electrical specifications of the alarm connector, please refer to Appendix **B** (Technical Specifications).

6.5 Ethernet ports

The Virtuoso is equipped with four Ethernet ports. Together, these allow monitoring of hundreds of IP encapsulated MPEG transport streams. There is, however, an upper limit to the overall bit rate of the transport streams that can be monitored simultaneously. Two of the Ethernet ports are Ethernet 1G data ports, Eth M.1 and Eth M.2.

The data port LEDs give the following information:

Speed indicator (left)
: Unlit = 10 Mbit/s, green = 100 Mbit/s, yellow = 1000 Mbit/s

Traffic and link indicator (right)
: Green - lit when link is established, blinks when data is transmitted or received.

6.5.1 SFP+ ports

The Virtuoso provides two slots to accommodate two SFP+ modules, labeled Eth M.3 and Eth M.4. This will provide two additional Ethernet ports supporting fiber optical transmission.

Enabling of the SFP+ slot is done from the Networks->Ethernet M.3 or Networks->Ethernet M.4 pages.

6.6 USB port

The mini USB connector provides an IP network-independent means to configure and monitor the Virtuoso. This is useful especially when the unit shall be introduced into a network already in operation.

USB 1.1 standard is supported.

6.7 Technical Earth

Connect the Technical earth to a suitable system earth point.

6.8 Mains power connector

Figure 6.2 shows the unit with an AC mains power connector.

Section 4.5 provides details of the power supply, protective earth and security. Read these instructions carefully prior to connecting the unit to mains power.

6.9 I/O daughter boards

6.9.1 H.264/AVC Codec Board

Figure 6.4 Modular version of the H.264/AVC Codec Board

The H.264/AVC Codec board can either be configured as an Encoder or a Decoder, and is available for both the fixed and the modular chassis. In the current SW version (2.8.44) each port has the following configurations:

- BNC 1: ASI Input in Decoder mode / SDI Input in Encoder mode
- BNC 2: SDI Input or SDI Output
- BNC 3: SDI Input or SDI Output
- BNC 4: Reference Sync Input or ASI Output

HW ID: NEO1401.4610

6.9.2 High Bit Rate Accelerator

Figure 6.5 High Bit Rate Accelerator Board

The High Bit Rate Accelerator has the capability to load different SW images with different media functions. Available images in the current SW version (2.8.44): JPEG2000 Encoder, JPEG2000 Decoder, JPEG2000 Encoder/Decoder, Linear and TICO Encoder/Decoder

HW ID: NEO1501.4810

6.9.3 ASI Board

The ASI board is available for both the fixed and the modular chassis. In the current SW version (2.8.44) each port has the following configurations (starting with the leftmost when looking at the rear of the chassis):

- BNC 1: ASI Input / Output
- BNC 2: ASI Input / Output
- BNC 3: ASI Input / Output
- BNC 4: ASI Input / Output

HW ID: NEO1402.4213

6.10 Front Panel Display

Note: The presence of a front display is optional.

The Virtuoso contains a large, easy to read LCD display which is backlit, so it provides readable characters even in environments with dark areas or bright sunlight.

To the right of the display is an associated keypad which is backlit with the following buttons:

- 4 directional arrows

- Set/OK/Enter
- Back/Cancel

The display shows information to enable the identification of the unit, the status and basic configuration possibilities without the need of using the web GUI.

6.10.1 Using the Front Panel Display

When power is applied to the Virtuoso the display screen will show the booting progress of the system.

At start up, the default view shows the basic settings of the unit. This view is also shown after the device has been inactive for a period. This base view displays the following information:

- the product name and SW version number,
- the overall alarm status of the most critical alarm currently active on the unit,
- the IP address of the unit,
- the serial number.

When in the base view, pressing any of the six buttons will activate the main menu. The menu items are:

- Network
- System
- Active Alarms

In order to access these sub-menus, the up and down arrow keys are pressed to choose the correct item and pressing the Enter or right arrow button enters this menu.

For menus larger than the screen size, an arrow is shown on the top right or bottom right corner of the display telling the user that more items are available by scrolling up or down (using the up or down arrows). Pressing the Exit/Return button while being in a menu gives access to the parent menu (if any).

Network menu
: Displayed are the four IP interfaces - Eth M.1 to M.4 - and also the IP Routing option. Viewing and changing the IP interfaces is covered in **Section 7.3.3**.

  IP Interfaces
  : The interfaces are labeled with a status showing whether or not they are currently enabled or disabled. The options provided in this menu are IP Edit and Enter to Enable/Disable.

  IP Routes
  : This displays the list of current IP Routes along with the option of Add a New Route. More about IP Routes is described in **Section 8.5.1.3** where this function is covered for

the WEB interface. Pressing Enter on any selected IP route gives the following options for the selected route:

- View Route - This displays the parameters of the IP route.
- Edit Route - Here there are three configurable parameters available: IP address and subnet mask both edited in Edit Destination, Edit Gateway and Edit Metric. In order to apply the changes made, the Enter button must be pressed.
- Remove Route - This will delete the current route.

System menu

The two options available are Reboot and Reset to factory default. These both have an extra confirmation screen to which the user can only enable the selection by pressing enter. The confirmation page of the Reset to factory default menu contains a simplified disclaimer.

Active Alarm menu

The System Alarms menu can be found here, showing a list of all current system alarms, selecting one of these entries will display all the information about that alarm. This contains the same entries as the alarm log as described in **Section 8.3.6**

7 Operating the Equipment

The Virtuoso is configured and controlled locally and remotely through a Flash-based Web interface. The only application required on the computer to use this interface is a Web browser and the Adobe Flash Player.

Note: Adobe Flash Player 10.0.2 or newer is required to use the Web interface of the Virtuoso. As a general rule it is recommended to always use the latest official release of Flash Player. If the Flash Player is not installed on the adminstrator PC, a copy is provided on the CD delivered with the device. Alternatively, the latest Adobe Flash Player can be downloaded free of charge from http://www.adobe.com.

7.1 Accessing the graphical user interface

The default IP address of the Virtuoso will most probably not be suitable for the network where the unit will operate. Therefore the user should change the IP address of the management interface so that access may be gained from the network.

The Virtuoso offers several options to alter the user interface IP address; through an Ethernet connection or using a USB terminal interface or using a PC application. If your management computer allows setting a fixed IP address, change the IP address using the Ethernet option described in **Section 7.3.1**.

If a static address cannot be configured on your management computer, **Section 7.3.2** gives the procedure to initially configure device network parameters (IP, netmask, etc...) using the USB terminal interface.

Configuring the device functionality according to operational needs is done using the Web interface, see **Chapter 8**.

7.2 Password protection

Remote access to the device is controlled by password protection.

There are 3 user levels providing different user privileges, each with a separate default password:

Username	Default password	Privileges
admin	salvador	Full access to device
operator	natal	Configure setting, cannot alter passwords
guest	guest	View configuration and alarm logs

7.3 Changing the IP address of the unit

The default IP configuration on the Ethernet ports is described in **Table 7.1**.

Table 7.1 Default IP configuration

Interface	IP address	Subnet mask
Ethernet M.1	10.0.0.10	255.255.255.0
Ethernet M.2	10.0.2.100	255.255.255.0
Ethernet M.3	10.0.3.100	255.255.255.0
Ethernet M.4	10.0.4.100	255.255.255.0

7.3.1 Changing IP address via the Web GUI

Windows 7 example

The screen-shot in **Figure 7.1** shows how to configure the network interface in Windows 7 to communicate with the Virtuoso via Ethernet M.1 with factory default settings. The IP address/netmask is set to 10.0.0.20/255.255.255.0 which is on the same subnet as the Virtuoso, and does not conflict with the IP address of the device.

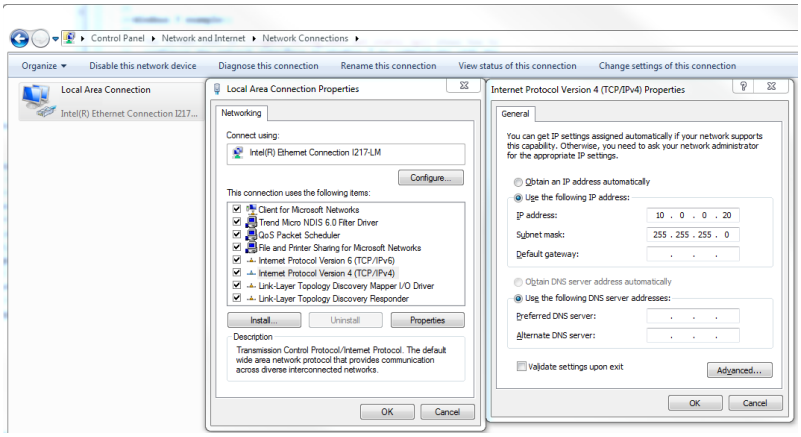


Figure 7.1 Setting static IP address 10.0.0.20 in Windows 7

Note: If several new devices are accessed one after the other, the ARP cache of the computer from which the devices are being accessed may have to be flushed between each new device access, since the same IP address will be used for different MAC addresses. On Windows 7 this is done on the command line typing the command `'arp -d *'`

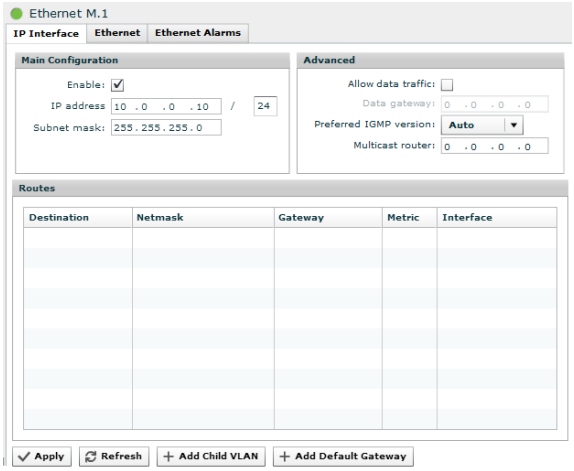


Figure 7.2 Configuring network settings via the Web GUI

1. Connect an Ethernet cable directly between the PC and the Ethernet port of choice on the Virtuoso. Configure the PC to be on the same subnet as the Virtuoso. See **Figure 7.1**.

2. Open your Web browser and type the default IP address of the chosen interface in the address field of the browser (for instance http://10.0.0.10 for Ethernet M.1). Log into the GUI with username **admin** and password **salvador**.

3. Browse to Network -> Ethernet M.1 in the GUI navigator, and set the correct IP address settings. Click Apply to activate the new parameters. **Figure 7.2** shows this GUI screen.

Note: Contact with the unit's GUI will now be lost. Please type http://<your new IP address> in your browser to reconnect to the unit.

7.3.2 Changing the management port IP address via the terminal interface

If a static IP address cannot be configured on your computer, follow the procedure below to configure the IP address via the terminal interface.

1. Install the USB driver from the product CD. (This step may be omitted if the driver has already been installed.)

2. Connect your computer to the Virtuoso via a USB cable to the USB port.

3. Access the terminal interface using a suitable terminal program, emulating an ANSI terminal, on your PC (e.g. HyperTerminal). The USB will appear as a virtual COM port on your PC. No specific serial port settings are required. Assure scroll lock is not on. Type <enter> and see that you have a prompt (app>).

4. In the terminal, type the following command and press <Enter>:

The interface name can be found using the command

```
ip addr
```

Using the interface name, an IP address can then be set to an Ethernet port using the command

```
ip addr set <interface num> <IPv4 address>/<Netmask length>
```

Example:

```
app>ip addr set 0 10.40.80.100/24
```

This will result in the IP address 10.40.80.100 being set on Ethernet M.1. The subnet mask is set to 255.255.255.0.

Note: The product CD shipped with the Virtuoso contains a USB driver to use for serial communication with the device on the USB port. The MS Windows driver installation script is configured to give a one-to-one relationship between the physical USB port number on the PC and the COM port number to use on the PC.

7.3.3 Changing the IP address via the display

In order to access the IP interface menu using the display, choose the Network item and press Enter. Under the IP interface menu items; Eth M.1 to M.4, the two choices are: IP Edit and Enable/Disable.

IP Edit allows the user to set the IP address of the Ethernet interface and the subnet mask. The IP address / subnet mask is shown in the following form:

010.040.080.100/24

In order to change the IP address or the subnet mask, the left and right keys are used to move a blinking cursor along the digits and select the ones which need to be altered. Using the up and down arrows increments or decrements the digit that is currently selected.

The Enable/Disable option will enter into a confirmation page where the user can press Enter to enable or disable the selected interface.

7.3.4 Changing the IP address via Detect

Nevion has made a free to use PC application called Nevion Detect that may be used to configure the IP address of the unit. Simplest way to use this application is to connect back to back to the Ethernet interface that you would like to change the IP address of, and launch the application. This tool will also detect the current IP address of the interface. Contact Nevion Support to get the application or download it from our webpage.

7.4 Software upgrade

Upgrading the software of the main board is described in **Section 8.4.9.2**. The daughter boards, if any, are all running their own software. Upgrading the software of daughter boards is done using the same interface as for main board, with a few exceptions as listed below.

8 WEB Interface

The Virtuoso is entirely controlled through a WEB interface using the web browser's Flash plugin. After log-in the main status page appears displaying an overall view of the device functionality and status. It also displays a number of tabs giving access to all functional controls of the device.

This chapter goes through the different GUI pages used to control the Virtuoso and get status information.

8.1 Login

Access the Virtuoso by entering its IP address in the address field of your favourite browser. When accessing the Virtuoso the first time, the progress bar (**Figure 8.1**) should appear while the Flash application is loading from the device.

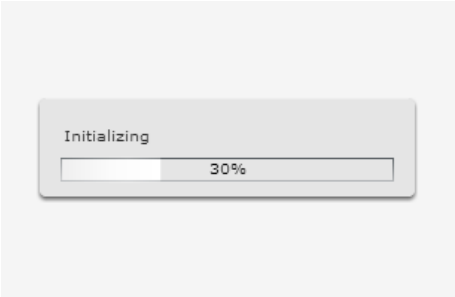


Figure 8.1 Flash application loading

When the loading of the Flash application is finished, the login window (see **Figure 8.2**) is displayed. Type the username and password to enter the GUI application. The default passwords are listed in **Section 7.2**.

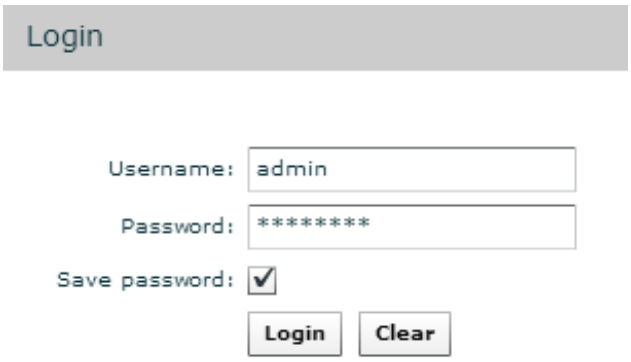


Figure 8.2 GUI login window

The login dialogue has an option "Save password", which makes the browser store the username and password in a cookie and use them as default values at next login.

8.2 Status header

After successful login the start page is shown. The top part of the page (shown in **Figure 8.3**) is called the status header, while the bottom part of the page (shown in **Figure 8.4**) is called the status footer.

Figure 8.3 The status header

Figure 8.4 The status footer

In the status header the product name is shown on the left hand side, along with the configurable product label, see **Section 8.4.1**.

The status header displays an alarm indicator showing the overall alarm status of the device. The colour of the indicator shows the highest level alarm currently active in the unit. It is green if no alarm is active. Other possible colours are described in **Appendix D**.

Several items are presented in the right corner/section of the header. Starting from the left:

- A text showing the current user name followed by the users access level in brackets.
- A button to log out from the GUI.
- A button to switch current user level.
- The Nevion logo.
- A button for minimising the header. Using this hides a lot of the header information and gives more space for the rest of the page.

In the status footer the following items are present from left to right.

- The name of the current configuration, if any. See **Section 8.4.1** for details on how to configure this.
- The current software version
- Fill level of the alarm log, see **Section 8.3.6**.
- The local device time, see **Section 8.4.4**.
- An activity indicator.

Note: The activity indicator shows one box for each request being processed by the unit. Each box may change from green to red if excessive time elapses during the processing. During normal operation, no squares should turn red. If squares start turning red there might be a problem with the communication between the device and the computer, or the device may be busy. If the device has not responded to a request within 20 seconds, the indicator turns yellow. If no response has been received after 40 seconds, it turns red.

A tab bar is located beneath the status header. The exact number of tabs and tab labelling depends on the units operational mode and licences. Clicking a tab will open the corresponding page with a navigation pane to the left as shown in **Figure 8.5**. This pane is used to navigate between sub-pages of the tab.

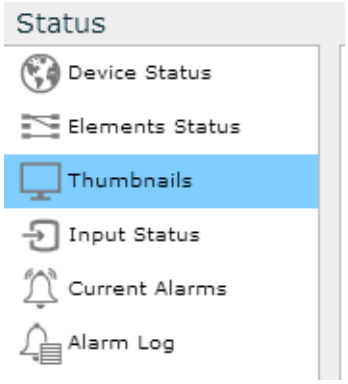


Figure 8.5 Status navigator

Note: The navigator can be collapsed to economise on screen space. Click the vertical grey line with two small arrows to the left of the navigator.

8.3 Status

The status page is the main page when logging on to the Virtuoso.

The following sub-pages are available within the status page:

Functional Status
: This page shows an overview of how all the physical and logical elements in the Virtuoso are connected. Note that unused elements, i.e. elements that are not connected to anything is not displayed by default.

Device Status
: Main page which summarizes the current status of the unit as a whole and by showing individual input status. All the inputs on the unit is shown in this view, and the color of the inputs represents its current alarm state. Additionally, hovering the mouse over any input will provide the user with further information about the current status and configuration of the input.

Thumbnails
: This page allows the user to see the thumbnails of all SDI Inputs and Encoders/Decoder in one view.

Input Status
: This page shows all the current inputs on the Virtuoso. The page allows the user to select which information to show for each input, and whether or not to show disabled inputs.

Current Alarms
: Shows the currently active alarms on the device.

Alarm Log
: Presents the device alarm log and provides operations for clearing the log or exporting it as a comma separated value file (.CSV).

New Alarms
: Shows new alarms in log since last time alarms was acknowledged.

8.3.1 Device Status

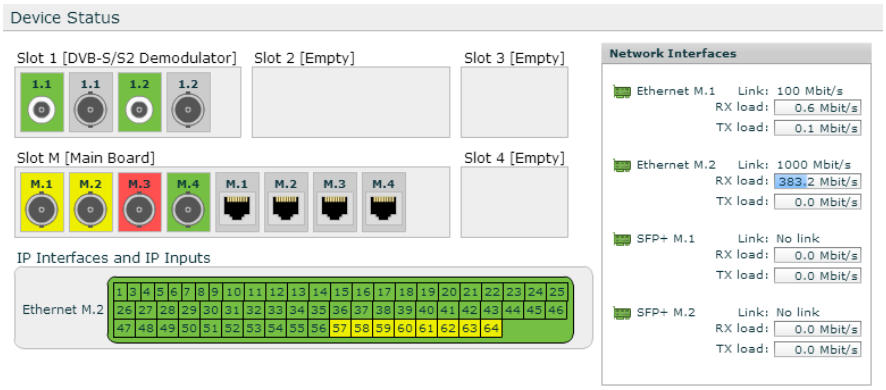


Figure 8.6 Current status page

Figure 8.6 shows the Current status page. This gives a visualization of the current unit being operated, and shows its hardware configuration with main and daughter boards.

8.3.2 Elements Status

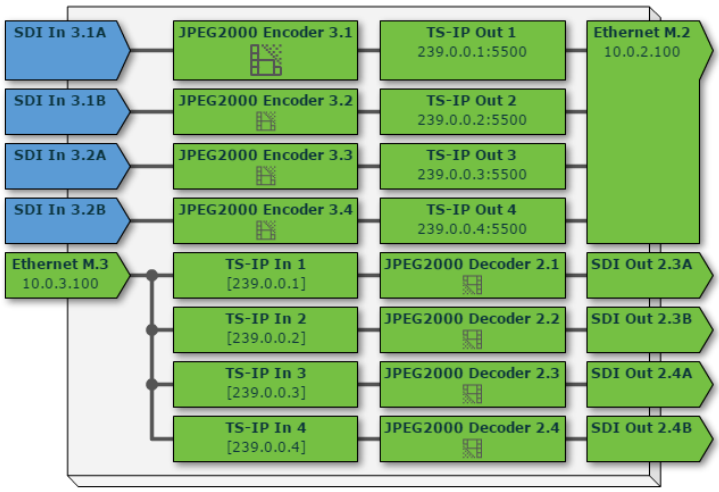


Figure 8.7 Elements status page

Figure 8.7 shows the Elements Status page. This page shows an overview of how all the physical and logical elements in the Virtuoso are connected. Note that unused elements, i.e. elements that are not connected to anything is not displayed by default. It is also possible to make new connections in this view simply by dragging elements on top of each other. This includes the unused elements at the bottom, but note that this is not supported by all elements, and the order in which you make connections may be important. It is also possible to add new logical elements by clicking the appropriate buttons in the top right corner.

8.3.3 Input Status

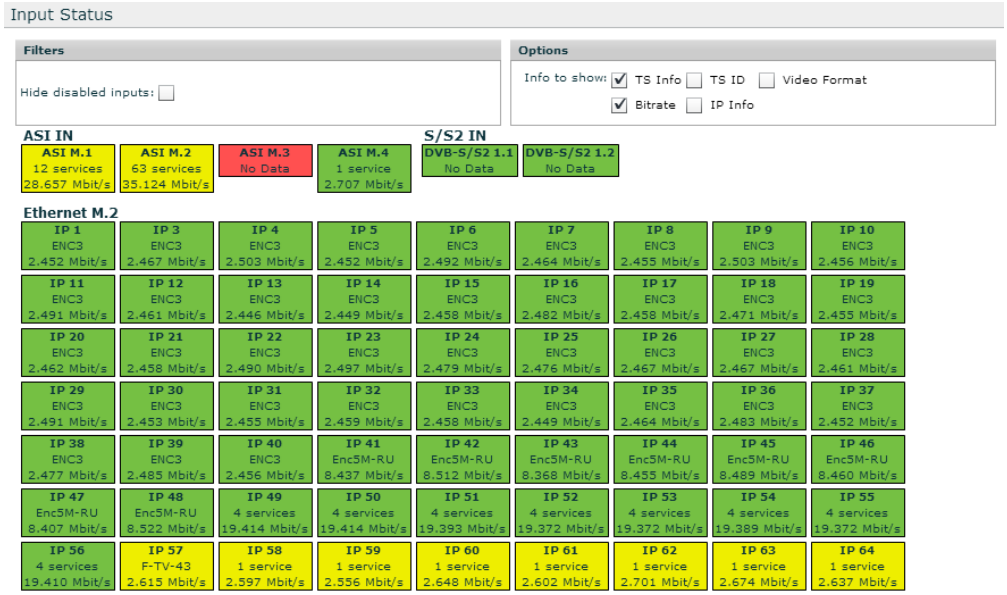


Figure 8.8 Input status page

Figure 8.8 shows the Input status page. On this page, all the inputs are shown. This includes all physical inputs and all the IP inputs. The user can configure what this page should show.

In the Filters section above the inputs, the user can select whether or not to display disabled inputs. The Options section gives the user a number of tick boxes to select whether or not to display various information for each input, such as bit rate or transport stream ID.

8.3.4 Thumbnails

In figure 8.9, the Thumbnails page is shown. This page allows the user to see the thumbnails of all SDI Inputs and Encoders/Decoder in one view.

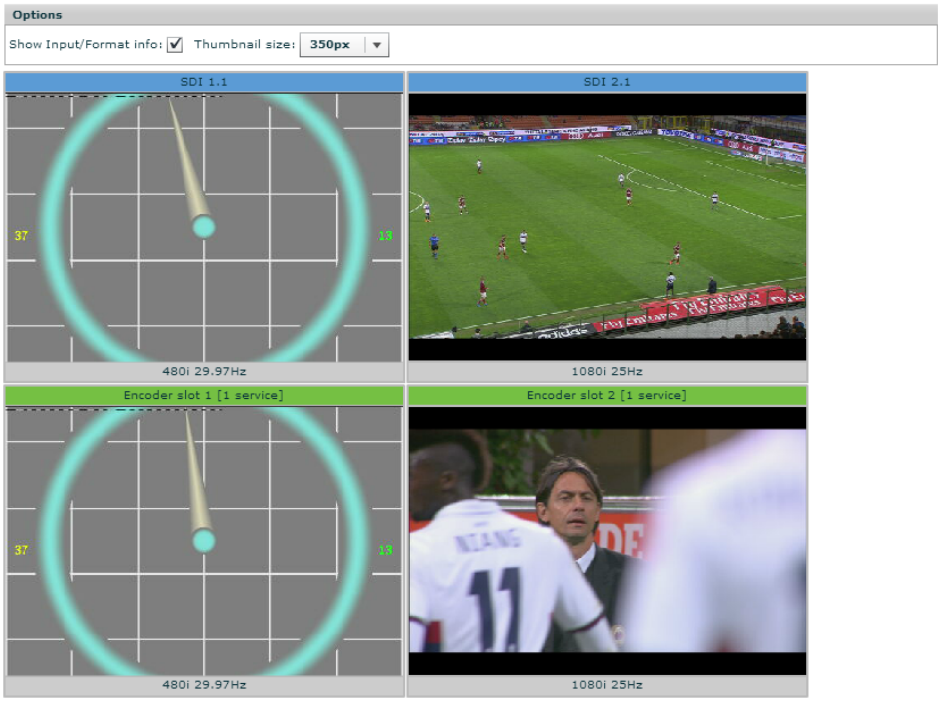


Figure 8.9 Thumbnails overview page

8.3.5 Current alarms

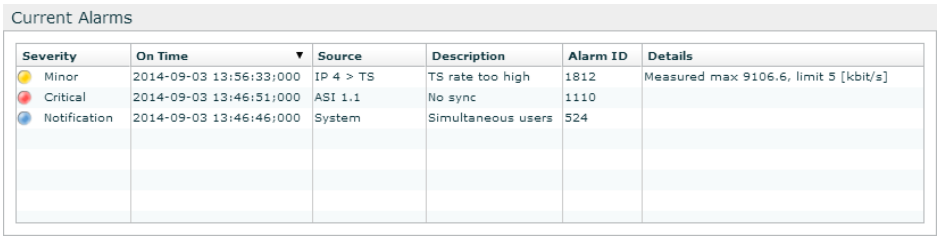


Figure 8.10 Current alarms subpage on the status page

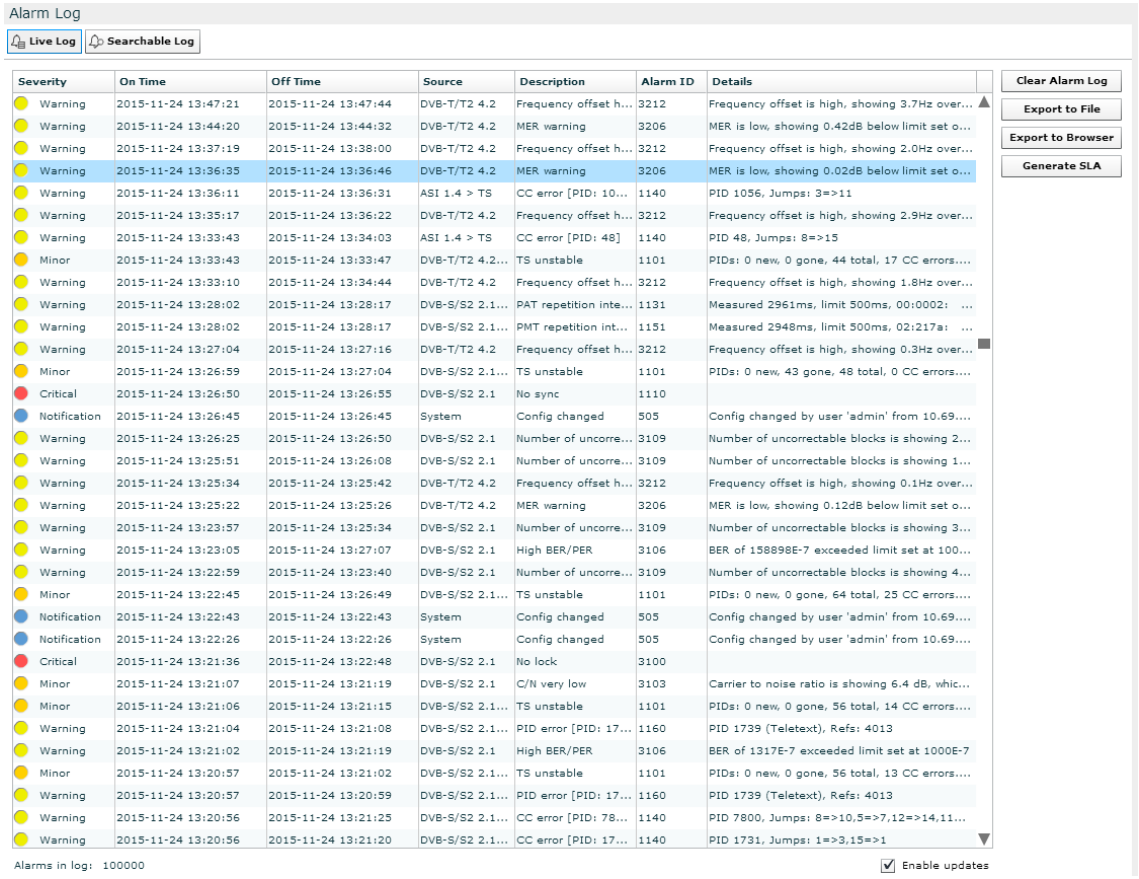
Clicking the Current alarms button the navigator on the left side takes the user to the page shown in figure 8.10.

Descriptions of the column values for each entry is described in 8.3.6.

8.3.6 Alarm log

The page gives access to two sub-pages described below.

8.3.6.1 Live Log



Severity	On Time	Off Time	Source	Description	Alarm ID	Details
Warning	2015-11-24 13:47:21	2015-11-24 13:47:44	DVB-T/T2 4.2	Frequency offset h...	3212	Frequency offset is high, showing 3.7Hz over...
Warning	2015-11-24 13:44:20	2015-11-24 13:44:32	DVB-T/T2 4.2	MER warning	3206	MER is low, showing 0.42dB below limit set o...
Warning	2015-11-24 13:37:19	2015-11-24 13:38:00	DVB-T/T2 4.2	Frequency offset h...	3212	Frequency offset is high, showing 2.0Hz over...
Warning	2015-11-24 13:36:35	2015-11-24 13:36:46	DVB-T/T2 4.2	MER warning	3206	MER is low, showing 0.02dB below limit set o...
Warning	2015-11-24 13:36:11	2015-11-24 13:36:31	ASI 1.4 > TS	CC error [PID: 10...	1140	PID 1056, Jumps: 3=>11
Warning	2015-11-24 13:35:17	2015-11-24 13:36:22	DVB-T/T2 4.2	Frequency offset h...	3212	Frequency offset is high, showing 2.9Hz over...
Warning	2015-11-24 13:33:43	2015-11-24 13:34:03	ASI 1.4 > TS	CC error [PID: 48]	1140	PID 48, Jumps: 8=>15
Minor	2015-11-24 13:33:43	2015-11-24 13:33:47	DVB-T/T2 4.2...	TS unstable	1101	PIDs: 0 new, 0 gone, 44 total, 17 CC errors....
Warning	2015-11-24 13:33:10	2015-11-24 13:34:44	DVB-T/T2 4.2	Frequency offset h...	3212	Frequency offset is high, showing 1.8Hz over...
Warning	2015-11-24 13:28:02	2015-11-24 13:28:17	DVB-S/S2 2.1...	PAT repetition inte...	1131	Measured 2961ms, limit 500ms, 00:0002: ...
Warning	2015-11-24 13:28:02	2015-11-24 13:28:17	DVB-S/S2 2.1...	PMT repetition int...	1151	Measured 2948ms, limit 500ms, 02:217a: ...
Warning	2015-11-24 13:27:04	2015-11-24 13:27:16	DVB-T/T2 4.2	Frequency offset h...	3212	Frequency offset is high, showing 0.3Hz over...
Minor	2015-11-24 13:26:59	2015-11-24 13:27:04	DVB-S/S2 2.1...	TS unstable	1101	PIDs: 0 new, 43 gone, 48 total, 0 CC errors....
Critical	2015-11-24 13:26:50	2015-11-24 13:26:55	DVB-S/S2 2.1	No sync	1110	
Notification	2015-11-24 13:26:45	2015-11-24 13:26:45	System	Config changed	505	Config changed by user 'admin' from 10.69....
Warning	2015-11-24 13:26:25	2015-11-24 13:26:50	DVB-S/S2 2.1	Number of uncorre...	3109	Number of uncorrectable blocks is showing 2...
Warning	2015-11-24 13:25:51	2015-11-24 13:26:08	DVB-S/S2 2.1	Number of uncorre...	3109	Number of uncorrectable blocks is showing 1...
Warning	2015-11-24 13:25:34	2015-11-24 13:25:42	DVB-T/T2 4.2	Frequency offset h...	3212	Frequency offset is high, showing 0.1Hz over...
Warning	2015-11-24 13:25:22	2015-11-24 13:25:26	DVB-T/T2 4.2	MER warning	3206	MER is low, showing 0.12dB below limit set o...
Warning	2015-11-24 13:23:57	2015-11-24 13:25:34	DVB-S/S2 2.1	Number of uncorre...	3109	Number of uncorrectable blocks is showing 3...
Warning	2015-11-24 13:23:05	2015-11-24 13:27:07	DVB-S/S2 2.1	High BER/PER	3106	BER of 158898E-7 exceeded limit set at 100...
Warning	2015-11-24 13:22:59	2015-11-24 13:23:40	DVB-S/S2 2.1	Number of uncorre...	3109	Number of uncorrectable blocks is showing 4...
Minor	2015-11-24 13:22:45	2015-11-24 13:26:49	DVB-S/S2 2.1...	TS unstable	1101	PIDs: 0 new, 0 gone, 64 total, 25 CC errors....
Notification	2015-11-24 13:22:43	2015-11-24 13:22:43	System	Config changed	505	Config changed by user 'admin' from 10.69....
Notification	2015-11-24 13:22:26	2015-11-24 13:22:26	System	Config changed	505	Config changed by user 'admin' from 10.69....
Critical	2015-11-24 13:21:36	2015-11-24 13:22:48	DVB-S/S2 2.1	No lock	3100	
Minor	2015-11-24 13:21:07	2015-11-24 13:21:19	DVB-S/S2 2.1	C/N very low	3103	Carrier to noise ratio is showing 6.4 dB, whic...
Minor	2015-11-24 13:21:06	2015-11-24 13:21:15	DVB-S/S2 2.1...	TS unstable	1101	PIDs: 0 new, 0 gone, 56 total, 14 CC errors....
Warning	2015-11-24 13:21:04	2015-11-24 13:21:08	DVB-S/S2 2.1...	PID error [PID: 17...	1160	PID 1739 (Teletext), Refs: 4013
Warning	2015-11-24 13:21:02	2015-11-24 13:21:19	DVB-S/S2 2.1	High BER/PER	3106	BER of 1317E-7 exceeded limit set at 1000E-7
Minor	2015-11-24 13:20:57	2015-11-24 13:21:02	DVB-S/S2 2.1...	TS unstable	1101	PIDs: 0 new, 0 gone, 56 total, 13 CC errors....
Warning	2015-11-24 13:20:57	2015-11-24 13:20:59	DVB-S/S2 2.1...	PID error [PID: 17...	1160	PID 1739 (Teletext), Refs: 4013
Warning	2015-11-24 13:20:56	2015-11-24 13:21:25	DVB-S/S2 2.1...	CC error [PID: 78...	1140	PID 7800, Jumps: 8=>10,5=>7,12=>14,11...
Warning	2015-11-24 13:20:56	2015-11-24 13:21:20	DVB-S/S2 2.1...	CC error [PID: 17...	1140	PID 1731, Jumps: 1=>3,15=>1

Figure 8.11 Alarm log

The alarm log shows every alarm that has been triggered since the last time the alarm log was cleared, along with any alarms that were currently active when the alarm log was last cleared.

The Virtuoso will store up to 100000 alarm entries. When the log is full it will start discard the oldest entry when adding a new one. The alarm log is persistent, i.e. it will not be lost even if power is lost.

The table consists of the same columns as the Current Alarms table, but does not show details by default. Additionally a column named Off Time shows the time the alarm condition was cleared. Rows will not have the Off Time set if the alarm is still active.

Each row provides additional information via a tool-tip shown when hovering the cursor over the row. The tool-tip entries are:

Sequence #
: A number identifying this specific alarm instance. This number is incremented each time an alarm condition is raised.

SubID 1
: The primary numerical index of the alarm instance. This index is reserved for future use and is always set to 1 in the Virtuoso.

SubID 2
: The secondary numerical index of the alarm instance. When the alarm is of type Port alarm this index contains the port number for which the alarm was raised. Other types of alarms may use this index to identify a sub module, but normally it is set to 0.

SubID 3
: The tertiary numerical index of the alarm instance. The use of SubID 3 depends on the type of alarm. Some of the Port type alarms use this index to signal the PID value or Service ID for which the alarm was raised. For example, if the CC Error of a PID is raised then the PID value is given by SubID 3.

Details
: An optional string providing more information about the alarm in human readable form. The content and format of this string depends on the alarm type.

Description
: Description of what the alarm means. For ETR290 alarms, the specification is described.

Source
: The source of the alarm, whether it is a TS alarm for an ASI port (example ASI 1.1 > TS), a System alarm or an alarm related to RF parameters.

On time
: This gives the time the alarm was triggered

Off time
: This gives the time the alarm was turned off.

Severity
: The severity of the alarm described in text.

Alarm
: The title describing the alarm.

Alarm ID
: The unique ID for each type of alarm.

Beneath the alarm table is a caption showing the total count of alarms currently stored in the alarm log.

To the right of the table are four buttons and a check box.

Clear Alarm Log
: Clears all alarms from the alarm log.

Export to File
: Saves the alarm log to a comma-separated value (.CSV) file. The button opens a file dialog where the user can choose the destination to save the file on the computer.

Export to Browser
: Opens the complete log in a new browser window, showing the alarm log as a comma-separated value list. The format of this list is a text file (not HTML or XML).

Generate SLA
: Generates a service level agreement visualization based on the complete alarm log for the unit. This feature is described more in **Section 8.6.2.2.2**. This button also exists for every input, and will create an SLA report for the desired input.

Enable updates
: This check box can be unchecked to stop the log from scrolling if new alarms are triggered while watching the log.

8.3.6.2 SLA

The Service Level Agreement monitoring page is accessed by pressing the Generate SLA button which exists on the main page for every input. Additionally, the button exists on the alarm log page for each input, and on the alarm log page for the Virtuoso as a whole.

Pressing the Generate SLA button brings up a window showing the SLA generated from the alarm log, which can be presented in a number of ways. These visualizations include:

SLA (pie)

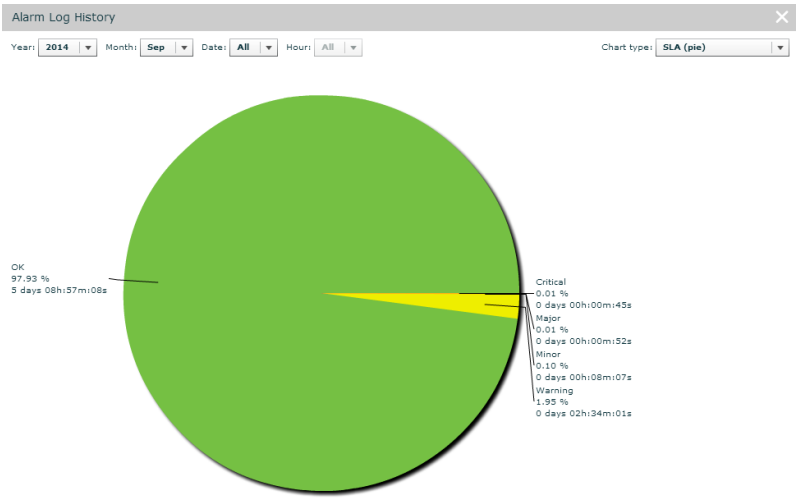


Figure 8.12 SLA Generator - Pie chart view of SLA

Figure **8.12** shows the pie view of the SLA. Each slice of the pie represents an alarm state, and visualizes the percentage of time that input has been in that particular state. Each area of the pie chart has indicators containing the data in numbers of the area's properties. This includes

the percentage, time in days, hours, minutes and seconds, and the name of the alarm state (also indicated by color).

SLA (column)

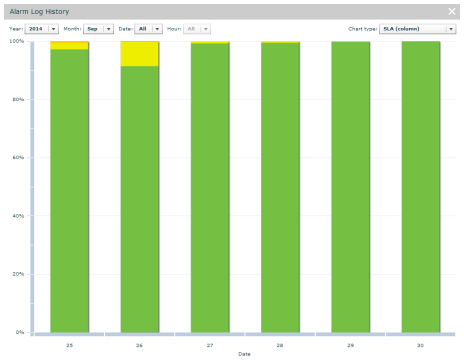


Figure 8.13 SLA Generator - Column view of SLA

Figure 8.13 shows the column view of the SLA. Each column is made up the various alarm states the input or system has been in since the stats were cleared. Essentially, this gives the same information as the pie chart, only in a different view. A mouseover of the different colored segments of a column will bring up the properties in numbers.

Severity changes

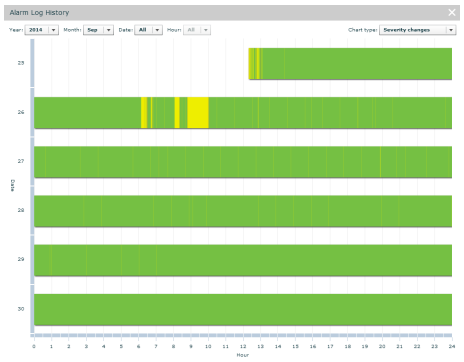


Figure 8.14 SLA Generator - Severity change view

Figure 8.14 shows the view which illustrates the severity changes of the input. This view visualizes the alarm state of the input or unit over time. Mouseover for any row of severity change bar will give details about the actual times the input changed severity, and what severity it changed to.

Simultaneous alarms

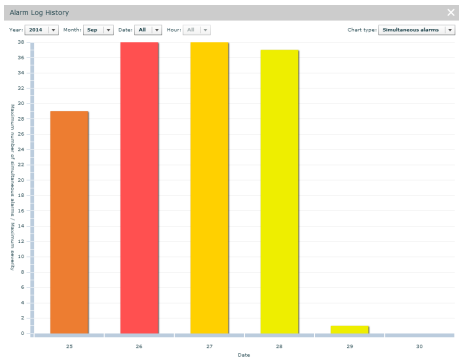


Figure 8.15 SLA Generator - Maximum number of simultaneous alarms

Figure 8.15 shows the fourth visualization mode for the SLA. This is a graph showing the maximum amount of simultaneous alarms for the input or for the unit as a whole. This is displayed using column bars, where the column height indicates the highest number of alarms the input or unit has has simultaneously.

8.3.7 New alarms

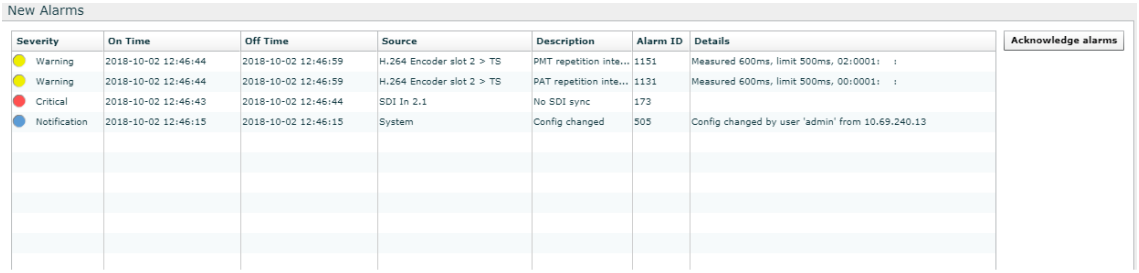


Figure 8.16 New alarms page

The new alarms page shows all new alarms that have been triggered since the last time the "Acknowledge alarm" button was pressed.

8.4 Device Info

The device info page contains all the information and settings that are not related to a single input or output port. It is divided into multiple sub pages accessed via the navigation list to the left. In the list of physical interfaces in the navigation list, the currently active interface is shown in bold. See Figure 8.17.

The exact layout of the navigator depends on the resources and features currently available in the device.

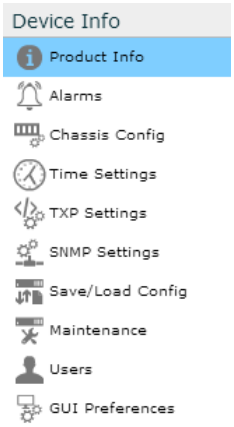


Figure 8.17 Device Info navigator

8.4.1 Product info

The product info page contains general device information.

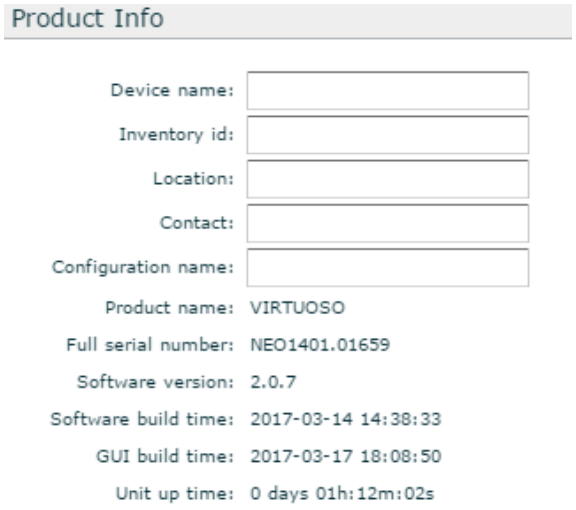


Figure 8.18 Product Information

Device name
: Configures the current user defined name of the unit. This parameter, together with the management network parameters are used as device identifiers and remain untouched if the unit configuration is changed by loading a different configuration file. See **Section 8.4.8**. The device name is shown in the web GUI status header (see **Section 8.3.1**), and in the web browser title bar to facilitate identification of each device.

Inventory ID
: Configures the current user defined inventory ID of the unit. This parameter, together with the management network parameters are used as device identifiers and remain untouched

if the unit configuration is modified. It is only intended as a label/tag and will not affect the operation of the unit.

Location
: Configures a location for the unit. The same remarks as those made for Inventory ID applies.

Contact
: Configures a contact for the unit. The same remarks as those made for Inventory ID applies.

Configuration name
: Configure a user defined name for the current configuration of the unit. This name is displayed to the left in the status footer as shown in **Figure 8.4**. The Configuration ID does not, as opposed to the Name and Inventory ID fields, remain untouched when loading a new unit configuration. Loading a new unit configuration will change the Configuration ID. See **Section 8.4.8** on how to load a new configuration.

Product name
: Displays the name of the product as designated by Nevion.

Full serial number
: The serial number of the device.

Software version
: The version of the software currently installed on the device. The software version is given by the following syntax:

  `<major_version>.<minor_version>.<patch_version>`

  The convention for the SW version numbering is as follows:

  major_version
  : Incremented for significant SW changes.

  minor_version
  : Incremented for minor changes. The minor version number is even for official retail releases and odd for beta releases.

  patch_version
  : If minor_version is even, patch_version gives the patch level of that version. A patch level of zero means the SW is built on the latest code base, an even patch_version means this is a released SW patch on a previous release. An odd patch_version means that this is a test version. If minor is odd, this is a beta version, and the patch_version simply gives the build number.

Software build time
: Reports the time of which the current release image was built.

GUI build time
: Reports the time of which the current user interface was built.

Unit up time
: The amount of time that has passed since the device was last reset.

8.4.2 Alarms

The Alarms page is shown in Figure 8.19:

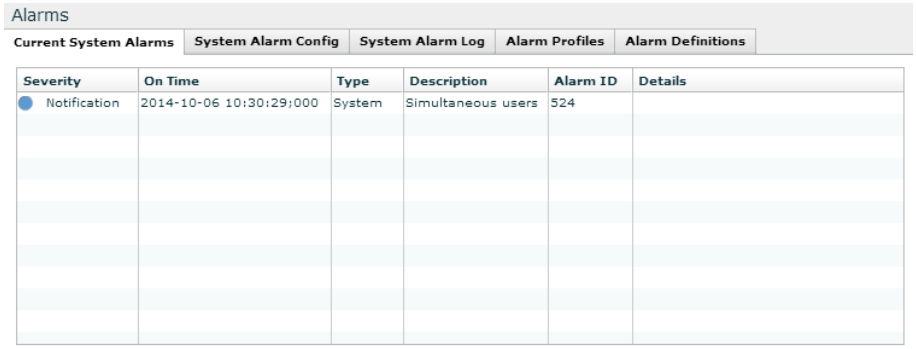


Figure 8.19 Alarm main page showing current system alarms.

The front page of the Alarms page for the Device info shows the currently active alarms on the system. It gives access to the following sub pages:

- System alarm config
- System alarm log
- Alarm profiles
- Alarm definitions

8.4.2.1 System alarm config

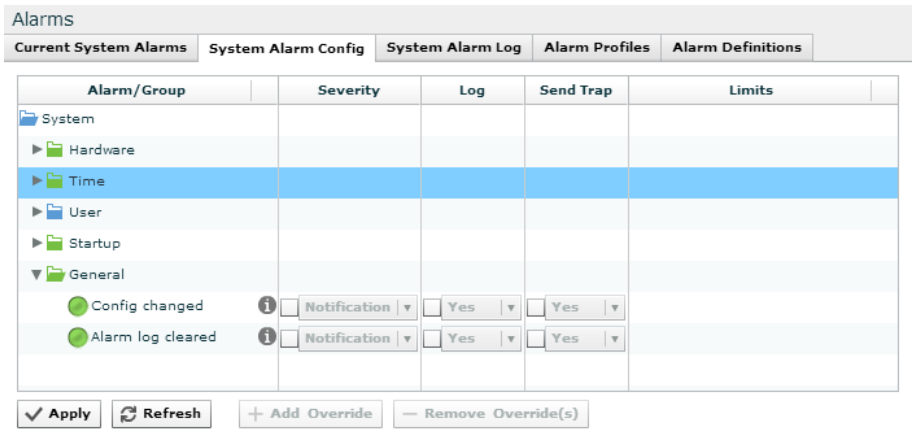


Figure 8.20 Global alarm configuration

This sub page shown in figure 8.19 allows the user to configure all the system alarms which are defined on the Virtuoso. As an example, the user can define the “Config changed” alarm to be of severity level Critical by ticking the box and changing the severity in the dropdown box shown in the figure.

8.4.2.2 System alarm log

This page shown in figure 8.21 shows the all the entries from the alarm log which are in the System source category. This log has the same entries as the main alarm log which was described in Section 8.3.6.

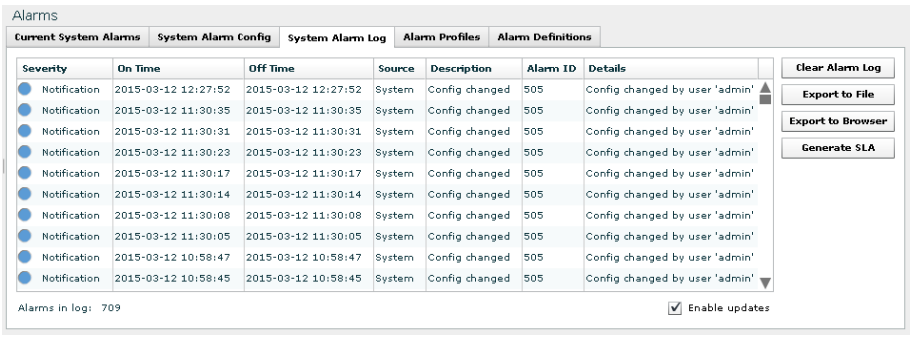


Figure 8.21 System alarm log.

8.4.2.3 Alarm profiles

The alarm profiles subpage lists all the profile categories that exists for the Virtuoso. This is shown in figure 8.22. For each profile category, the user can view which saves profiles exists for each one.

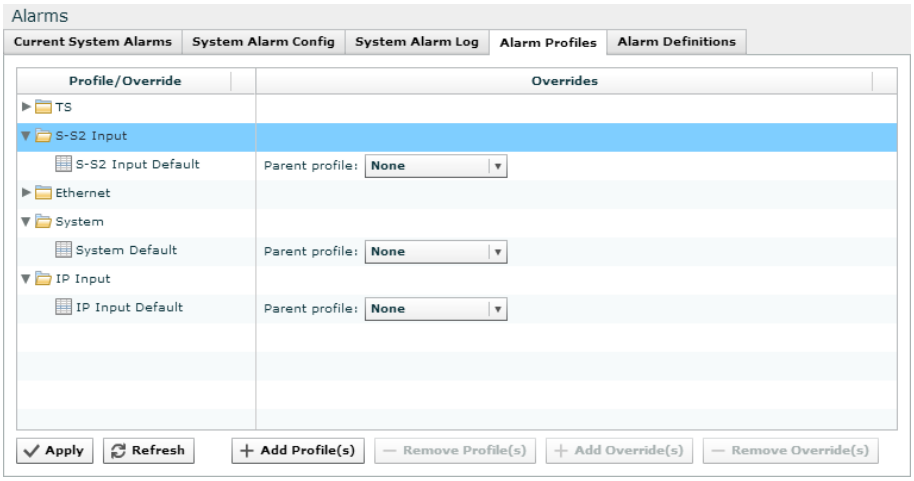


Figure 8.22 Alarm profiles.

8.4.2.4 Alarm definitions

This page shown in figure 8.23 gives a full list of all the alarms defined on the unit. The list is searchable, and gives information about all the alarms. This information contains the type, title, alarm ID, severity and a description of the alarms.

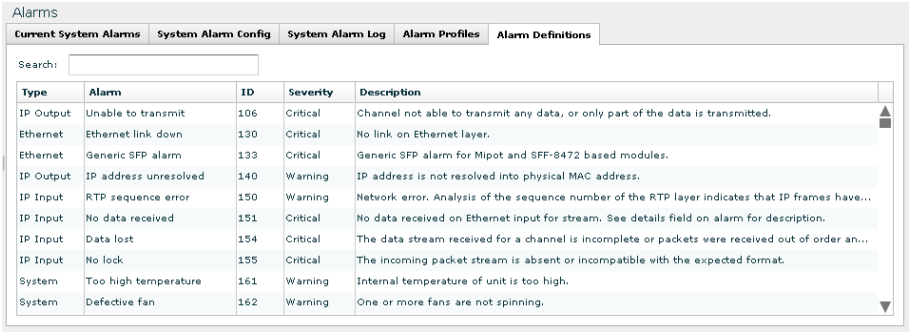


Figure 8.23 Alarm definitions.

8.4.3 Chassis Config

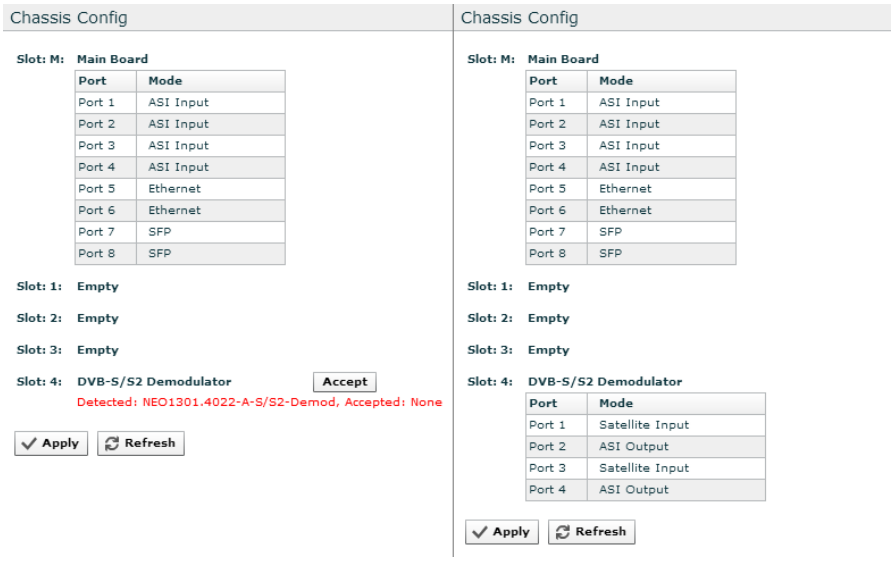


Figure 8.24 Chassis config page for Virtuoso. Left shows before accepting configuration, right picture shows a completed configuration for the chassis.

The “Chassis config” page is accessed by going to “Device info”, and choosing “Chassis config” in the navigator on the left side.

This page will show the list of the boards in the current unit, with its inputs and outputs.

8.4.3.1 Accepting new boards

If a new board has been added to the unit, it will appear in red font and have an Accept button next to it, as shown in left in figure 8.24.

If a new daughter board has been added into the Virtuoso, the user shall go to this Chassis config page to configure the newly acquired I/O board. This is needed in order to add the physical ports into the configuration system. This is done in the following way:

1. Browse to “Device info -> Chassis Config” in the Web GUI. A page similar the left in figure 8.24 should appear.
2. The page shows a list of the boards in the unit, including the main board. For the new board, there will be an Accept button belonging to it, as shown in the figure. Press this button to add the board with its inputs and outputs to the configuration.
3. For any boards where the ports are configurable in direction, there will be a dropdown menu to pick the available options from here.

The effect of accepting the boards like this, is to get the unit configured with the correct inputs and outputs. For certain boards, this is where you change a directions of a port, if it is bi-directional. Otherwise, the page will only serve as a reference to confirm the ports and boards currently in the unit.

8.4.3.2 Ejecting/removing boards

To prepare a board to be removed while the unit is operational, press the Eject button next to it. The configuration associated with the board will be deleted, and the card can be removed from the unit.

8.4.3.3 Select/change SW type

Some boards support running different types of SW images, for example the High Bitrate accelerator board. Next to the card there is a drop-down list over valid SW images loaded onto the board. Select the desired application and press the Accept button. The current configuration for the card will be deleted, and the card will have to be accepted after a reboot.

8.4.4 Time Settings

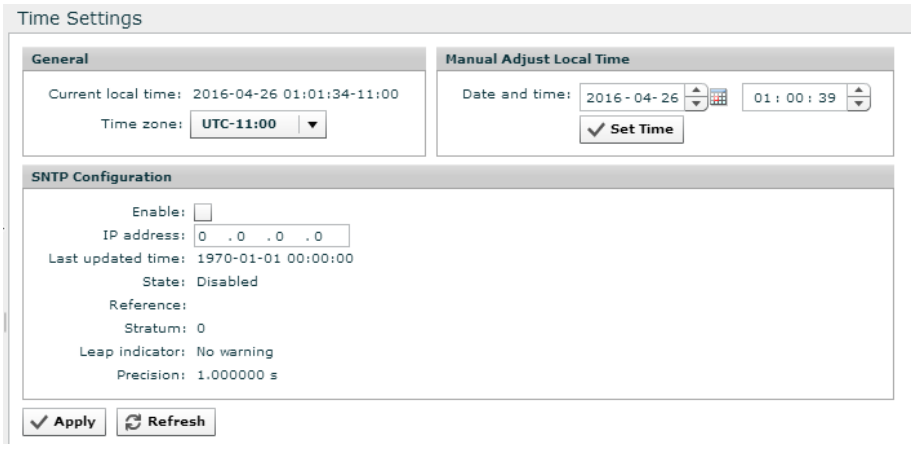


Figure 8.25 Time Settings

The time settings page contains settings related to internal time on the unit. Time is mainly used for reporting alarms, but may also be used by some other modules.

The time source page lets the user configure time zone, the source for synchronising the internal device time clock and set the internal clock in case of failure of all external sources of clock synchronisation. The main use of the device time is stamping the entries of the alarm log.

The page consists of several parts. Top left is the General box, containing the following parameters:

Current local time
: The current time as reported by the device.

Time zone
: Drop-down list to configure the time zone of the unit.

The Manual Adjust Local Time section gives the user one field, Date and Time, in which the user can manually input the local time for the unit to be configured with. Note that if any SNTP server is enabled and responding the manually set time will be overridden.

The SNTP Configuration section allows the user to specify the address of two SNTP servers. The unit will always prefer the main SNTP server, but will fall back to the spare one if main does not respond. The section contains the following fields:

Enable
: Enables the SNTP as a timesource.

IP Address
: The address of the SNTP server to use as a timesource.

Last updated time
: The last time the timesource was changed.

Used as reference
: Indicates which SNTP server is currently being used by the unit.

State
: The current state of the timesource. Can be Ok, Not OK, Never OK, Disabled.

Reference
: Provides the time reference source address of accessed time source.

Stratum
: Indicates the hierarchy level of the current time source. The master reference is at stratum 0 (highest).

Leap indicator
: Indicator of leap second warning level. Can be No warning, Last minute has 59 seconds, Last minute has 61 seconds and Not synchronized.

Precision
: The expected timing accuracy of the current time source.

8.4.4.1 Daylight Saving

Enabling automatic daylight saving time functionality will adjust the local time of the unit. The current time will show the daylight saving adjusted time, with correct UTC offset. This will mainly have an effect on alarm log entries and reading the time from the GUI. When enabled, there are four DST modes to choose from:

Europe
: Standard European settings. Daylight saving time starts on the last Sunday in March at 1AM UTC, and ends on the last Sunday in October at 1AM UTC.

USA
: Standard USA settings. Daylight saving time starts at 2AM local time on the second Sunday in March, and ends at 2AM local time on the first Sunday of November. This setting does not take into account the exceptions where daylight saving time is not observed, such as Arizona, Hawaii, Puerto Rico, American Samoa, Guam, Northern Mariana Islands and the United States Virgin Islands. These locations should simply have daylight savings time disabled.

Manual dates
: Manual dates which can be inputted in the autumn and spring fields that appear when this option is chosen. Will only occur on these times, and need to manually be updated in order to change the following years. If both the manual dates has passed, the time is set to not be in daylight saving, even if the last date was a spring date. The number of minutes to adjust the time for daylight savings can be set in the Offset in minutes field.

Manual recurring
: Gives drop-down lists to input a rule, such as "First Sunday in February 02:00". This will set dates based on the selected input, and happens each year on that day. The number of minutes to adjust the time for daylight savings can be set in the Offset in minutes field.

On the right hand side of the page some status information is shown to indicate the status of the daylight saving time module.

Now in summer time
: Whether or not the current time is in daylight saving time (summer time).

Time to next change
: Countdown to the next time will be adjusted to or from summer time. If it displays "No change set to occur", the mode is likely set to Manual dates, with the two set dates having passed, or minutes offset being set to 0 minutes.

Minutes DST offset
: Number of minutes the clock is set to change by for daylight saving.

Next spring change
: The spring date for the next daylight saving change.

Next autumn change
: The autumn date for the next daylight saving change.

8.4.5 Clock Reference

8.4.5.1 PTP Clock Reference

This page lets the user choose from Ethernet interfaces that has support for IEEE 1588 v2 and use them as the clock reference for the unit. The page features configuration and status overview of the enabled PTP interfaces, as well as an alarm configuration for each interface.

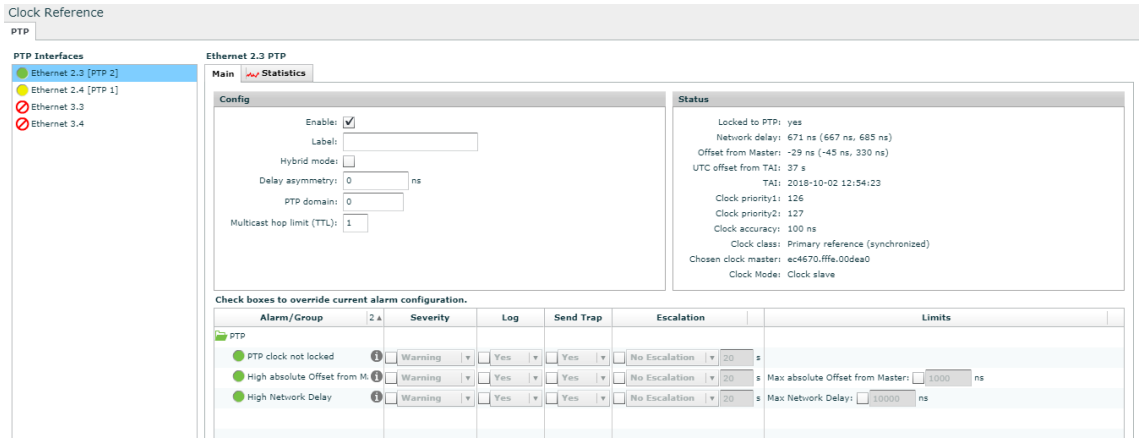


Figure 8.26 PTP Clock reference page

The configuration window has the following options:

Enable
: This will enable the reception of IEEE 1588 v2 and will be used as a clock reference if a valid signal is found.

Label
: The displayed name for the PTP interface.

Hybrid Mode
: Enabling this will make delay requests be sent to the unicast address taken from the masters announce message.

Delay asymmetry
: This value is used for compensate for any delay asymmetries between reception and transmission data path in the network. This can occur if the data path of the PTP messages travels through switches that does not compensate for processing delay and/or link speed conversion.

PTP Domain
: Selectable PTP domain. Choose the domain that the grandmaster clock transmits on.

The status window has the following fields:

Locked to PTP
: Yes or no, dependent on the input signal. If it cannot lock it will trigger "PTP clock not locked" alarm.

Network delay
: The measured network delay between the client and the master.

UTC offset from TAI
: The time offset in seconds between UTC and TAI. The difference is the amount of leap seconds that has been added to the UTC time.

TAI
: TAI time.

Clock Priority 1
: Clock priority 1 field in IEEE 1588. This is configured on the clock master in the system.

Clock Priority 2
: Clock priority 2 field in IEEE 1588. This is configured on the clock master in the system.

Clock accuracy
: The accuracy of the master clock.

Clock class
: The clock class specifier of the reference that the master clock uses.

Chosen clock master
: The ID of the currently chosen clock master.

Clock Mode
: The clock mode of the client. Currently only clock slave is supported.

8.4.6 TXP Settings

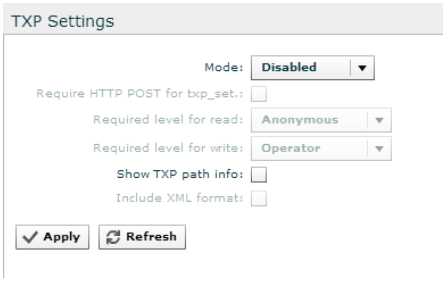


Figure 8.27 TXP settings for Virtuoso.

The TXP Settings page shown in figure 8.27 is the page to configure the TXP protocol communication with the unit. TXP is used for simple and fast access to the unit, either from a NMS or from scripts. TXP may be used to extract the same information as shown in the GUI and configure the same settings. There is a separate document describing this protocol, which you may get be contacting Nevion support.

It contains the following configurations:

Mode
: Whether the TXP protocol should have read only access, read/write access or is disabled.

Require HTTP POST for txp_set
: Require HTTP POST for txp_set operations. If unchecked, GET operations will be accepted. This is not recommended, as the risk of unwanted configuration changes increases.

Required level for read
: Set the user level which is required to perform reading operation using the TXP protocol.

Required level for write
: If mode is set to read/write access, this field sets the user level which is required to perform a write operation using the TXP protocol.

Show TXP path info
: If enabled, information about path and attribute will be shown in the bottom left corner when hovering the mouse over most GUI components that are bound to a TXP value. Right clicking on a page with bindings will also allow copying binding information to the clipboard.

Include XML format
: If enabled, a TXP XML version will always be copied to the clipboard in addition to the TXP string version. If disabled the XML version will only be copied if there is no TXP string version that will work.

8.4.7 SNMP Settings

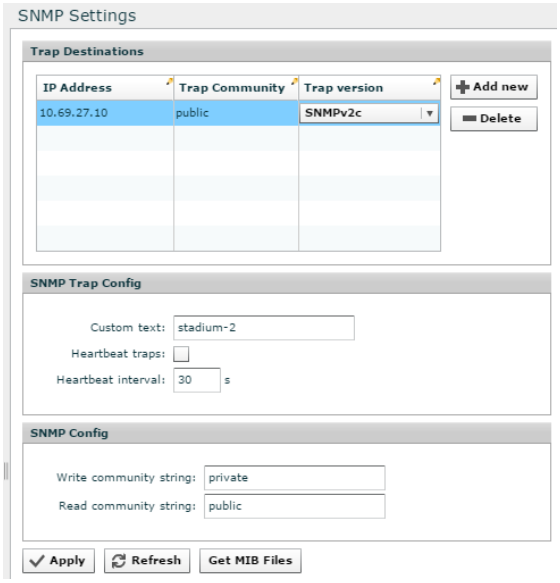


Figure 8.28 SNMP settings page for Virtuoso.

Trap Destinations

The SNMP Settings page allows the user to add several SNMP trap destinations.

Pressing the Add new button adds a new row to the trap destinations list shown in figure 8.28. On this line, the user can input the

IP address
: This is the IP address for the SNMP trap destination.

Trap community
: Here the user can input trap community string to send the message with.

SNMP version
: Set the SNMP version. Currently supported are SNMPv1 (legacy) and SNMPv2c.

SNMP Trap Config

Custom text
: This text field is inserted into every trap, as a way of identifying the SNMP trap sender without using the source IP address.

Heartbeat traps
: Enabling this will send a Trap every X number of seconds to notify to SNMP receiver that the unit is alive. The heartbeat trap is a regular alarm with id 536.

Heartbeat interval
: Number of seconds between each heartbeat trap.

SNMP Config

The SNMP config controls the community string for SNMP read and write, i.e. simple passwords.

Write community string
: A SNMP write request need to use this password to be allowed to change parameters.

Read community string
: A SNMP read request need to use this password to be allowed to read parameters.

8.4.8 Save/Load Config

This page provides an interface to extract the currently used configuration of the unit, or to load a new configuration on the unit. Configurations that are extracted from the unit may be loaded onto other units. IP address settings will not be copied between units.

The configuration are XML files, and may be edited offline.

8.4.8.1 Save Configuration To File

This is the interface for exporting the current running configuration as an XML file. Clicking the Save Config button prompts the user with a standard Save as dialogue requesting a location to store the configuration file. This location can be any place the user has access permissions to write files.

During the transfer of the file from the device to the user's system the user has the ability to click the Cancel button to cancel the transfer. Note that, depending on the web browser used, an incomplete file may be left on the user's system after canceling.

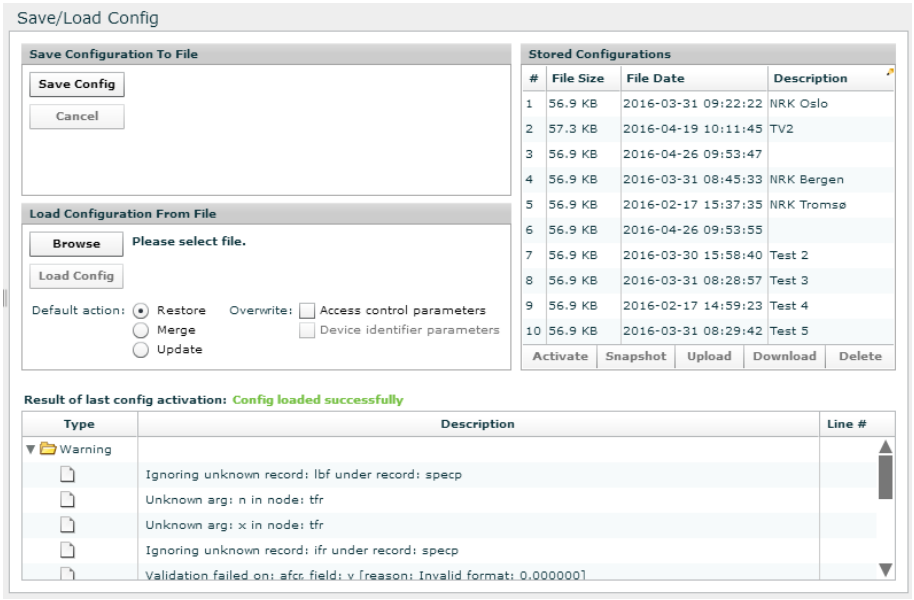


Figure 8.29 Configuration manager

Upon completion of the transfer the transfer progress bar will turn green. If an error occurs during the transfer the progress bar will turn red and display an error message.

Files exported from the device using this option contain a complete device configuration and can be restored to the device at a later time. Or it may be installed on another device using the Load Configuration option.

8.4.8.2 Load Configuration From file

The Load Configuration From File field of the page provides a mean to directly import a file-based configuration snapshot as the new running configuration. All options from the snapshot are loaded and verified before making them active, thereby minimizing the risk of errors in the file that would render the device in a non-operational state.

Clicking the button marked Browse prompts the administrator with a standard system File Open dialogue allowing the administrator to select the file of his choice to import. Once selected, clicking Load Config performs the following actions :

- Transfers the configuration snapshot from the administrator's PC to the device.
- Validates the configuration to make sure that all the options in the file are compatible with each other and with the device itself.
- Presents the user with additional information, such as skipped options.
- Activates the configuration.

When an import has been successfully completed the progress bar color turns green and changes its text to OK. Upon failure at any point the progress bar will turn red, and details of the reason for the failure will be presented as messages in the Result of last config activation list.

By default, options specific to the device, including device name and management port network configuration, are disregarded during the import process. This is a convenience feature allowing configurations to be easily moved from one device to another. It also makes management easier in that the Web UI will continue to communicate with the device after a new configuration has been loaded. The default behavior can be changed with the load options, please see **Section 8.4.8.2.1** for a description of the options.

Partial configuration files are supported to allow a subset of configuration options to be changed instead of the entire unit configuration. Partial configuration files are validated as differences from the current running configuration upon import before being made active.

8.4.8.2.1 Load options

These options are used to modify the behavior on configuration loading. The options are available when loading from a file (**Section 8.4.8.2**)

.

Default action
: This parameter modifies the algorithm used when modifying lists (collections) in the configuration.

  Restore
  : Modify list to contain exactly the entries specified in the file loaded.

  Merge
  : List entries that are present in the running configuration but not in the file loaded are left in the list. New entries specified in the file loaded but not in the current configuration are added. Entries present both in file loaded and in running config are modified.

  Update
  : Only update nodes that are present in running configuration and in file loaded, i.e no list entries are added or removed.

Overwrite
: This parameter is used to modify how specially tagged parameters are handled during file loading.

  Access control parameters
  : Tick to overwrite SNMP community strings and TXP access parameters.

  Device identifier parameters
  : Tick off his check box to overwrite the device identifiers device name and inventory ID. Ethernet Interface IP addresses are not overwritten using this option.

8.4.8.3 Stored Configurations

The table on the right of the page provides an interface to management of on-device stored configuration snapshots. Up to 10 full system configuration snapshots can be stored.

The table lists the currently stored snapshots, and columns in the table provide information specific to each snapshot as follows:

File Size
: Size of the configuration file.

File Date
: Date at which the file has been created (snapshot or import of an existing configuration file).

Description
: A descriptive text can be entered in this field by clicking on the field itself and typing text.

At the bottom of the table several buttons are provided to perform the following actions:

Activate
: Loads the selected snapshot as the active configuration of the device.

Snapshot
: Stores the current running configuration as a snapshot in the slot selected in the snapshot table. This operation will overwrite the configuration file currently stored in that position.

Upload
: Imports a configuration file from disk to the selected slot. This operation will overwrite the configuration file currently stored in that position.

Download
: Downloads the selected configuration file to disk.

Delete
: Delete the entry selected in the snapshot list.

At the bottom of the page is the Results of last config action field, which will show the result and a list of errors (if any) of the last action performed.

8.4.9 Maintenance

The Maintenance page centralises information regarding the hardware configuration of the device and provides a means for updating firmware images and managing software feature licences.

The page gives access to three sub-pages described below.

8.4.9.1 General

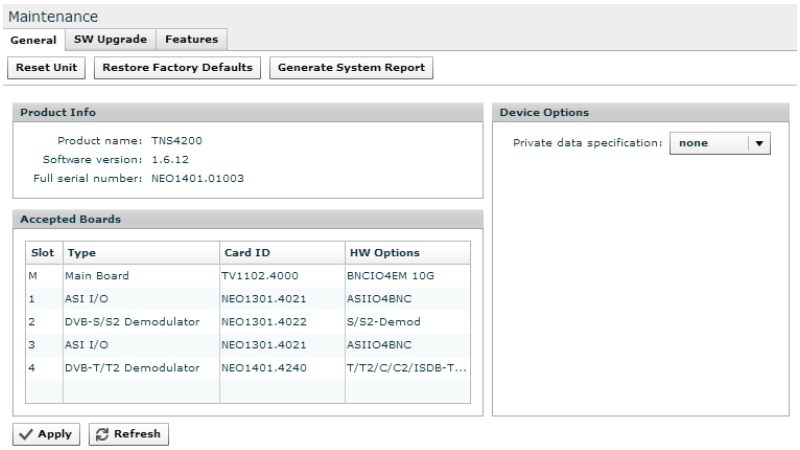


Figure 8.30 Maintenance

The General tab on the maintenance page details the current software, hardware and licence configuration of the device. Note that the items listed vary between devices.

At the top are two buttons for resetting purposes:

Reset Unit
: Provides an interface to perform a restart operation on the unit. Following a restart boot delay the user is prompted to reload the Web UI in the browser.

Restore Factory Defaults
: Resets all non-device specific settings to the factory default settings. Settings remaining unchanged include the device name and the management interface IP configuration. This will also reboot the unit.

Generate System Report
: Generates an status report of the unit in XML format. Please attach this system report when contacting Nevion Customer Support.

The Product info field provides the following information:

Product name
: This is the product model name.

Software version
: The version of the firmware image installed in the unit.

Full serial number
: The manufacturer assigned serial number used for warranty and software licensing.

The page also shows a list of accepted boards in the Virtuoso chassis. The list contains the following information about the accepted boards:

Slot
: Which slot in the chassis the board belongs to.

Type
: Description of the type of board.

Card ID
: Board identification code.

HW Options
: Describing the hardware options of the boards installed.

8.4.9.2 Software Upgrade

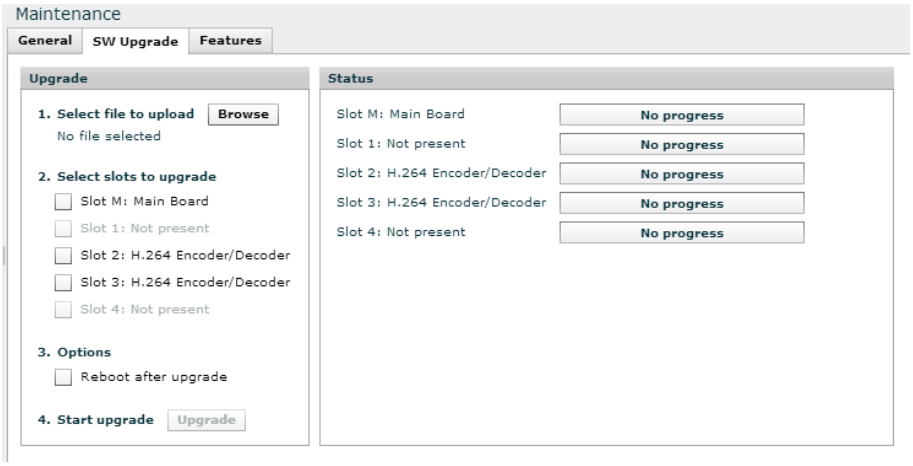


Figure 8.31 Software Upgrade

The Software Upgrade sub-page lets the user upgrade the software of the device. The upgrade is accomplished in four steps:

Browse
: Prompts the administrator with a standard system Open file dialogue to specify the new software image file to install.

Select slots to upgrade
: The user selects which part of the system to upgrade with the selected software image. Only the main board and the slots that are upgradable are selectable.

Options
: Reboot after upgrade: if selected (by default), the unit will be rebooted upon SW loading completion. If this option is not checked the SW will be loaded but will not be activated before the user performs a manual reboot. Note that this option is not stored on the device, and Reboot after upgrade will be enabled next time you enter the SW upgrade page.

Start upgrade
: The upgrade procedure is initiated. The status of the transfer for each slot is visible in the status bars in the Status section, and operation can be aborted at any time by pressing the Cancel button. Once the file has been transferred, it is verified using and internal checksum value and set as the new active firmware image.

If the upload is successful the progress bar turns green and the unit reboots itself loading the new image, unless the Reboot after upgrade option has been unchecked.

If the upload is unsuccessful the progress bar turns red and an error message is displayed in the Status section.

Multiple SW images

Note that some boards supports multiple SW images (ex. the High Bitrate Accelerator Board). For those boards the uploaded image will automatically replace the existing image of same type. To active a new type of image, go to the Chassis Config page after upload. Figure **Figure 8.32** shows existing software images on the different boards. If there is no room for more SW images, select an image and press the Remove images button.

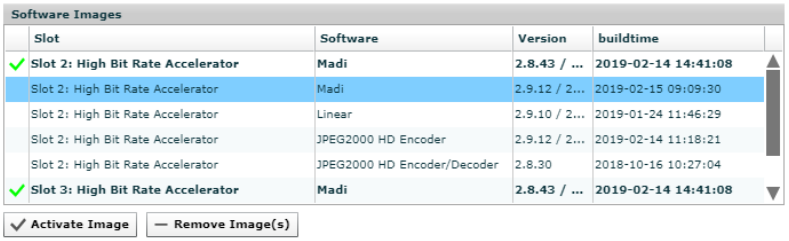


Figure 8.32 Software Images

After uploading, if the Progress bar shows OK but the web interface does not change to the Waiting for reset state, allow some time for the device to reset itself and then reload the web UI via the web browser reload button.

Note: It is recommended to verify the new software version via the "Product Info" page (**Section 8.4.1**) to verify that the update was successful and the latest software revision is active.

8.4.9.2.1 FTP upgrade

It is possible to perform a software upgrade using FTP. The Virtuoso has a built in FTP server which gives access to the application image. Connect to the unit using any FTP client and log in as admin (see **Section 7.2**). Replace the /flash/app.bin by your newer application image. Reboot the unit. Note that replacing the SW image with FTP will disable the built in checks to see if the SW image is compatible and valid. It also opens the possibility to load a SW image that is outside the maintenance period. (see **Section 8.4.9.3**)

8.4.9.3 Features

The Features sub-page provides two tabs, Feature List and Upgrade.

Feature list

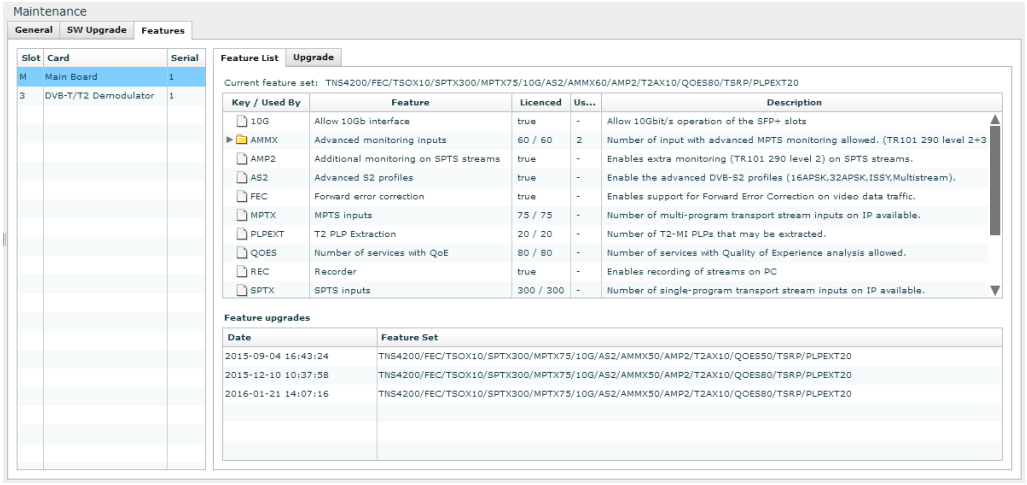


Figure 8.33 Feature List page

After having selected the device or a slot, the Feature List tab shown **Figure 8.33** gives a list of the all the software features and their current value on that slot.

Key / Used by
: Contains the key of the licence type. The licences are usually represented as a file. If the licence is associated with a number of ports (the value field is a number), then the licence is shown as a folder and all the ports using one instance of the licence are listed within it.

Feature
: Contains the licence name and for each port, depending on the type of feature controlled by the licence, it is possible to:

  - disable a port
  - disable the feature on one port
  - convert the feature to a related one.

Value
: Each licence is associated with a value which may be false/true or a number. In the first case the value simply states whether the feature controlled by the licence is available on the unit. In the case of the second case, the value states the maximum number of simultaneous usage of a given feature.

Description
: Contains a detailed description of the particular licence.

Maintenance licence

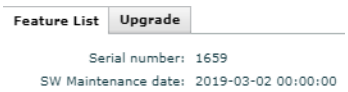


Figure 8.34 Maintenance licence expiration date

The software maintenance licence shows the current maintenance date of the unit. You will not be able to load a Virtuoso SW image that has been built after this date. An alarm is triggered when the maintenance licence has expired. Contact support to renew your licence.

Feature upgrade

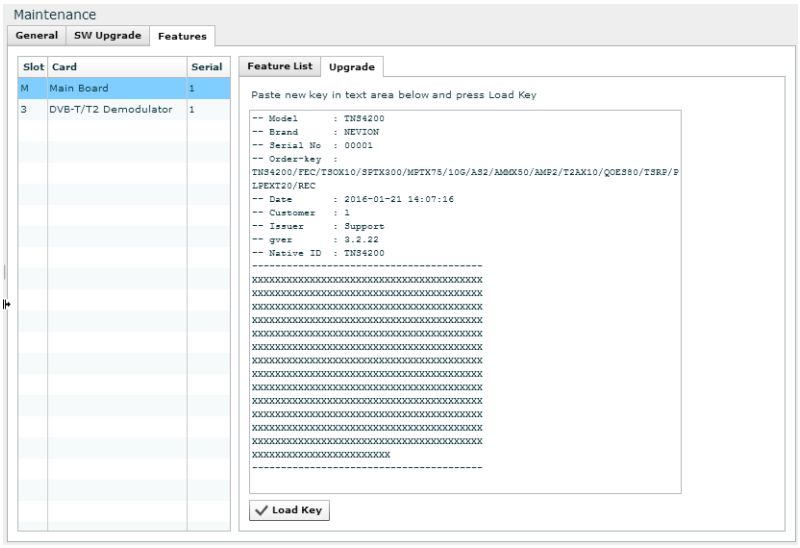


Figure 8.35 Feature Upgrade page

In the Upgrade tab shown **Figure 8.35**, the user is provided an interface to upload new software licenses to upgrade the feature set of the Virtuoso as well as the cards optionally attached to the slots. The license key is provided as a text file. Select the slot to update, paste the content of the file into the text area and click the Load Key button.

Reset can be performed from the GUI as explained on the Maintenance > General tab in **Section 8.4.9.1**.

Note: The entire content of the licence key text file must be copied into the text box, not just a portion of the file.

8.4.10 Users

The Users page (**Figure 8.36**) provides a simple interface for selecting unit log in mechanism and for managing user accounts. Additionally, it presents a view of all active GUI sessions.

Auto login

With this option an operator can enable automatic log in to the unit. When enabled a user is automatically logged in without the initial login screen (cf. **Figure 8.2**). The user identity is set to "autologin" and the access level is set to the selected access level.

To change the identity when the automatic log in is enabled, a user can use the "Change user" link located in the black ribbon at the top of the web page (cf. **Figure 8.3**)

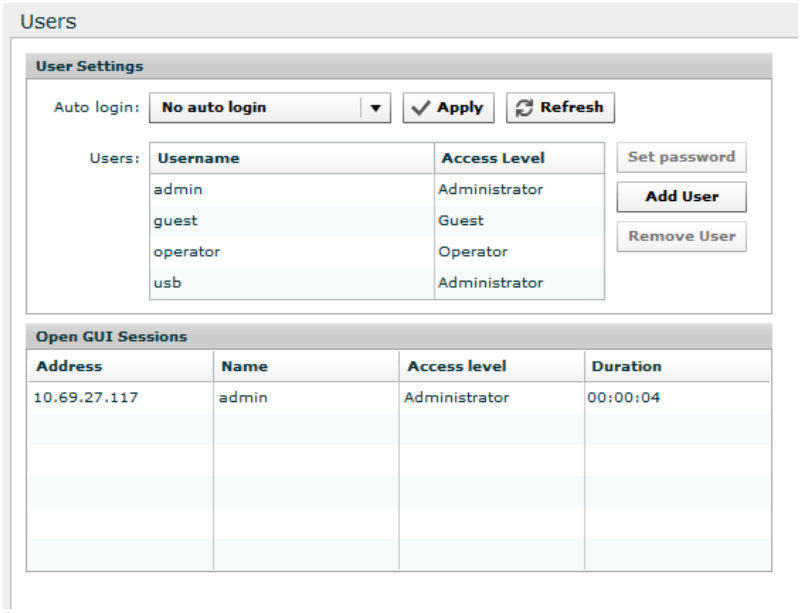


Figure 8.36 Users page

Users
: The Users table lists user accounts available in the system along with access levels. The view is only available to administrator users. An administrator can add a new user, delete, or change password of an existing user. A user name can only be composed of alphanumeric and underscore characters.

  A few user names are reserved by the system. On an attempt to create a user with such name, an administrator will receive a message "User name 'username' is reserved".

The account system provides three basic user access levels:

Guest
: A guest can view configuration information and alarm logs.

Operator
: An operator can configure the unit settings. However, it cannot view or modify the user account settings.

Administrator
: An administrator has full access to the unit.

The bottom window on the page presents a list of all active GUI session. It includes information about the peer IP address, user name, access level, and sessions duration.

8.4.11 GUI Preferences

The GUI Preferences page contains settings that affect the web interface.

Enable confirmation on Apply
: Configures the web UI to prompt users for confirmation before committing changes to the

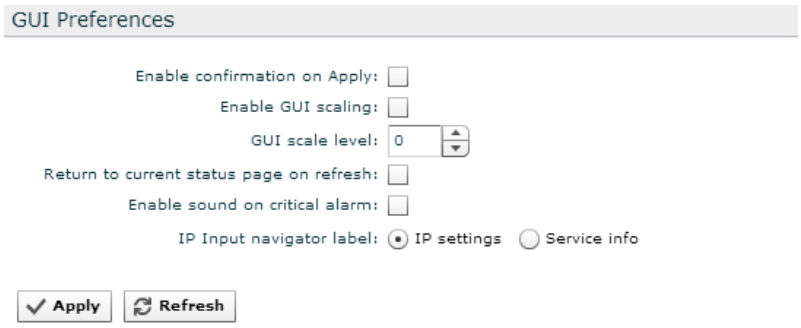


Figure 8.37 GUI Preferences page

device configuration. When disabled the Web UI will only prompt for confirmation prior to performing severe operations such as device reset.

Enable GUI scaling
: If enabled, the web interface will be shown with the currently configured GUI scale level. It also enables the use of CTRL + + and CTRL + - to change scale level. When enabling or disabling this option the web interface may hang for some seconds as it changes the font used.

GUI scale level
: The current scale level for the GUI. This is ignored if GUI scaling is not enabled. A value of 0 means normal size.

Return to current status page on refresh
: Check this to return to status page once refreshing the GUI WEB page. If not checked, you will return to the last visited sub-page when reloading the page.

Enable sound on critical alarm
: This option makes the computer play an alarm sound continuously if browser is connected to unit while it has a critical alarm. Use with care.

Note: Every browser session will play sound independently of each other if you enable this on multiple devices and/or have multiple open browsers.

IP input navigator label
: This can be set to IP Settings or Service info, depending on whether the user wants to see the IP settings of the input in the IP input overview described in **Section 8.6.1.3** or the service info of the input. Setting it to IP Settings will show the IP address of the input in the overview, while setting it to Service info will give a service info description in the IP input overview.

Note: 'Enable confirmation on Apply' is stored on the device, while the other options are stored as browser cookies and thereby only affect the local browser and PC.

8.5 Network

The network page contains all the information and settings that are related to the Ethernet ports on the device, such as setting network configurations, adding VLAN or searching for transport stream traffic on links with the IP snooper. It is divided into multiple sub pages accessed via the navigation list to the left, shown in figure 8.38.

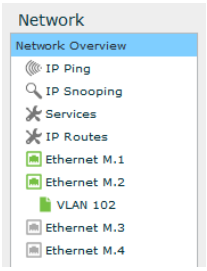


Figure 8.38 Network page navigator

8.5.1 Network overview

The network overview shows the list of Ethernet ports on the unit. As shown in figure 8.39, it gives some status of the different Ethernet ports, like the IP address or host name, the link speed of the port, whether in duplex mode and the current TX and RX bitrates.

Network Overview

Interface	IP Address / Hostname	Link Speed	Duplex Mode	TX Bitrate [Mbit/s]	RX Bitrate [Mbit/s]	Enabled	Data	Management
Ethernet M.1		1000 Mbit/s	1	104.678	426.222		-	
Ethernet M.2		1000 Mbit/s	1	662.984	517.014		-	
Ethernet M.3		1000 Mbit/s	1	35.096	834.681		-	
Ethernet M.4		1000 Mbit/s	1	367.809	123.020		-	

Figure 8.39 Network overview page for the Virtuoso, showing all the Ethernet interfaces and their current status.

8.5.1.1 IP Ping

The IP Ping page present two tables of IP targets currently probed by the unit. The top table contains targets that were selected manually by a user. A user can add a new target to the table by using the interface located next to the "Start Ping" button. A new target is defined by typing the IP address in the left window and the probe interval time in the right window. The unit begins to probe the selected target immediately after click on the "Start Ping" button.

The bottom table contains targets that were set automatically as a part of the TS IP output configuration. The configuration is available in the "Outputs" section under the IP Destinations/Ping page (cf. Section 8.10.2.3.4). A user can stop probing a target either from the IP Destinations/Ping page or by click on the "Stop" button located in the right column of the table.

The tables provide the following information elements about probed targets:

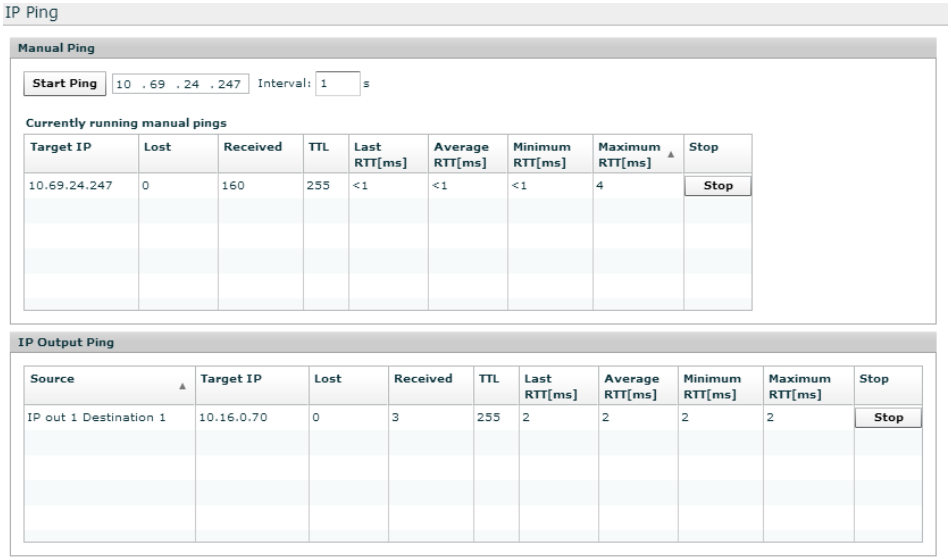


Figure 8.40 IP Ping tool page

Source
: Identifies IP output element that set up the probe - only applicable for IP Output Ping

Target IP
: IP address of the probed target

Lost
: Total amount of probe packets lost in the network

Received
: Total amount of received probe packets

TTL
: Time To Live (TTL) of the last received packet

Last RTT[ms]
: Last measured Round Trip Time (RTT)

Average RTT[ms]
: Average Round Trip Time (RTT)

Minimum RTT[ms]
: Minimum Round Trip Time (RTT)

Maximum RTT[ms]
: Maximum Round Trip Time (RTT)

Stop
: Stop probing the target

8.5.1.2 IP Snooper

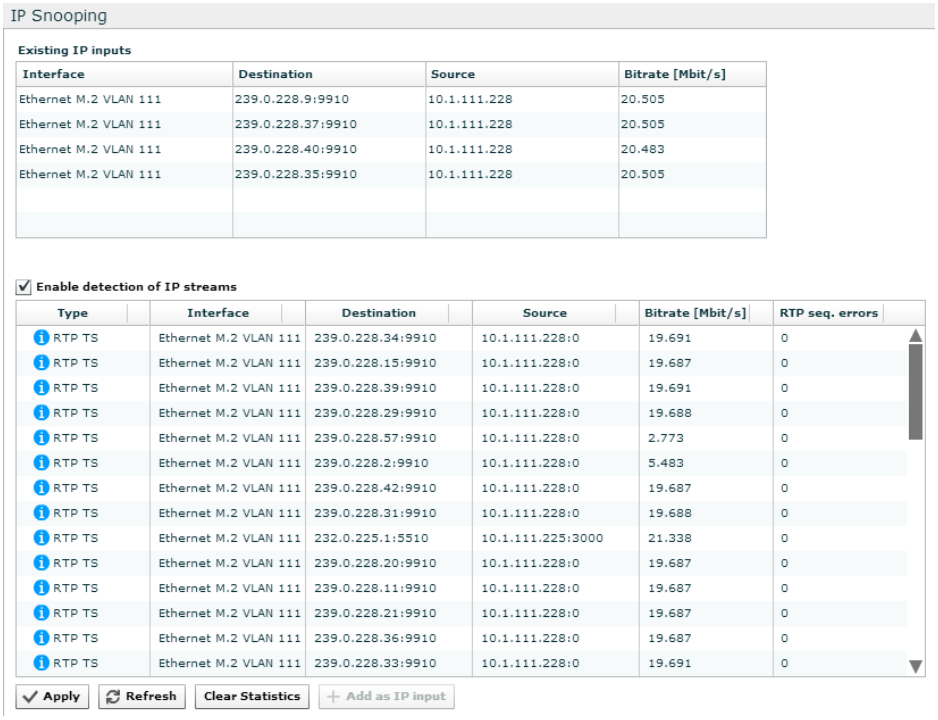


Figure 8.41 IP Snooper page for Virtuoso.

The IP snooper is a helpful tool to detect existing transport streams on a link connected to the port. The user interface for the IP snooper is shown in figure 8.41. By simply pressing the tick box entitled Enable detection of IP streams, and then the Apply button, any incoming streams on IP will show up in the table below the tick box, if any are detected. It is recommended to only have this feature enabled while configuring this unit, as the IP snooping feature is quite resource intensive.

The IP snooper will show any multicast or unicast streams available at any of the Ethernet interfaces. Note that streams will not be detected on the Ethernet interface unless other network equipment forwards these streams to the Virtuoso.

If any streams are detected, the user can select one or more, and click the Add as IP input button at the bottom, and they will be added as IP inputs on the corresponding interface. These streams can then be monitored from the Inputs page, as described in Section 8.6.2.

8.5.1.3 IP Routes

The IP Routes page allows the user to configure the IP routing table for the device. The routes configured in this table will be used when routing outgoing IP traffic from the device.

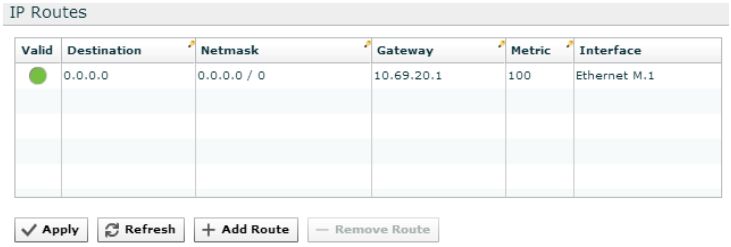


Figure 8.42 Routing page for Virtuoso.

8.5.1.3.1 Adding a new IP route

Note: To configure a *default gateway* for the device, see **Section 8.5.1.3.4**.

To add a new IP route, press the Add Route button shown in 8.42. A new line will appear in the table where the following parameters may be configured:

Destination
: The destination IP network/host address to use for matching against this routing rule.

Netmask
: The subnet mask to use for matching against this routing rule. You may configure either a x.x.x.x style network mask, or alternatively just specify the prefix length of the network mask (number of leading 1s). Specifying the mask 255.255.255.255/32 will give a host specific route that will only match the exact host IP address configured as Destination.

Gateway
: The IP of the IP router/gateway that should be used for forwarding IP packets matching this routing rule. The gateway address MUST be a locally reachable IP address, matching the IP subnet configured on one of the local interfaces on the device.

Metric
: The metric associated to the routing rule. If a destination address matches more than one routing rule that has the same Netmask length, the rule with the lowest metric will be used.

Two additional colums give additional status information about the routes:

Valid
: A GREEN virtual led indicates that this route is currently active. A RED virtual led indicates that this route is conflicting with other IP parameters configured on the device, and is not currently active.

Interface
: Indicates on which interface outgoing packets matching this routing rule will be output. The interface is found by matching the rule's Gateway address against the IP subnets configured on the local interfaces.

All newly added routes will appear in the table with a yellow background color which indicates that this is a new route that has not yet been applied to the running device configuration. Repeat the process above to add multiple routes at the same time.

8.5.1.3.2 Removing an existing IP route

To remove an existing route entry, select the entry in the table, and press the Remove Route button at the bottom of the page. The entry's background color will change to red, indicating that the entry has been scheduled for deletion.

8.5.1.3.3 Applying IP routing changes

To apply all changes in the routing table press the Apply button at the bottom of the page. This will commit the new routing table to the system and from this point the new configuration will be used for all outgoing IP traffic.

8.5.1.3.4 Configuring a default gateway for the device

The default IP gateway on a device is the router which is used if outgoing IP traffic is not destined to any of the networks configured on the local interfaces, or does not match any of the network specific IP routes configured in the device routing table.

There can only be ONE SINGLE default gateway configured in the device at any time - hence the name "default".

To add a default gateway routing entry to the routing table, press the Add Route button, and enter parameters like this:

```
Destination: 0.0.0.0
Netmask: 0.0.0.0/0
Gateway: <Default GW address>
Metric: 0
```

Note about the Metric parameter

Note that the only way a route will be deactivated is by disabling the destination interface of the route - a link down event will not alter the routing table.

This means that if multiple routes have the same Destination and Netmask, but different Gateway/Interface and Metric values, only the route with the lowest metric will be used as long as all interfaces are enabled.

Note about IP data output Manual destination interface option

If the Manual interface option has been selected on an IP data output channel, the data stream will be sent directly to the destination IP address as long as this is either an IP address matching the IP subnet configured on the interface, or is an IP multicast address.

If a unicast destination address is used which does not match the local IP subnet configured on the interface, the stream is directed to the gateway that has been configured as the Data gateway on the specific destination interface. See **Section 8.5.2.1** for more about configuration of Data gateway on an interface.

8.5.1.4 Network Services

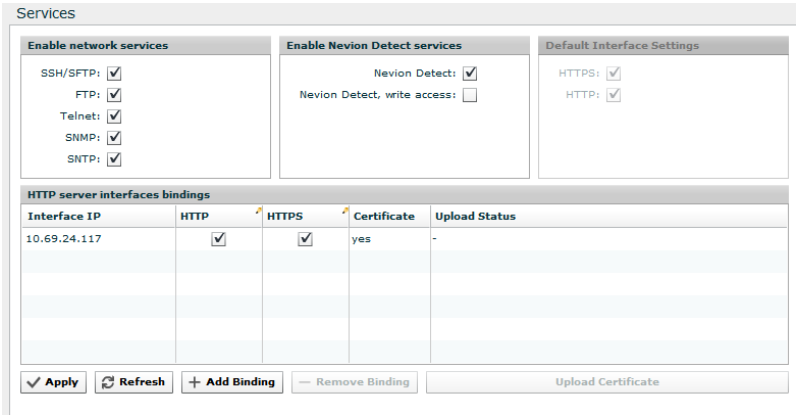


Figure 8.43 Network Services Page

The Network Services page enables a user to select network services the unit provides. The services can be accessed via all network interfaces with "Allow management traffic" turned on (see **Section 8.5.2.1**). The page is divided into four windows described here.

Enable network services

The window presents a group of services for accessing the unit console line, file system, status and configuration, and to enable network time synchronization.

The console line can be access via SSH or Telnet protocols on port number 22 and 23 respectively. Telnet and SSH is mainly for Nevion developer access and may be turned off. The unit file system can be access via FTP or SFTP on port number 21 and 22 respectively. FTP and SFP will normally never be needed and may be turned off. Only 'sftp' user can log in via SFTP and it is not possible to user SFTP with other users. If the 'sftp' user does not exist in the unit user database it can be created via the Users page cf. **Figure 8.36**.

The unit status and configuration can be accessed via SNMP or port 161. Simple network time protocol communicates via port 123.

Enable Nevion Detect services

The window provides control over the Nevion's proprietary Nevion Detect protocol that enables detection of Nevion devices in a local network. When the write access is enabled, a Nevion Detect client software can modify the unit network interface settings. Since the protocol does not implement any type of authorization, it is important to disable the write access in local networks where units can be exposed to malicious actions. The Nevion Dectect protocol uses UDP on port 3972. See also **Section 7.3.4**.

Default Interface Settings

When no interface binding is defined in the HTTP Service Interface Bindings section, this window contains the web server settings. The HTTP checkbox enables HTTP access on port 80 and the HTTPS checkbox enables secure HTTP access on port 443. The HTTPS server authenticates itself with a default SSL certificate where the common name (CN) field is set to 'localhost' and the organization (O) field is set to 'Nevion'. In order to use own SSL certificate, a user must define interface bindings in the window below.

HTTP Server Interface Bindings

The window contains information on which interfaces the web server should bind to and what protocols and certificates it should use. If no interface binding is specified, the web server binds to all interfaces and uses the settings from the Default Interface Settings window.

When adding the first binding, it is important to bind the web server to the interface that a client currently connects through. Otherwise, the connection will be lost, as the web server will be only bound to the just added interface.

By default, the web server provides the default SSL certificate on all interfaces. A user can upload own SSL certificate for each interface individually by click on the "Upload Certificate" button. This brings the file browser view where a user can select the certificate. The unit validates uploaded certificates and reports the result in the "Upload Status" column. The unit accepts only certificates with the following structure:

```
-----BEGIN RSA PRIVATE KEY-----
[webserver private key]
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
[webserver certificate]
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
[optional intermediate CA certificate]
-----END CERTIFICATE-----
```

The encrypted private key is not supported.

8.5.1.4.1 Security considerations

If the unit is located on an unknown and possible unsure network, you should disable as many networks services as possible and only use the secure versions of the protocols if applicable (SSH instead of Telnet, SFTP instead of FTP and HTTPS instead of HTTP). The only protocol needed for web GUI access is HTTPS, and should thus always be enabled. It is also possible to limit the management traffic to specific IP interfaces, using the "Allow management traffic" described in **Section 8.5.2.1**.

8.5.2 Ethernet port

8.5.2.1 IP Interface

This is the main page when selecting an Ethernet port from the navigation list. It contains IP configuration fields:

Enable
: This enables the Ethernet interface

IP address
: This field is used to set the IP address of the Ethernet interface. The second field is to set the

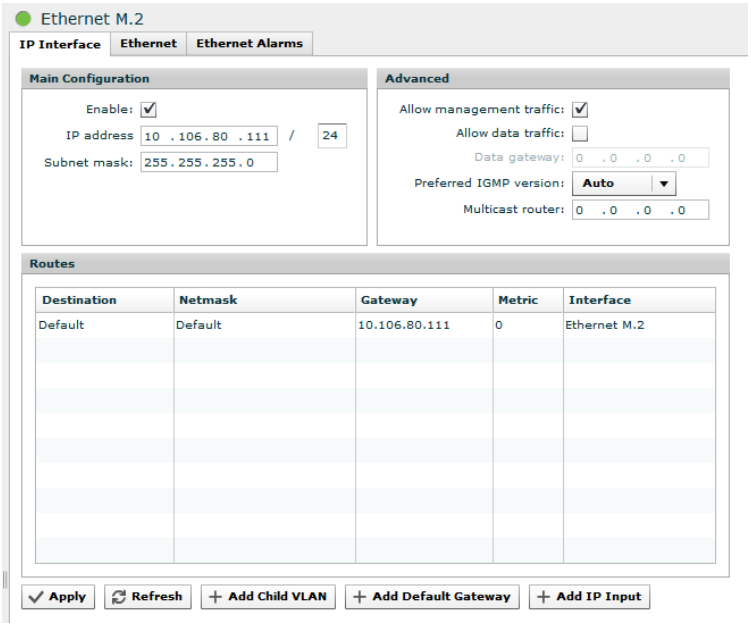


Figure 8.44 The main page for an Ethernet port on the Virtuoso.

subnet mask length. This can alternatively be set by inputting the subnet mask in the next field.

Subnet mask
: This field is used to specify the subnet mask for the Ethernet port.

Allow management traffic
: When enabled, a user can access device network services such as command line, file system, or web GUI via this interface. To improve security, disable management traffic on interfaces that are not used to access the device.

Allow data traffic
: When this parameter is set, IP data traffic is allowed to be transmitted and received on the interface. Disable Allow data traffic for interfaces that are used for dedicated management connections, to avoid accidentally transmitting high bitrate IP data streams on such networks.

Data gateway
: The data gateway field specifies what IP router/gateway that should be used for forwarding of outgoing IP *data* traffic that is forced to be output on this interface, and for which the destination is an IP subnet that does not match the subnet configured locally on the interface. This field is only configurable when Allow data traffic field is enabled.

Note: This field can NOT be used for specifying the *default gateway* for the device. The default gateway for the device must be configured in the device's routing table, see **8.5.1.3**.

Preferred IGMP version
: This configuration which is a dropbox under the "Advanced" field on the same page. Here the user can set the preferred IGMP version for the port. It can be set to Fixed v2, Fixed v3 or Auto.

Multicast router
: This field configures the IP address of an IP router/gateway that should be used for forwarding of IP multicast traffic that is to be transmitted on this interface. The address must be on the same IP subnet as that which is configured locally on the interface. To use the multicast router for forwarding of multicast traffic the Use multicast router parameter must be enabled on the Advanced tab of the IP output channel, see **Section 8.10.2.3.5**.

The RIPv2 related parameters are explained in detail in **Section 8.10.2.3.3.1**.

Under the routes field on the Ethernet port page, there is a list of added routes for the interface, if any are added. New routes can be added from the routing page described in **Section 8.5.1.3**, or by clicking the Add Default Gateway at the bottom of this page.

Adding a VLAN to an interface is done by clicking the Add Child VLAN button at the bottom. This brings up a dialog box where the user inputs the VLAN ID, and by applying, the VLAN is added to the currently selected interface. The VLAN is then reachable from the navigator on the side.

8.5.2.2 Ethernet

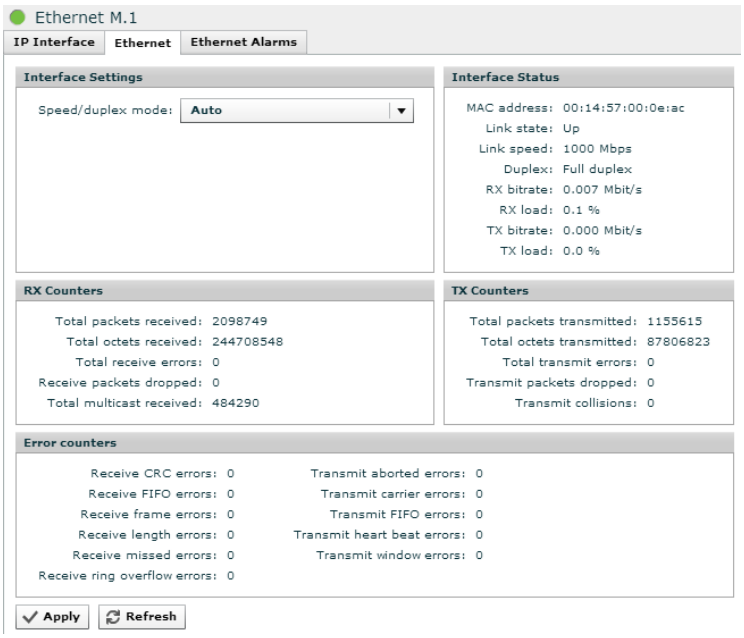


Figure 8.45 Sub-page for Ethernet port to set interface settings and view status on the Virtuoso.

Selecting the Ethernet subpage on the Ethernet port page by clicking the tab brings the user to the page shown in figure **8.45**.

Here the user can set the speed/duplex mode (currently only supporting Auto).

Additionally, there are four fields with status parameters for the interface: interface status, RX counters, TX counters, error counters.

These four fields give status information under these four umbrella categories. The interface status field gives:

MAC Address
: MAC address of the interface.

Link State
: Indicates whether the Ethernet link is up or down.

Link speed
: The detected link speed of the interface.

Duplex mode
: The detected current duplex mode of the interface. The duplex mode indicates whether data may flow in one direction (half duplex) or bidirectionally (full duplex).

RX bitrate
: The total bitrate received.

RX load
: Interface receive load, measured relative to max speed.

TX bitrate
: The total bitrate transmitted.

TX load
: Interface transmission load, measured relative to max speed.

The RX and TX counters gives information about:

Total packets received/transmitted
: The total number of IP packets received/transmitted.

Total octets received/transmitted
: The number of octets received/transmitted

Total receive/transmit errors
: The number of erroneous receive/transmit errors.

Receive/transmit packets dropped
: The amount of receive/transmit packets that have been dropped.

Total multicast received / Transmit collisions
: Gives information about the total multicast packets received for the RX part, and the number of packet collisions for the TX part.

Finally there is a field with a number of error counters:

Receive CRC errors
: Indicates the number of packets received with a CRC (FCS) error by this network device.

Receive FIFO errors
: Indicates the number of receive FIFO errors seen by this network device.

Receive frame errors
: Indicates the number of received frames with error, such as alignment errors.

Receive length errors
: Indicates the number of received error packet with a length error, oversized or undersized.

Receive missed errors
: Indicates the number of received packets that have been missed due to lack of capacity in the receive side.

Receive ring overflow errors
: Indicates the number of packets received discarded due to a ring buffer overflow.

Transmit aborted errors
: Indicates the number of packets that have been aborted during transmission by a network device (e.g: because of a medium collision).

Transmit carrier errors
: Indicates the number of packets that could not be transmitted because of carrier errors (e.g: physical link down).

Transmit FIFO errors
: Indicates the number of packets having caused a transmit FIFO error.

Transmit heart beat errors
: Indicates the number of packets transmitted that have been reported as heartbeat errors.

Transmit window errors
: Indicates the number of packets not successfully transmitted due to a window collision.

8.5.2.3 Ethernet alarms

The Ethernet alarms tab brings the user to the configuration page for the defined alarms belonging to an Ethernet input. Here the user can change the defined alarm severities and other configurations, in the same way as described in **Section 8.4.2.1**.

The page has another subpage reached by clicking the Alarm Log tab. This page shows all the entries in the alarm log which belongs to the selected Ethernet port. The same buttons exists here as for the alarm log described in **Section 8.3.6**, so the user can clear, export or generate SLA on this alarm log.

8.5.2.4 VLAN

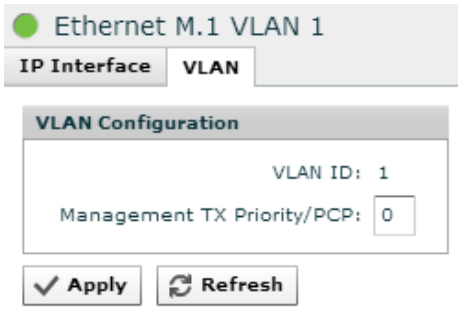


Figure 8.46 The VLAN subpage for a VLAN under a particular Ethernet interface for the Virtuoso.

See section 8.5.2.1 for info about how to add a VLAN interface.

If a VLAN is added to an Ethernet interface, it is reachable from the sidebar navigation. The IP configuration main page for a VLAN looks the same as for an Ethernet interface, as shown in figure 8.44.

In addition for a VLAN interface, there is also a sub-page called VLAN, which is shown in figure 8.46. In this sub-page, the VLAN ID is shown, and the user can input a priority level to be used for outgoing management traffic.

Note: VLAN interfaces are not available in the software recovery mode of the unit ("boot monitor", "mon>" prompt). Due to this limitation, it is recommended to use at least one non-VLAN interface (untagged) for management of the unit.

8.6 Inputs

The Inputs page contains all information and settings that apply to the input ports of the device. The navigation list to the left lets the user select which input to view, or select Inputs Overview to view a summary of all the inputs to the device.

The labeling of the inputs is a combination of the user defined name of the input and the physical number of the input port.

8.6.1 Inputs Overview

The Inputs Overview page shows a graphical view of all the current inputs on the unit, as shown in figure 8.47.

Each input has a symbol referring to illustrate whether it's an IP , SDI or ASI, and each symbol is colored by its current alarm severity level. The input type is also written in the symbol box, along with its port numbering (as described in **Section 6.1**) and the label or a generated service description if no label is set.

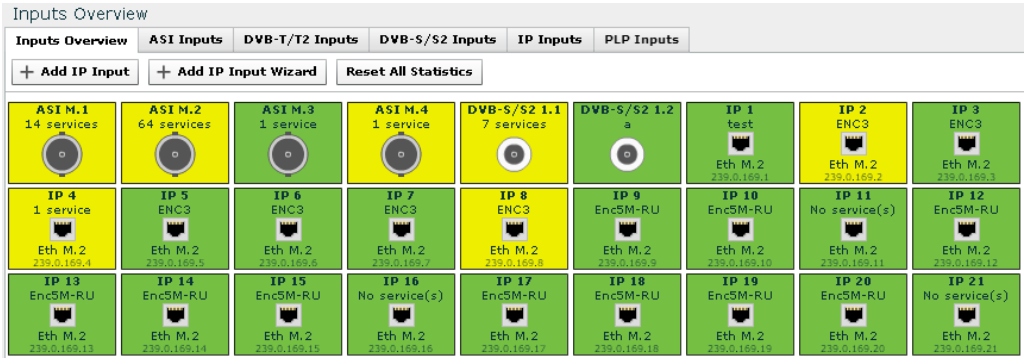


Figure 8.47 Inputs Overview

Mouseover on any input icon will give some configuration status, transport stream details and port specific details.

There are two buttons on the inputs overview page:

Add IP input
: This button adds a new IP input with an empty configuration and disabled.

Add IP Input Wizard
: This button opens up a dialog starting a wizard to help add and configure one or several IP inputs. This wizard is described in **Section 8.6.1.1**.

8.6.1.1 IP input wizard

Pressing the Add IP Input Wizard button on the inputs overview page brings up dialog box containing the IP Input Wizard. This wizard lets the user define the first IP input, and set a rule to create a number of inputs based on the first input, by setting stepping values and the number of inputs as described below.

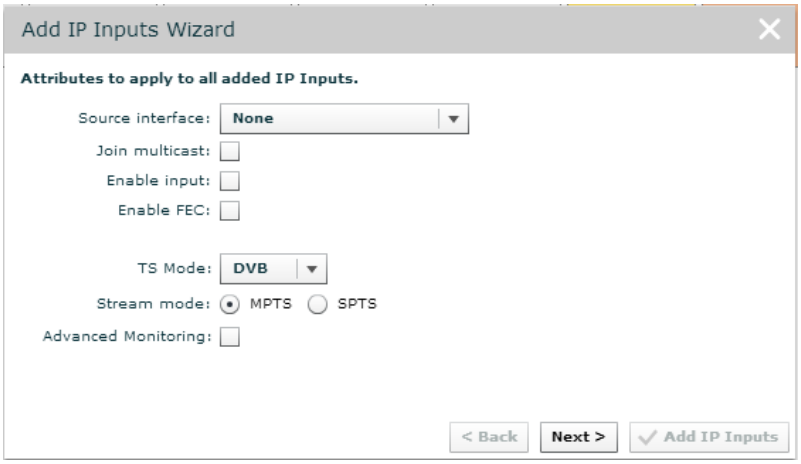


Figure 8.48 IP Input Wizard - First dialog window.

The first screen of the wizard is showed in figure 8.48 and it contains the following fields:

Source interface
: A drop down box where the user can select which Ethernet interface to add the IP inputs on.

Join multicast
: Tick box where the user can define whether or not to use a multicast source address to add the inputs.

Enable input
: Tick box to instruct the unit to enable the inputs as soon as the wizard is finished.

Enable FEC
: Tick box to instruct the unit to enable the Forward Error Correction on the created inputs.

TS Mode
: Select which monitoring mode is used on the created inputs (MPEG, DVB or ATSC).

Stream Mode
: Select which stream mode is used on the created inputs (MPTS or SPTS).

Advanced Monitoring
: Tick box to instruct the unit to enable the advanced monitoring features on the created inputs.

Figure 8.49 IP Input Wizard - Second dialog window with multicast.

The second screen is shown in figure 8.49 or 8.50, depending on the Use multicast tickbox in the first window of the IP Input Wizard. When using multicast, the following fields are configurable:

Multicast address
: This is an IP field where the user can input the address of the multicast to join.

Multicast source address
: Multicast source address if used.

UDP port
: Input field where the user types in the UDP port for the first IP input in the

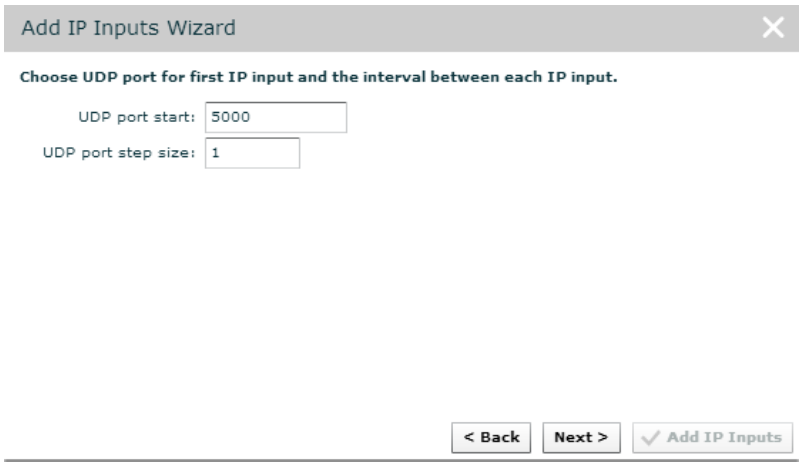


Figure 8.50 IP Input Wizard - Second dialog window without multicast.

Multicast stepping
: If the user wants to use multicast address stepping, this is the field to input the stepping rule. For example 0.0.0.1 means the fourth byte will increment by 1 for each input.

Multicast source stepping
: If the user wants to use multicast source address stepping, this is the field to select this and input the stepping rule for the source address.

UDP port stepping
: If the user wants to use UDP port stepping between the added inputs, this is where the incremental value between the UDP ports will be used. For example, setting this to 10 will increment the UDP port by 10 for each input added.

When not using multicast, the following fields are available for the user:

UDP port start
: Entering the starting port number for the UDP stream.

UDP port step size
: Step size between the inputs the user wants to add. This is the incrementation stepping value from the UDP start port value when adding several inputs.

The third and final screen shown in figure **8.51**. It only contains one field for configuration, and one field to read out the result:

Number of ports
: Here the user inputs the number of IP inputs to add based on the base IP input and the stepping rules set on the previous screen.

Result
: This text box shows the properties of the resulting IP inputs which will be created by pressing the Add IP Inputs button.

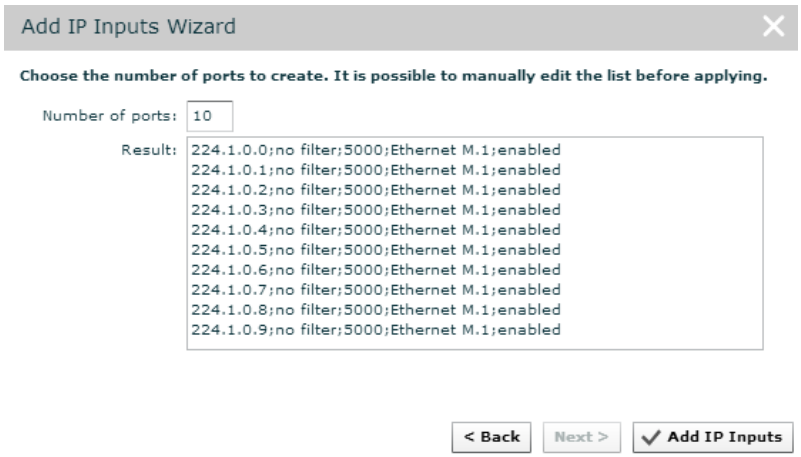


Figure 8.51 IP Input wizard - Third and last dialog window.

Note: It is possible to modify the content of the text box as long as the format is semi-colon separated and follows the pattern indicated below the text box. Pro tip: Use a spreadsheet application which handles CSV formats.

Pressing the Create IP Inputs button will now the number of IP inputs which the user typed into the Number of ports field.

8.6.1.2 ASI Inputs

This page shows the list of ASI Inputs on the Virtuoso. This is shown in figure 8.52. The page allows the user to look at basic status and configurations of the ASI inputs, or make configurations to the current inputs. Columns in the grid are:

Enable
: This shows whether the ASI input is enabled or not. An input is enabled or disabled by clicking the check box and hitting Apply.

Input
: The name of the ASI input, consisting of the factory defined label with the physical port number and the user defined name. If no user defined label is defined, a generated name based on the TS is shown.

TS Mode
: Set the format of the TS being received, either as DVB, ATSC or MPEG.

Sync
: Status showing whether the input currently has a transport stream sync.

TS id
: Status field showing the transport stream ID.

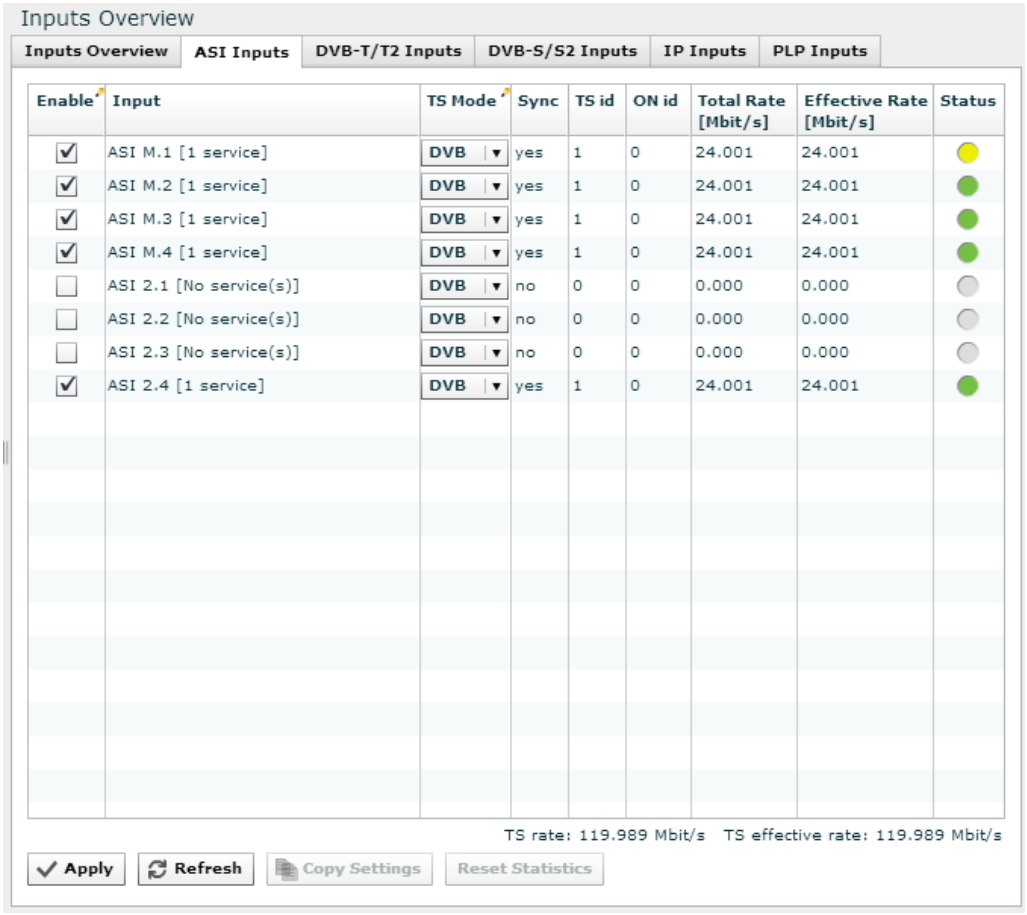


Figure 8.52 Inputs Overview - ASI Inputs

ON id
: Shows the original network id for the transport stream.

Total rate [Mbit/s]
: The total bitrate of the transport stream currently received on the input in Mbit/s.

Effective rate [Mbit/s]
: The effective bitrate (excluding null packets) of the transport stream currently received on the input in Mbit/s.

Status
: Shows alarm status on the switch input. This is not the same as the status on the currently selected physical port.

Below the table two values are shown:

TS rate
: The sum of bitrate of all the transport stream received over ASI.

TS effective bitrate
: The sum of the effective bitrate of all the transport stream received over ASI.

The Copy Settings button at the bottom works in the same way as it does for IP inputs, as described in **Section 8.6.1.3**.

8.6.1.3 IP Inputs

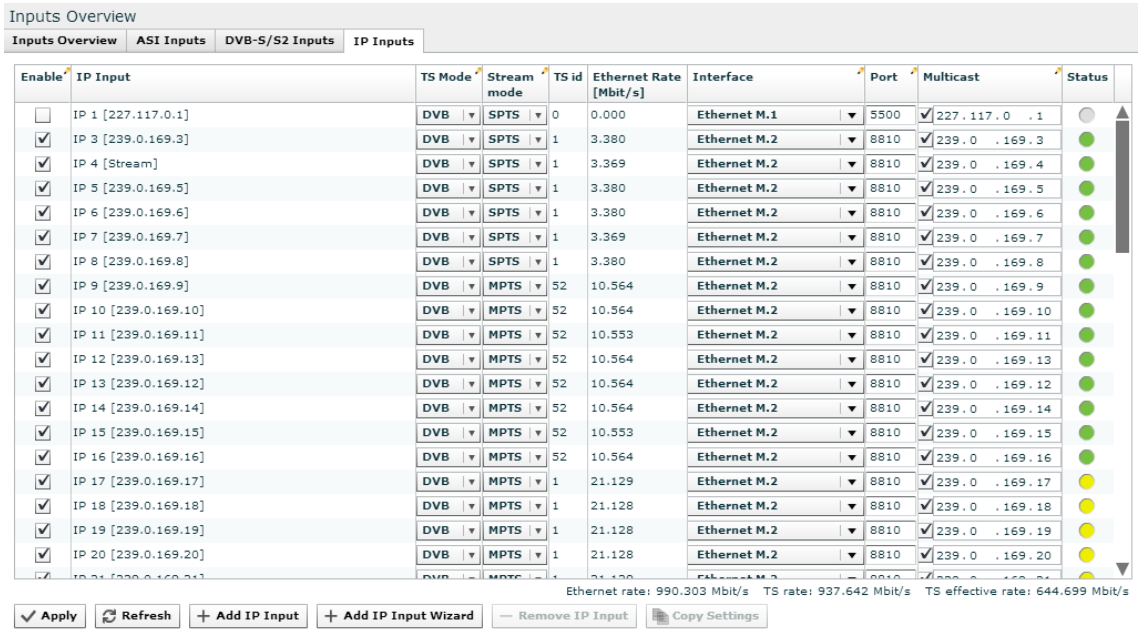


Figure 8.53 Inputs Overview - IP Inputs

The page lists IP input streams defined and offers an interface to add or remove input streams. The table has the following columns:

Enable
: This shows whether the IP input is enabled or not. An input is enabled or disabled by clicking the check box and hitting Apply.

IP Input
: The name of the IP input, consisting of the factory defined label. The name also consists of either the multicast address or a generated service info description based on the TS. Which of the two, depends on the settings described in **Section 8.4.11**.

TS Mode
: The format of the TS being received, either as DVB, ATSC or MPEG.

TS id
: Status field showing the transport stream ID.

Ethernet Rate [Mbit/s]
: The currently received bitrate in Mbit/s, measured at the Ethernet level.

Interface
: The interface that this IP input is configured to receive data through.

Status
: The current alarm status of the input is shown as a colored indicator; the colour indicating the highest severity level of the active alarms. If the port is disabled the indicator is grey.

Below the table three values are shown:

Ethernet rate
: The sum of the Ethernet bitrate received over all the IP inputs.

TS rate
: The sum of the bitrate of all the transport stream received over IP.

TS effective bitrate
: The sum of the effective bitrate of all the transport stream received over IP.

The Add IP Input and Remove IP Input buttons at the bottom of the page lets the user add or remove IP inputs.

After clicking the Add IP button the Apply button must be clicked before the channel parameters can be edited. A new channel is shown with a plus sign in the navigator until it has been edited (and the edit applied).

The page also includes the Add IP Input Wizard button, which starts the same wizard as described in **Section 8.6.1.1**.

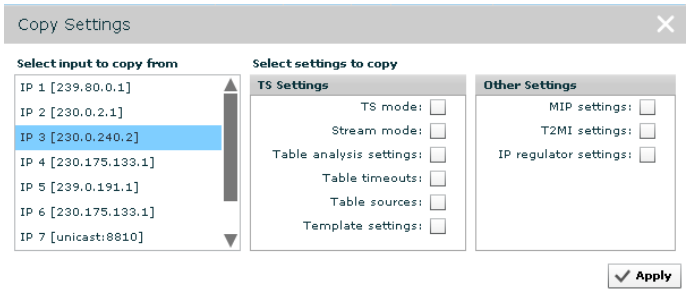


Figure 8.54 Inputs Overview - Copy settings dialog.

The Copy Settings button allows the user to select a number of inputs to share a particular setting between them. By selecting any number of inputs and pressing the Copy settings button, the user is presented with the dialog box shown in figure **8.54**. Here, the user can select which of the selected inputs to copy settings from on the left side. On the right side is a list of settings the user can copy onto the other inputs which will be done on pressing apply.

Note: To change a setting available on the inputs list on many inputs at once, the user can hold the ctrl or shift key to select multiple rows, and perform an action on one of the inputs, and the change will follow the rest of the selected inputs. The same goes for removing IP inputs, multiple inputs can be selected before pressing the Remove IP Input button and then Apply.

8.6.1.4 SDI Inputs

Figure 8.55 SDI Overview

This page shows the Main page of an SDI Input on the Virtuoso. This is shown in figure 8.55. The page allows the user to look at basic status and configurations of the SDI input.

8.6.1.4.1 SDI Configuration

Enable
: This shows whether the SDI input is enabled or not. An input is enabled or disabled by clicking the check box and hitting Apply.

Label
: This is the user defined name of the SDI input, which can be changed by typing a new label and hitting Apply. It is only used in the WEB GUI to identify the input.

8.6.1.4.2 SDI Status Section

Shows basic information of the SDI input like video format, sync status and PPM offset.

8.6.1.4.3 Audio Channel Info

Shows which audio channels are present on the SDI Input

8.6.1.4.4 Thumbnail

Check the enable box to create downscaled images of the video input on the SDI Port. The image will be automatically updated with regular intervals.

8.6.1.4.5 MADI Input

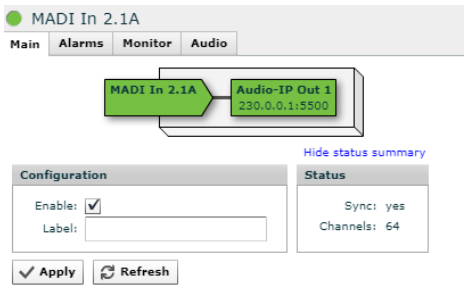


Figure 8.56 MADI Input

Figure 8.56 shows status and configuration for the MADI input.

8.6.2 TS (Transport Stream) Inputs

When a specific input is selected, a page with information about that input is displayed. The header of the page shows the name and the current alarm status of the input and a list of tabs that is dependent on what sort of input is selected (ASI, IP,...) and what options are selected.

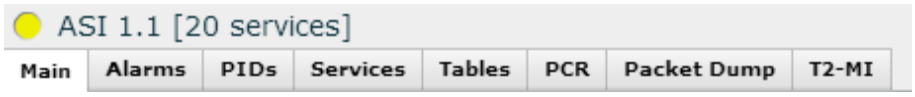


Figure 8.57 Input header

Holding the mouse cursor over the alarm status indicator brings up a tool tip displaying up to 30 of the current alarms (if any) on this particular input.

Beneath the name of the input is a tab navigator containing different sub pages with information about the selected input. The choices are:

Main
: This page shows a summary of the transport stream currently received on the input, including a summary of the running PIDs and services.

Alarms
: This page lets the user view the status of all alarms on the input, and override the severity of these alarms.

IP
: This tab is present only if the input selected in the navigator is an IP input. It gives access to the IP specific features of the input.

PIDs
: This page gives detailed information about the currently present PIDs.

Services
: This page gives detailed information about the services that are currently running and the components of those services.

Tables
: This page shows which tables are present on the input and allows selecting tables that should be analysed by the unit.

PCR
: This page shows the PCR PIDs present on the transport stream and information about them. In addition you can analyse PCR jitter on any of the PCR PIDs.

Packet Dump
: This page offers dumping of a sequence of TS packets with a selected PID.

In all sub-pages, for a selected input, the list of the current alarms for that input is shown at the bottom of the page. The list is identical to the list displayed in the Current Status view, described in **Section 8.3.1**.

8.6.2.1 Main

The content of the Main tab depend on what sort of input is selected (ASI, IP,...).

8.6.2.1.1 Main (ASI input)

The Main page is divided into a various number of sections depending on the type of the input.

Exampled here is an ASI input with its main tab. The main tab for ASI and IP inputs will look different in terms of the fields describing configurations and status for the various inputs.

The main tab for IP inputs specifically is described in **Section 8.6.2.1.2** .

Looking at the input exampled in figure **8.58** the first field is the ASI Configuration. This contains the configuration parameters which are common for all input types (while IP and RF inputs might have some extra as well):

Enable
: This shows whether the input is currently enabled. The input is enabled or disabled by clicking the check box and then Apply.

Label
: This is the user defined name of the input port, which can be changed by typing a new label and hitting Apply. It is only used in the WEB GUI to identify the port.

Advanced monitoring
: Turns on advanced monitoring of the input, if available. If available and applied, this brings up the Templates, PCR and Packet Dump tabs on the input header shown in figure **8.57**.

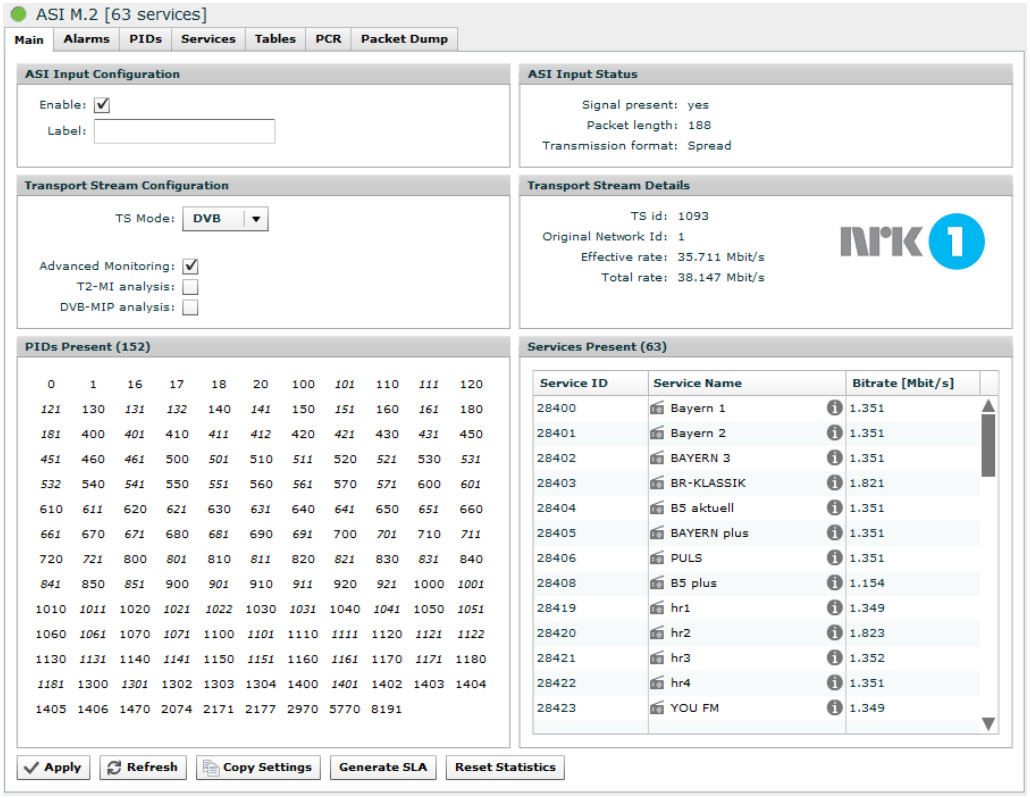


Figure 8.58 Main tab.

For ASI inputs, the ASI InputStatus field also gives some basic status for the input. Theses status parameters are:

- Signal present - yes or no.
- Packet length - 188 or 204 bytes.
- Transmission format - burst or spread mode.

The Transport Stream Details field contains information and some configuration parameters concerning the transport stream:

TS id
: The transport id of the transport stream currently received on the input. The value of this depends on PAT being present and decoded on the input.

Original Network Id
: The Original network id of the transport stream currently received on the input. The value of this parameter depends on the SDT actual being present and decoded on the input.

Effective rate
: The effective bitrate (excluding null packets) of the transport stream currently received on the input in Mbit/s.

Total rate
: The total bitrate of the transport stream currently received on the input in Mbit/s.

The Transport Stream Details section shows all the PIDs that are present on the selected input. The number in parentheses is the total number of PIDs present. A PCR PID is represented by a number shown in italics. A colored PID number provides additional PID status information:

Red
: A continuity counter (CC) error alarm is raised.

Blue
: Stream is scrambled. The shade of blue represents whether the scrambling mode is odd or even.

Hovering the mouse pointer over a PID provides detailed information about that PID.

On the right hand side of the page is the Services Present section. This shows a list of all the services that are currently present on the selected input. The list depends on PAT and PMT being present and successfully decoded on the input. The service name depends on SDT actual being present and decoded. The number in parentheses is the total number of services present.

The list has three columns:

Service ID
: The program number/service id of the service.

Service Name
: The name of the service as conveyed by the SDT Actual table. If there is no SDT Actual table or if the SDT table is not analysed, the name is displayed as Service <SID>.

  The icon prefixing the service name indicates the alarm status of the service and, if the SDT table is analysed, the type of service. A list of active alarms (if any) on the service is displayed by holding the mouse pointer over this icon.

  Detailed information about the service is displayed by holding the mouse pointer over the "I" icon to the right.

Bitrate [Mbit/s]
: The current bitrate of the service, i.e. the aggregate bitrate of all the service components.

Double clicking on a service will navigate to the Services page, with the folder for the service at hand being expanded.

The Generate SLA button at the bottom of the page will generate an SLA report for the current input, as described more in **Section 8.6.2.2.2**.

The Reset Stats button at the bottom of each input page gives access to a dialogue box that allows reset of channel statistics (shown **Figure 8.59**). Select the statistics items you want to reset and then press Apply.

Figure 8.59 Reset statistics dialog box

8.6.2.1.2 TS-IP In - Main

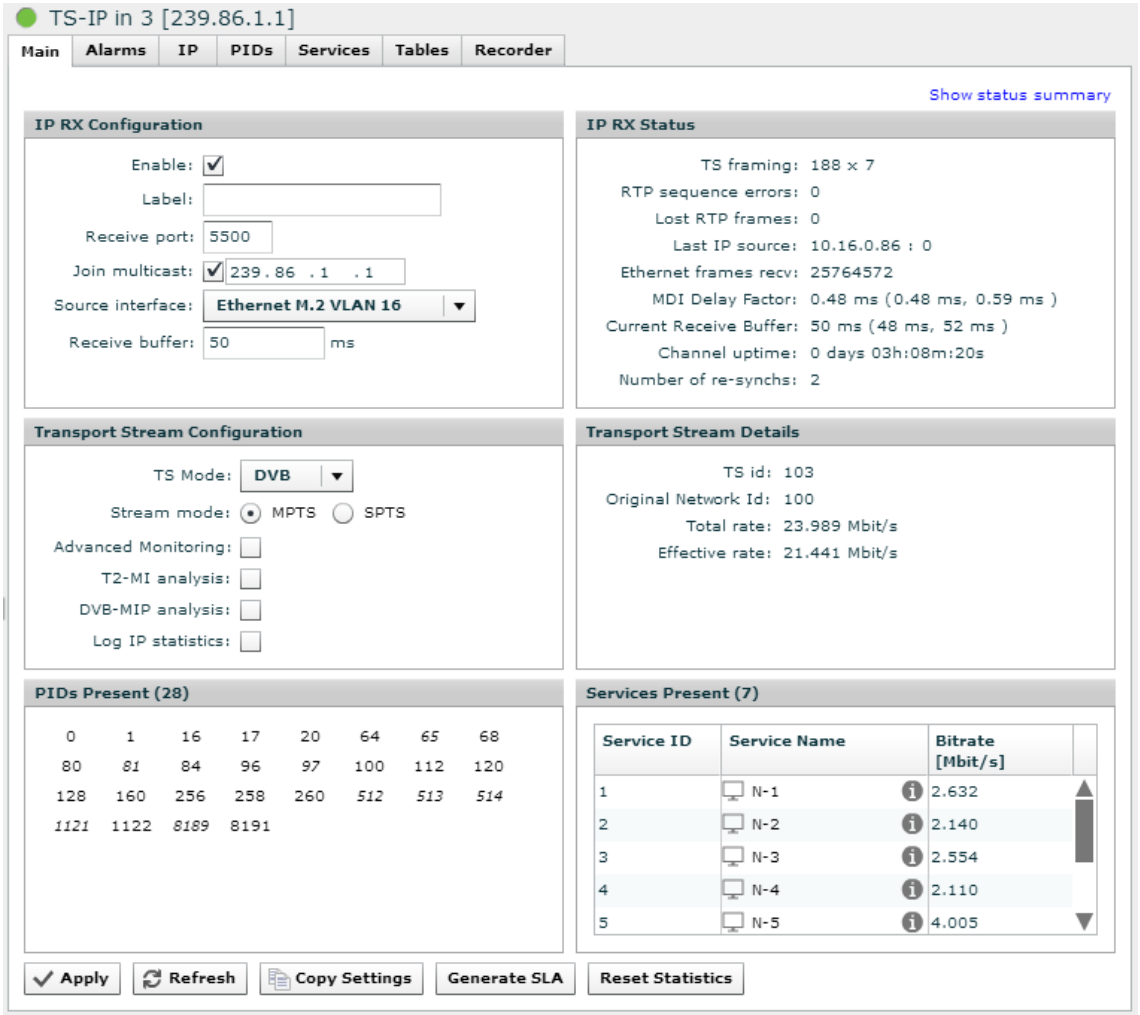


Figure 8.60 Main page for a TS-IP input channel.

The IP inputs main page is shown in figure 8.60. The Transport Stream Configuration, Transport Stream Details, PIDs Present and Services Present sections are common with ASI inputs and are therefore described in **Section 8.6.2.1.1**.

The IP RX Configuration section contains settings related to the IP layer:

Enable
: This shows whether the input is currently enabled. The input is enabled or disabled by clicking the check box and then Apply.

Label
: A user configurable label

Receive port
: UDP port to listen to. This is used for both unicast and multicast reception.

Join multicast
: This option contains a checkbox to whether or not the user wants to join a multicast stream. If this is checked, there is an IP field to input the multicast group address. If the box is not checked, the input is configured for unicast reception. This field might have an icon next to it if additional configuration options are used. See **Section 8.6.2.3**.

Source interface
: A dropdown menu which allows the user to specify which Ethernet interface the incoming IP stream is being received on.

The IP RX Status section presents some information about the IP data received:

TS framing
: The number of bytes per TS packet on the incoming transport stream (either 188 or 204 bytes) followed by the number of TS packets being received per IP frame.

RTP sequence errors
: A counter showing the number of RTP sequence errors caused by lost packets or packets received out of order. A value of zero indicates that all packets are received in correct sequence.

Lost RTP frames
: A counter showing the number of RTP frames that have been lost, i.e. lost and not corrected by the unit.

Last IP source
: The IP address of the transmitter.

Ethernet frames recv
: The number of Ethernet frames received.

MDI Delay Factor
: MDI delay factor. The minimum and maximum values are shown in the parenthesis.

Current Receive buffer
: Current size of receiver buffer. The unit will always try to keep the buffer at the configure

Receive buffer value, but might sometimes be off target due to jittering signals or if the initial buffer playout rate was too far from the actual bitrate. Minimum and maximum values are also shown in the parenthesis.

Channel uptime
: Tie elapsed since the establishment of the channel.

Number of re-synchs
: Number of time the channel has re-synchronized since its establishment.

The remaining of the page is similar to the Main page of an ASI input.

8.6.2.2 Alarms

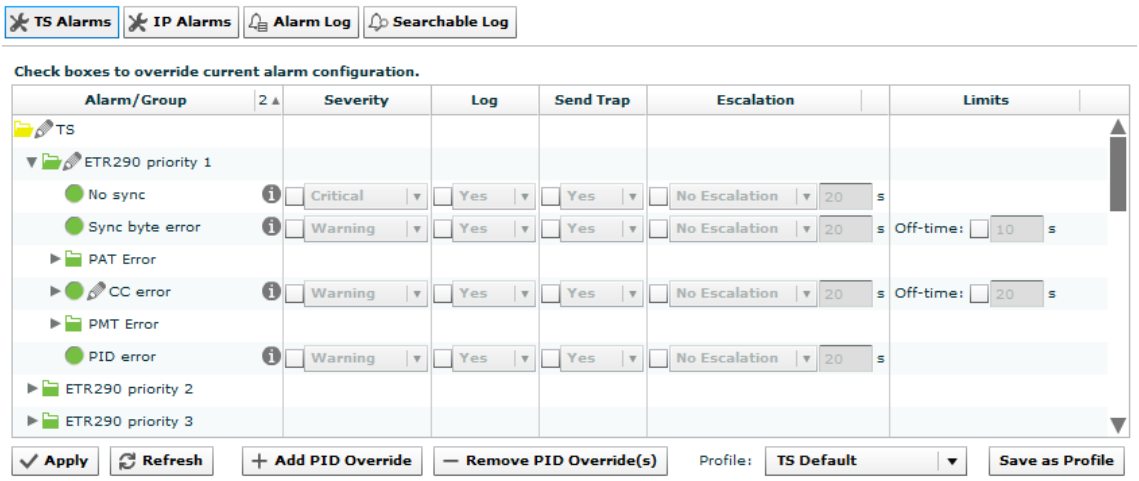


Figure 8.61 Input alarm configuration (for an IP input)

The Alarms page lets the user configure and view the status of all alarms belonging to the selected input. The page has three or more tabs at the top, depending on the type of input. For ASI inputs, there are three tabs, TS Alarms, Alarm Log, and Searchable log, which are present for all inputs. Inputs with extra alarms, such as IP or RF inputs will have an extra tab for configuring the alarm tree for that particular type.

8.6.2.2.1 TS alarms

In figure 8.61 the TS Alarms page is shown. Alarms are organized hierarchically and expandable branches are indicated by a clickable arrow to the left of the branch name.

The alarm list is presented in a table with different columns, where the left most column shows the Alarm/Group which is where to navigate the alarm tree.

A section of the expanded input alarm tree is shown in figure 8.62.

The alarm tree has two types of nodes:

Folder
: Corresponds to a group of alarms. The colour of the folder shows the highest severity of all

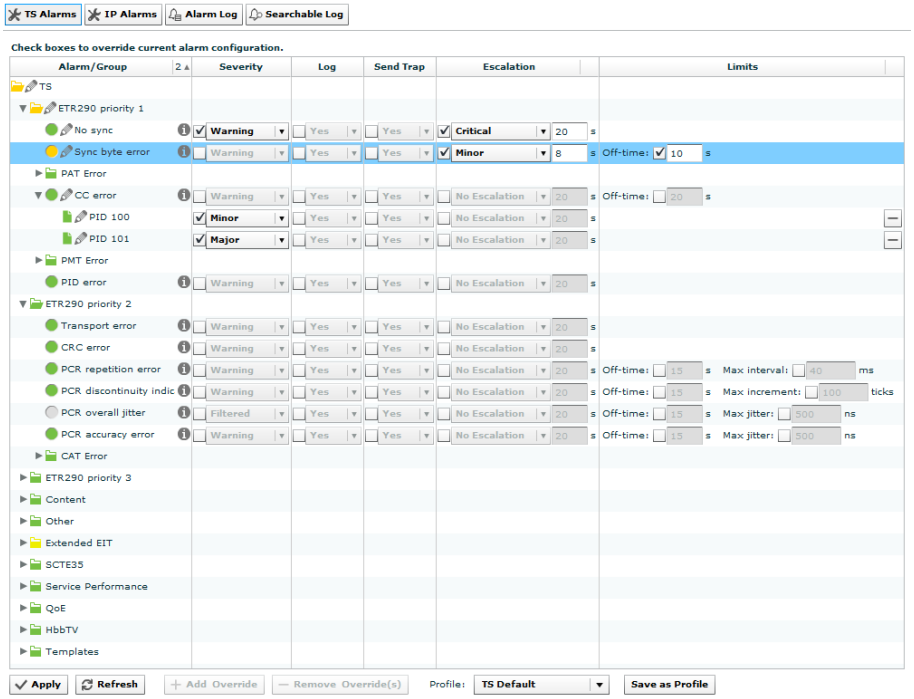


Figure 8.62 Input alarm tree

the alarms belonging to the group. The group is expanded or collapsed by clicking on the arrow next to the group.

Alarm node
: Shows the title description of the alarm itself. These have a coloured indicator showing the alarms current status. On the right side of each alarm node, there is an information icon.

By doing a mouse-over on the information icon for any alarm node, an alarm details box shows up which gives some extra details for the alarm. The alarm details section includes the following information and buttons.

Alarm ID
: The internal ID of the selected alarm. A complete list of alarms is found in Table D.3.

Alarm
: Name of the alarm.

Description
: A short description of the alarm.

The other columns on the Alarms page, which are configurable are as follows:

Severity
: Overrides the default severity for the given alarm. The default severity is in brackets to the right of the drop down list. De-ticking the checkbox sets the alarm back to its default severity.

Log
: If this is de-selected, any alarm entries of this type will not be added to the alarm log. This is selected for all alarms by default, so all entries are logged.

Send trap
: If this is de-selected, any alarm entries of this type will not sent as an SNMP trap. This is selected for all alarms by default, so all entries are sent as traps.

Escalation
: Most alarms support configuration of a two stage severity level triggering, when supported 3 fields are shown in this column, a checkbox to enable/disable the function, a dropdown for severity and a time field.

  When escalation is enabled, the alarm has a primary severity level configured in the Severity column, and a secondary severity level configured in the Escalation column. Also a number of seconds for the secondary level to activate is configured in this column.

  When the alarm activates, the primary severity level is used for the configured number of seconds and if the alarm stays active longer than that, the severity level is automatically changed to the escalated level.

  Remark that either or both the primary and secondary levels are allowed to be set to filtered, and the secondary level can be set lower than the primary level.

  Remark also that if the alarm supports an off-time, the escalation time should be set higher than the off-time to avoid escalation always to happen, since the off-time is the minimum time the alarm would stay on.

  When an alarm is escalated, the alarm details is prepended with a tag informing that the alarm has been escalated and with a reference to the sequence number and the on-time of the original alarm.

Limits
: This column consists of zero to three fields, depending on the alarm definition. These limits can be threshold values for a certain parameter, where an alarm will be triggered if these limits are breached. The default value is shown in the greyed out text box next to a tick box. To go back to default value after having configured a different value, simply untick the box.

The Off time is a configurable field for a high number of alarms. Its function is different from the other limit alarms:

Off time
: This field is shown for alarms that are automatically turned off after some time when no new errors are encountered. The time to wait from detecting the last error until the alarm is cleared is determined by the value in the box. This may be changed as required. The default value is shown to the right.

Note: Configuring a short Off time means that the alarm can be turned on and off at a fast rate, adding an entry in the alarm log every time. This could result in unintentional filling of the alarm log for certain error conditions. On the other hand, configuring a shorter Off time means that the alarm will stay on for a shorter time in the event of a short duration alarm condition.

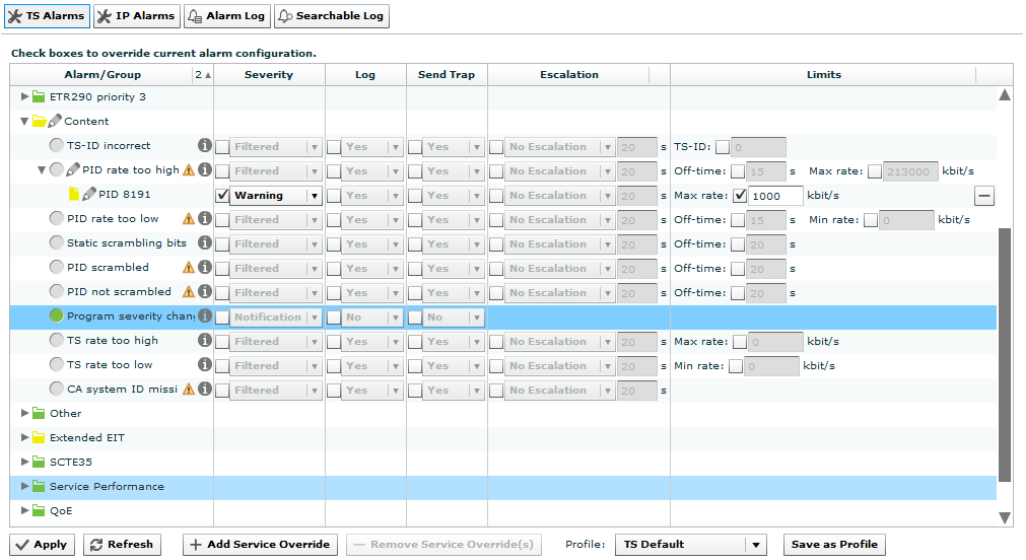


Figure 8.63 Alarm severity per sub-ID (typically Service or PID)

For certain alarms related to PIDs, the button at the bottom of the screen called Add PID Override will become active. Pressing this button brings up a dialog box where the user can enter a PID. When pressing Apply, a new line is added below the alarm the PID override is added to. This is shown in **Figure 8.63**. This allows the user to configure alarms differently based on the PID value.

8.6.2.2.2 Alarm Log

In the alarm log tab, the user can view the alarms belonging to the particular input. The alarm log tab is as described in **Section 8.3.6**, with the only difference being that all entries not belonging to that particular input are filtered out.

8.6.2.3 IP

This tab is only visible if an IP input is selected. There are multiple sub-pages, where some depend on licences.

8.6.2.3.1 Main

This page allows configuration of the IP parameters for the IP input and shows detailed IP status information for the input.

The IP RX Parameters section contains the following fields:

Auto configure
: Clicking on the button displays a list of all the incoming streams on all the interfaces (not being already used as input). Selecting a stream from the list automatically configure the subsequent fields.

Receive port
: The UDP port on which this input will listen for data.

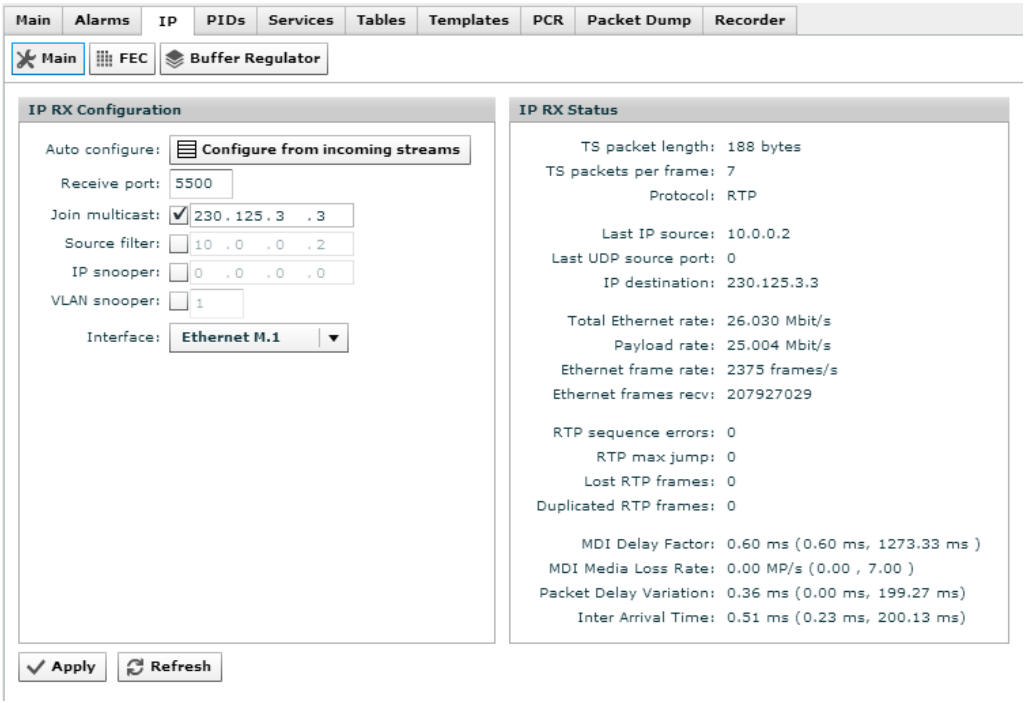


Figure 8.64 IP Configuration

Join multicast
: Option to select whether the user wants to join a multicast stream. If this is checked, there is an IP field to input the multicast group address. If the box is not checked, the input is configured for unicast reception.

Source filter
: Option to enable source filtering on IP receive. This might be used for both multicast and unicast reception. Note that this is not needed for most scenarios.

IP snooper
: This parameter enables snooping on IP streams not designated for this units. The IP field controls the IP address used when IP snooping is enabled. The IP address can be both unicast and multicast addresses. If a multicast address is given, IGMP messages will not be sent. This option takes precedence over Join Multicast. Note that the IP switch need to forward the streams to the given Ethernet interface for this functionality to work.

VLAN snooper
: This parameter enables snooping on IP streams on a given VLAN on the specified interface without having the VLAN as a separate interface.

Interface
: The interface on which this input will listen for data.

The IP RX Status section displays the following information:

TS packet length
: The number of bytes per TS packet on the incoming transport stream. This is either 188 or 204 bytes.

TS packets per frame
: The number of TS packets being received per IP frame. Ranges from 1-7.

Last IP source
: The source IP address of the last IP stream received by this input. If the input has never received an IP stream this value is set to 0.0.0.0.

Last UDP source port
: Source port for the UDP source.

IP Destination
: Last destination IP.

Total Ethernet rate
: The total Ethernet rate received on this input. Bitrate including Ethernet header.

Payload rate
: Bitrate for the payload. Excluding all IP and Ethernet headers.

Ethernet frame rate
: Ethernet frames per second for this stream.

Ethernet frames recv
: The number of Ethernet frames received.

RTP sequence errors
: A counter showing the number of RTP sequence errors caused by lost packets or packets received out of order. A value of zero indicates that all packets are received in correct sequence.

RTP max jump
: The max jump in RTP sequence number between two consecutive packets received.

Lost RTP frames
: A counter showing the number of RTP frames that have been lost, i.e. lost and not corrected by the unit (-1 if not supported).

Duplicated RTP frames
: A counter showing the number of duplicated RTP frames (-1 if not supported).

MDI Delay Factor
: MDI delay factor according to [14]. The minimum and maximum values are shown in the parenthesis.

MDI Media Loss Rate
: MDI media loss rate according to [14]. Minimum and maximum values are also shown in the parenthesis.

Packet Delay Variation
: Packet delay variation according to [15]. Minimum and maximum values are also shown in the parenthesis.

Inter Arrival Time
: Measured time between two consecutive RTP packets. Minimum and maximum values are also shown in the parenthesis.

8.6.2.3.2 Seamless IP Protection Switching

Please see Section 5.3 for a detailed technical description of the SIPS functionality.

SIPS Configuration

The SIPS sub-page is shown in figure 8.65. This page allows for configuration of common parameters relating to SIPS. A summary of the IP status information for flow A and B, and the SIPS module status is also available.

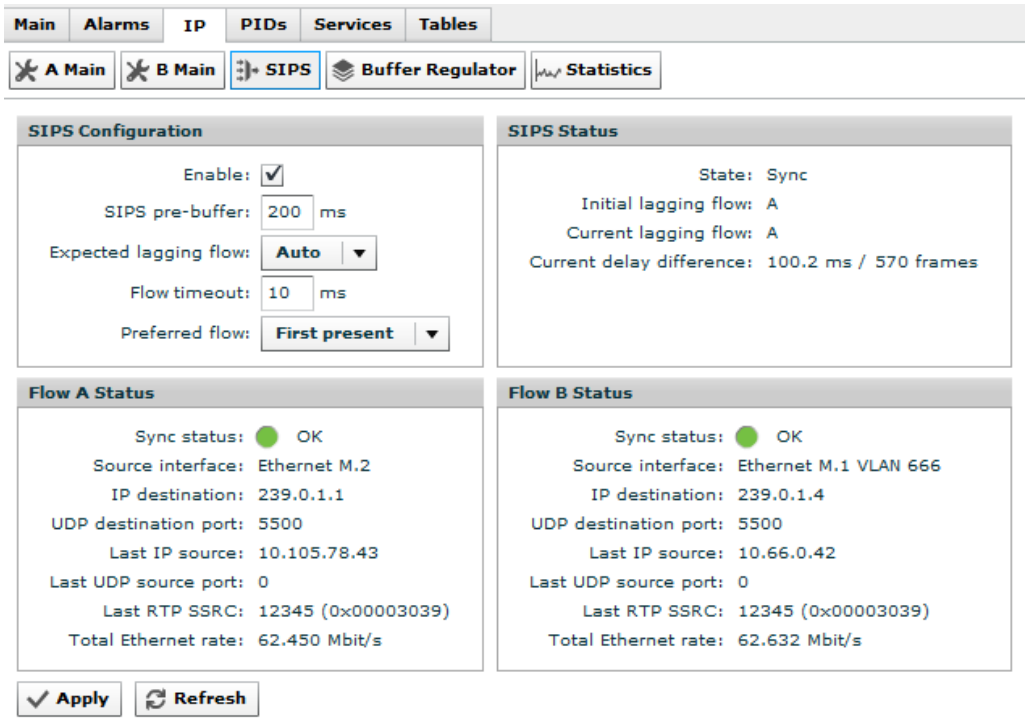


Figure 8.65 SIPS Configuration

Enable
: Enables the SIPS module, and enables the Main B tab where IP receive parameters for Flow B may be configured.

SIPS pre-buffer
: The pre-buffer delay is the maximum expected temporal latency difference between the two received IP media flows. Set this parameter to the highest anticipated delay difference between Flow A and Flow B.

If the Current delay difference status value under SIPS Status is higher than the configured SIPS pre-buffer parameter, an alarm will be raised, as there will be problems with the stream merging. If this is the case, the SIPS pre-buffer parameter needs to be increased to be higher than the current delay difference to allow for problem free operation.

Expected lagging flow

Allows configuration of which of Flow A and Flow B that is expected to be lagging in time, or have the greatest transit latency to the receive node.

If Auto is selected the lagging flow is detected automatically, but this mode may introduce extra receive delay depending on whether the leading or lagging or both flows are present at reception startup. This is because the receiver needs to account for a possible jump in both directions in the receive buffer if the leading stream is no longer present.

Manually configuring A or B as the expected lagging flow, will minimize the receive delay introduced, regardless of which flow is present at startup.

Flow timeout

If two non-identical media flows are received at input A and B, only the first present will be used as the source for the output signal. The Flow timeout parameter configures how long the original IP flow may be absent before the output is switched over to using the other input flow, and from then on effectively blocking the initial input flow if it reappears - as long as the input flows are not identical.

The Flow timeout parameter configures for how long the next IP frame of the preferred flow may be delayed compared to its expected arrival time, given the media stream rate, before the flow is considered lost.

This means that the parameter should be set higher than the expected network jitter, but also, to allow for an undisrupted output signal, the value should be set lower than the differential delay between the two input flows. This is to ensure a signal fall-over happens before the SIPS merge buffer is exhausted at the event of a flow timeout.

Preferred flow

If two non-identical media flows are received at input A and B, as default, only the first present will be used as the source for the output signal. The Preferred flow parameter configures which IP flow will be preferred in this scenario.

First present will prefer the flow that has been present for the longest duration. If the first flow disappears, and the Flow timeout period has passed, the other flow will be un-blocked and used as the preferred output signal, even if the initial flow later reappears.

A / B selects a specific flow that will be preferred, no matter which flow was present first. When two identical flows are present, this setting will decide which flow that will keep running if one of the inputs changes and the input flows no longer are identical.

When a specific flow is selected as preferred, this flow will be used as long as it is present. If the preferred flow disappears, the other flow (identical or not) will resume. As long as the preferred flow is not present, the non-preferred flow will be used as the media source. When the preferred flow reappears, this will take precedence and be used as the media source, no matter if it is identical to the flow running at the time or not.

SIPS Status

State
: The state parameter gives information about the state of the SIPS engine.

  Sync indicates that the two input flows are received and merged correctly.

  Not sync indicated that there is problems with one of the input streams, either that it is not present or that the input signals are not identical.

Initial lagging flow
: Which flow was lagging at channel reception startup.

Current lagging flow
: Which flow is currently lagging.

Current delay difference
: The current time delay difference between Flow A and Flow B at the point of reception.

Flow A/B Status
: This area summarizes the input status for IP Flow A and Flow B.

  Use the A Main and B Main tabs to configure the IP receive parameters for the two input flows.

8.6.2.3.3 FEC

The FEC sub page is shown in **Figure 8.66**. This page displays the status of the forward error correction processing of the IP input.

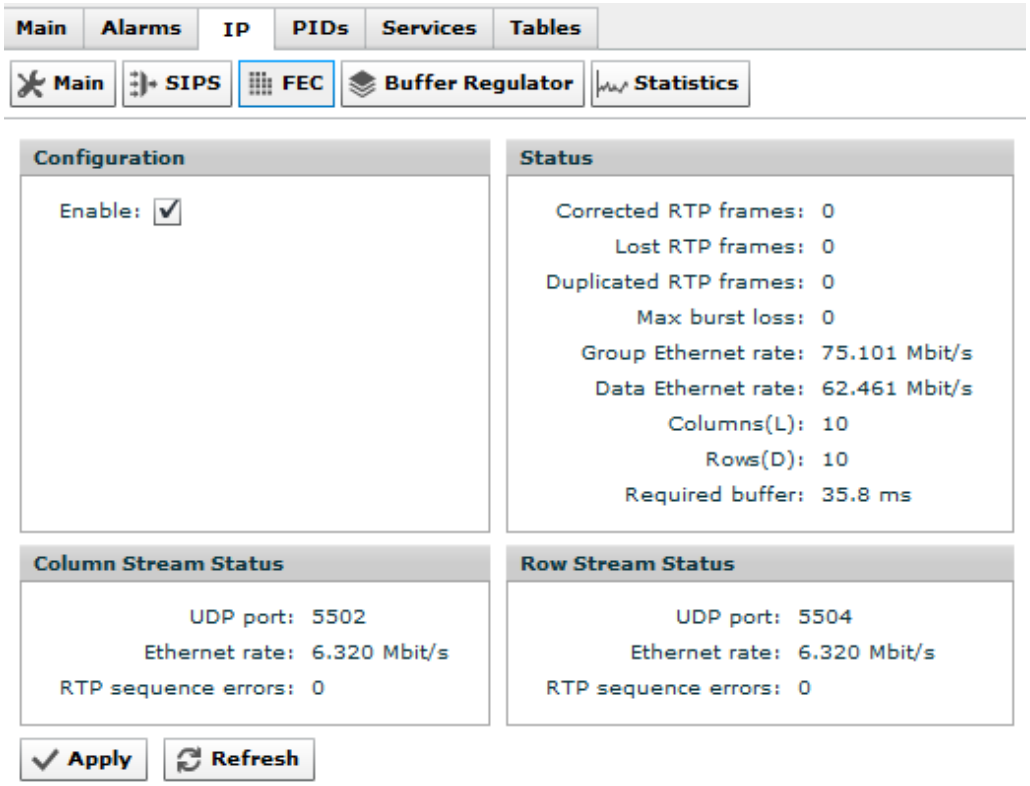


Figure 8.66 Input FEC configuration

The Configuration field provides a single check box to enable or disable input FEC processing.

The Status“ field shows the overall result of the FEC processing:

Corrected RTP frames
: The number of IP frames that were successfully regenerated by the FEC processing.

Lost RTP frames
: The number of IP frames lost. I.e. FEC processing has not been able to recover these frames.

Duplicated RTP frames
: The number of IP frames that have been regenerated while also being received correctly. This occurs if the IP frame is received out-of-order with sufficiently long delay (thus regarded as lost by the FEC processor).

Max Burst Loss
: The maximum number of consecutive IP frames that have been lost.

Group Ethernet rate
: The combined bitrate of the data frames and any FEC data related to this stream.

Data Ethernet rate
: The bitrate of the data frames excluding any FEC data related to this stream.

Columns(L)
: The number of columns used in the FEC matrix of the incoming signal.

Rows(D)
: The number of rows used in the FEC matrix of the incoming signal.

Required buffer
: The minimum size in milliseconds required by the input FEC processor to handle the incoming FEC matrix. The size of the IP receive buffer is configured on the Buffer Regulator subpage, see **Section 8.6.2.3.4**. If the input buffer is smaller than what is required for performing the FEC algorithm, the Too low latency for FEC alarm will be raised as FEC correction may not work as expected.

The Column Stream Status and Row Stream Status fields show the status of the IP stream carrying the column and row FEC IP datagrams, respectively:

UDP port
: The UDP ports receiving the column/row FEC data. Column = data port+2, row = data port+4.

Ethernet rate
: The bitrates of the column and row FEC data.

RTP sequence errors
: Shows the number of disruption in the sequence count of the RTP protocol. Data, column and row all have their own RTP sequence numbers.

For further details of FEC properties and usage, see **Appendix C**.

8.6.2.3.4 Buffer regulator

The Buffer regulator sub page is shown if figure 8.67. The IP receive buffer is used for compensating for IP network jitter and delay changes, and the regulator is used to maintain a constant receiver buffer by slowly adjusting the buffer play-out rate.

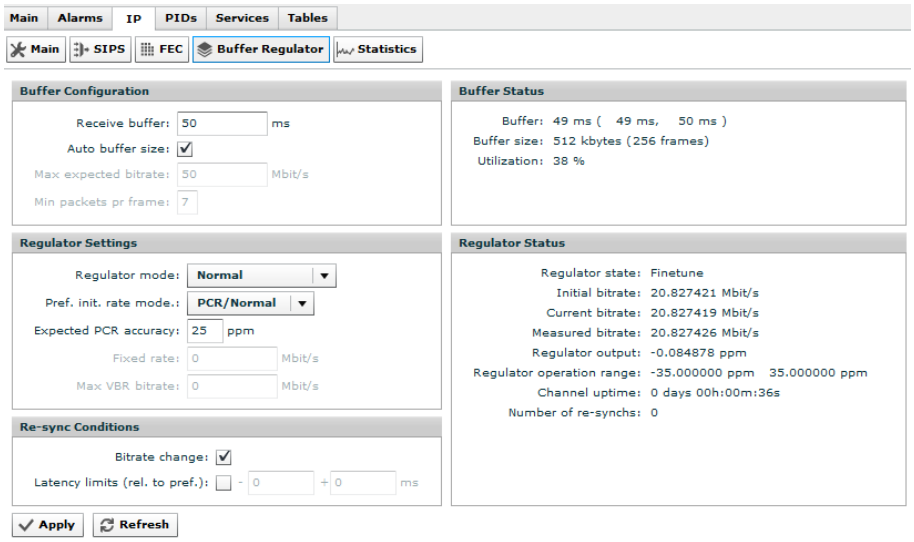


Figure 8.67 Buffer Regulator configuration

The Buffer Configuration section:

Receive buffer
: Specify the size of the receiver buffer in milliseconds. The buffer must be large enough to compensate for network packet jitter, network delay jumps, and the buffering required for FEC correction if applicable. The unit will always try to maintain a constant buffer size by slowly adjusting the playout rate from the buffer.

Auto buffer size
: The unit will automatically calculate the buffer size in bytes based on incoming bitrate to be able to buffer the Receive buffer number of milliseconds. This option should typically be enabled, but might be useful to disable in some cases where there are very high bitrate stream with high buffers.

Max expected bitrate
: Only used if Auto buffer size is disabled. This option, combined with Receive buffer, is used to calculation the receive buffer size in bytes.

Min packets pr frame
: Only used if Auto buffer size is disabled. Specify number of TS packets per IP frame.

The Buffer Status section:

Buffer
: Current size of receiver buffer. The unit will always try to keep the buffer at the configured Receive buffer value, but might sometimes be off target due to jittering signals or if the initial

buffer playout rate was too far from the actual bitrate. Minimum and maximum values are also shown in the parenthesis.

Buffer size
: Maximum size of buffer allocated in the unit.

Utilization
: Indicates how much of the allocated buffer is currently being used. Will typically be a lot less than 100% to have some margin.

The Regulator Settings section:

Regulator mode
: From the pull-down list select the preferred regulator operation mode.

  Normal
  : The default mode is Normal. Regulator will stay within ASI playout specifications.

  Coarse
  : In this mode the units attempts to set up the regulator very fast on the expense of possible jitter on the output. For ASI output this may initially create jitter outside of the specification and should only be used when having IP -> IP transmission. This mode is needed sometime if input signal jitter too much for Normal mode to keep track.

  SFN lock MIP
  : Requires rate mode DVB-T MIP. In this mode the regulator is disabled. Requires that the unit is locked to the same external 1PPS time as the MIP transmitter.

  SFN lock Manual
  : Same as SFN lock MIP, but uses the configured Fixed rate bitrate for playout.

  VBR
  : In this mode the unit attempts to read data from the input buffer at the rate entered in the Max VBR bitrate input. If the incoming rate is higher than this a buffer overflow alarm will be triggered.

Pref. init. rate mode
: From the pull-down list select the preferred algorithm to find the initial bitrate of a received data stream.

  PCR/Normal
  : The default mode is PCR/Normal, in which case a number of consecutive TS packets of the first PCR PID encountered are used to calculate the bitrate. If no PCR PID is found simple bitrate measurement over a couple of seconds is used.

  Coarse
  : Simple measurement of bitrate. May be used if the PCR is incorrect and not synchronized with the stream itself.

  DVB-T MIP
  : This mode may be used for a signal that does not contain any PCR PIDs, but does have

a DVB MIP PID (PID 21) as used in Single Frequency Networks. In MIP mode, two consecutive MIP packets are used to estimate the bitrate. The input signal must be a valid DVB-T feed in the sense that the MIP is valid, for this mode to work.

Expected PCR accuracy
: The expected clock accuracy of the PCR in the input signal. The configured value affects how far off the initial bitrate (determined from the incoming PCR) the buffer regulator may adjust the output bitrate to compensate for input latency. The default value (25ppm) should be sufficient to handle signals from professional DVB equipment at the same time guaranteeing that the output bitrate does not deviate beyond 25ppm. If you want to synchronise to streams coming from sources with less accurate clocks, you may have to configure a wider operation range to allow the output clock to be tuned further off to avoid buffer over-/underflow."

Fixed rate
: Configure fixed rate to play out from buffer. Only configurable for regulator mode SFN lock Manual. Requires that unit is locked to external reference.

Max VBR bitrate
: If VBR rate mode is chosen this parameter tells the unit the bitrate to use when reading from the input buffer.

The Re-sync Conditions section:

Bitrate change
: Checking this box will make the unit re-synchronise faster in the case of small bitrate changes. PCR based bitrate measurements deviating 100ppm or more from the initially determined bitrate causes immediate buffer re-synchronisation.

Latency limits (rel. to pref.)
: Checking this box will make the unit re-synchronise if the measured latency exceeds the configured limits set in the configured preferred latency.

The Regulator Status section.

Regulator state
: This parameter shows the current state of the buffer regulator. Possible states are Stopped, Rate Estimation, Coarse and Finetune.

  When data is received and an initial bitrate estimate is found the regulator enters the Rate Estimation state, where the signal is analysed to check if a better estimate of the bitrate can be found. When a better estimate is found the regulator switches to Coarse mode where the output bitrate is coarsely moved closer to the new rate. From Coarse mode the regulator enters Finetune mode.

Initial bitrate
: Here the exact initial bitrate found is displayed.

Current bitrate
: This parameter shows the exact bitrate played out on the ASI port at the moment.

Measured bitrate
: This parameter is an input to the regulator in the Rate Estimation and Coarse phases, and

shows the bitrate measured for the data stream since last re-sync. In the first minutes after a re-sync this measurement depends on IP network jitter and is highly inaccurate. After a few minutes of operation the value gets more and more accurate and can be compared to the current bitrate to see how far off the target bitrate the regulator is operating.

Regulator output
: Indicates the amount of correction the regulator must apply to the output bitrate, with respect to the initially measured input bit rate, in order to avoid buffer under-/overflow.

Regulator operation range
: Indicates the maximum clock correction (in ppm) that may be applied. This parameter is affected by the "Expected PCR accuracy" parameter and is typically configured slightly wider to allow headroom for buffer regulation.

Channel uptime
: The elapsed time since last re-synchronisation occurred.

Number of re-synchs
: Displays the number of re-synchronisations since the last unit power up, or since the Reset Stats function was last used (see **Section 8.6.2.1**).

8.6.2.3.5 Statistics

This page is only shown if the Log IP statistics option is enabled as shown in **Figure 8.60**.

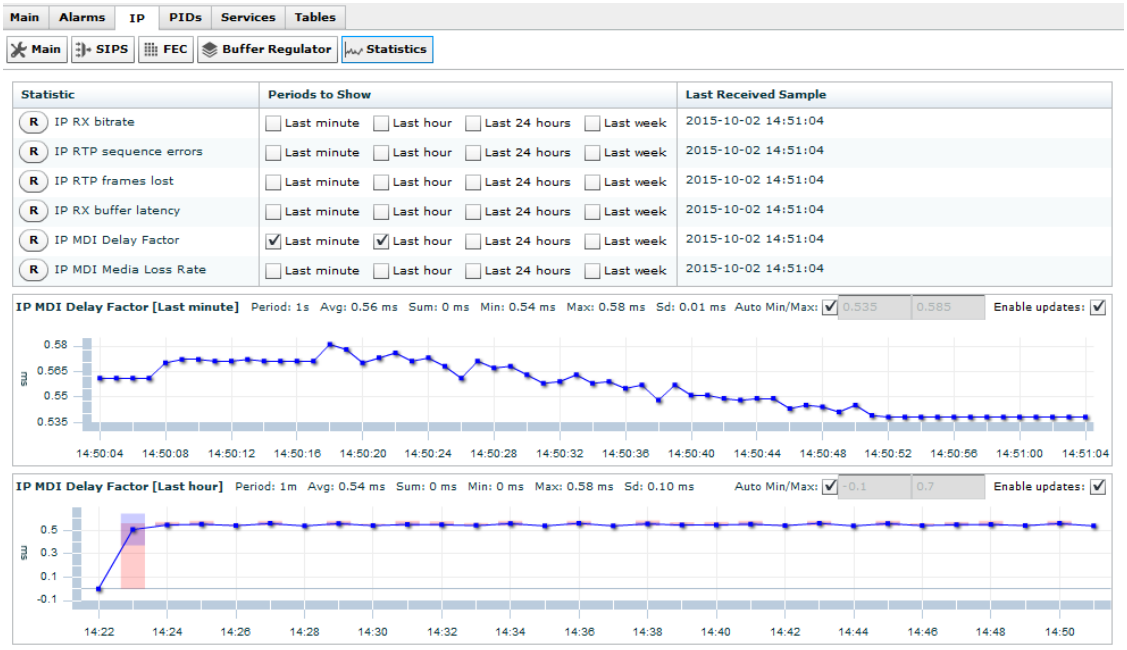


Figure 8.68 IP input statistics page

This page shows a listing of events that may be used to monitor and investigate the quality of the source IP connection as shown in **Figure 8.68**. Checking the various check boxes brings up a graph

showing the history of occurrences of the event selected for a period of time; the last minute, the last hour, the last 24 hours or the last week. The graphs are continuously updated.

8.6.2.3.6 Inter Arrival Time

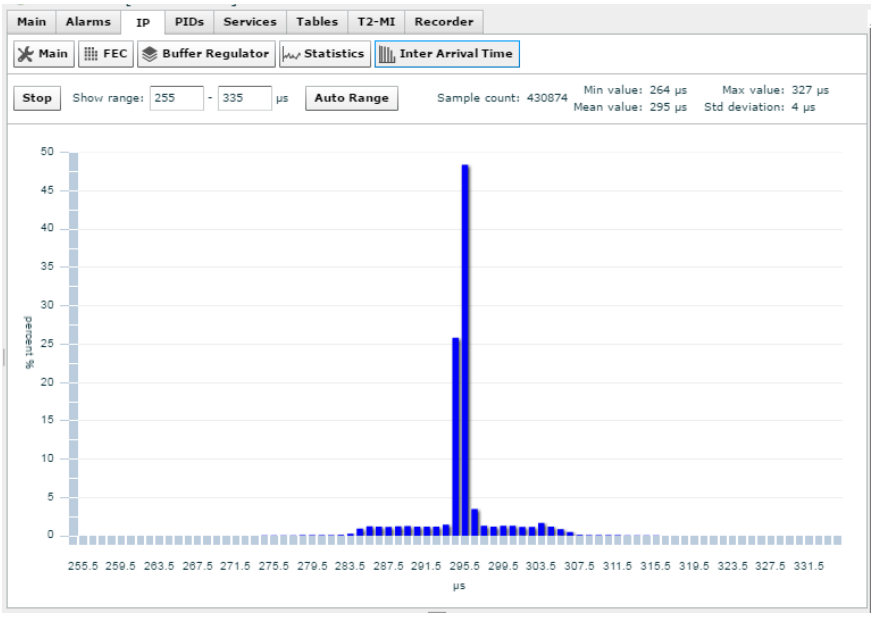


Figure 8.69 Inter Arrival Time distribution

This page displays the Inter Arrival Time distribution. The Inter Arrival Time is simply the difference in time between to successive IP packet, thus this graph provides a view of the network jitter. Press the button Restart/Stop to start/stop the measures. The range displayed can be set manually or automatically by pressing the button Auto range. Each bar of the diagram represents the percentage of inter-arrival times that matches the corresponding interval of time. Above the diagram is displayed the following information:

Sample count
: Number of samples the data is extracted from.

Min/Max value
: The minimum/maximum inter-arrival time measured.

Mean value
: The mean value.

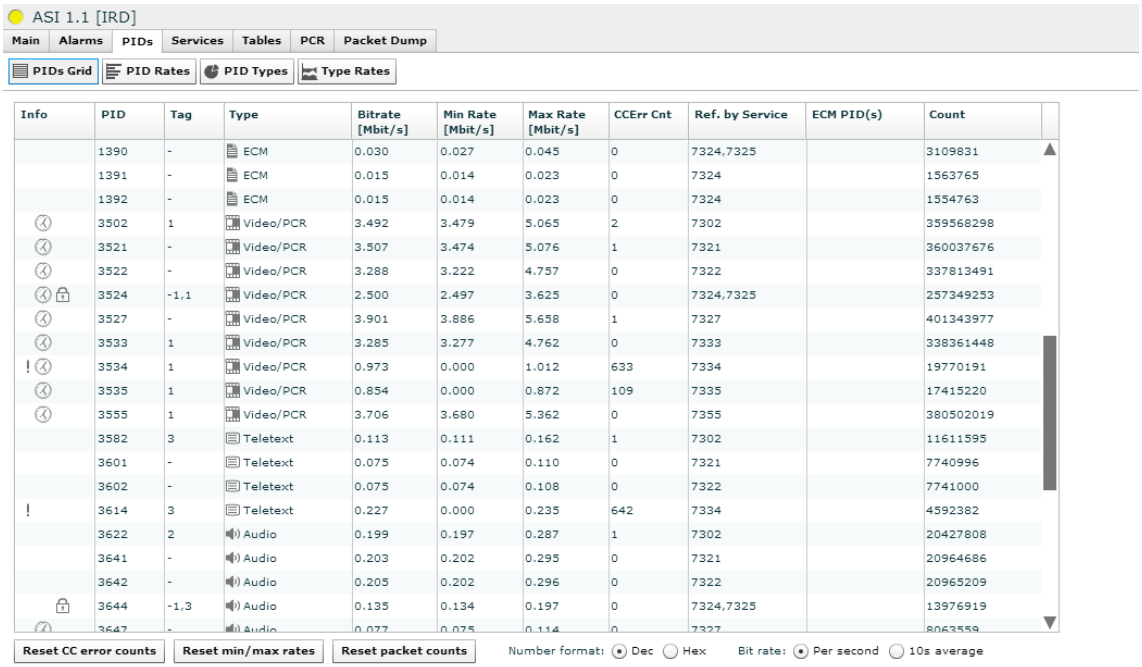
Std deviation
: The standard deviation.

8.6.2.4 PIDs

This page gives detailed information about the PIDs present on the input. Several different PID views may be selected with buttons on the tool bar at the top of the page.

8.6.2.4.1 PIDs Grid

The Grid button selects a listing of the PIDs in table form, the Rate button selects a bar graph representation, indicating dynamically the bit rate of each PID.



Info	PID	Tag	Type	Bitrate [Mbit/s]	Min Rate [Mbit/s]	Max Rate [Mbit/s]	CCErr Cnt	Ref. by Service	ECM PID(s)	Count
	1390	-	ECM	0.030	0.027	0.045	0	7324,7325		3109831
	1391	-	ECM	0.015	0.014	0.023	0	7324		1563765
	1392	-	ECM	0.015	0.014	0.023	0	7324		1554763
	3502	1	Video/PCR	3.492	3.479	5.065	2	7302		359568298
	3521	-	Video/PCR	3.507	3.474	5.076	1	7321		360037676
	3522	-	Video/PCR	3.288	3.222	4.757	0	7322		337813491
	3524	-1,1	Video/PCR	2.500	2.497	3.625	0	7324,7325		257349253
	3527	-	Video/PCR	3.901	3.886	5.658	1	7327		401343977
	3533	1	Video/PCR	3.285	3.277	4.762	0	7333		338361448
!	3534	1	Video/PCR	0.973	0.000	1.012	633	7334		19770191
	3535	1	Video/PCR	0.854	0.000	0.872	109	7335		17415220
	3555	1	Video/PCR	3.706	3.680	5.362	0	7355		380502019
	3582	3	Teletext	0.113	0.111	0.162	1	7302		11611595
	3601	-	Teletext	0.075	0.074	0.110	0	7321		7740996
	3602	-	Teletext	0.075	0.074	0.108	0	7322		7741000
!	3614	3	Teletext	0.227	0.000	0.235	642	7334		4592382
	3622	2	Audio	0.199	0.197	0.287	1	7302		20427808
	3641	-	Audio	0.203	0.202	0.295	0	7321		20964686
	3642	-	Audio	0.205	0.202	0.296	0	7322		20965209
	3644	-1,3	Audio	0.135	0.134	0.197	0	7324,7325		13976919

Figure 8.70 PID Details, table view

The PID table contains the following columns:

Info
: This column shows icons describing some aspects of the PID. The significance of the icons is given below.

Figure 8.71 Status icons in PID details

1. This icon is shown if there is an active CC error alarm related to the PID.
2. This icon is shown if the PID is a PCR PID.
3. This icon is shown if the PID is scrambled and the scrambling bit is odd.

4. This icon is shown if the PID is scrambled and the scrambling bit is even.

5. This icon is shown if the PIDs priority bit is set.

PID
: This is the packet stream id.

Type
: This is the packet stream type. Unsignalled PIDs have no type.

Bitrate
: This is the current bitrate of the packet stream in Mbit/s.

Min Rate
: This is the minimum rate of the packet stream in Mbit/s since the last rate reset.

Max Rate
: This is the maximum rate of the packet stream in Mbit/s since the last rate reset.

CCErr Cnt
: This is a counter which shows the number of Continuity Count errors on this packet stream since the last CC error count reset.

Ref. by Service
: This is a list of services referencing the PID. If there are too many services to show in the cell, holding the mouse over the cell will show a tool tip with all the services.

ECM PID(s)
: This list the PID's of the stream that contains Entitlement Control Messages.

Count
: Number of packets counted for this packet stream since last counter reset.

Beneath the PID table are three buttons:

Reset CC error counts
: This resets the CC error counters for all packet streams.

Reset min/max rates
: This button resets the min and max bit rate measurements for all packet streams.

Reset packet counts
: This button resets the packet counters for all packet streams.

8.6.2.4.2 PID rates

The PID rates sub-tab is shown in figure 8.72. To the left is the bar chart showing the PIDs and to the right are some options for configuring the view.

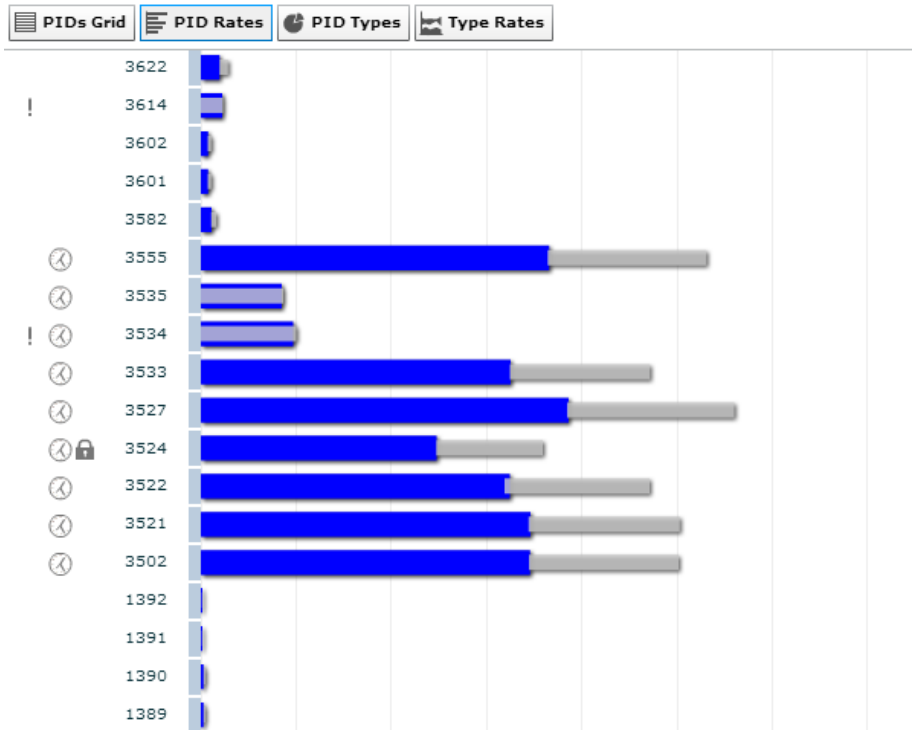


Figure 8.72 PID Details, rate view

Vertically, the chart displays one bar for each of the packet streams present on the input. Adjacent to the PIDs the symbols shown in figure 8.71 are shown if relevant.

Horisontally, the bar chart shows the current rate and the minimum and maximum rates measured for each packet stream. The blue bar shows the current rate. The grey bar shows minimum and maximum rates. Holding the mouse cursor over a bar shows a tool tip with the rates as a numeric value.

8.6.2.4.3 PID Types

The PID Types sub-tab shown in figure 8.73 displays the current contribution of each type of component in the total bitrate of the stream.

8.6.2.4.4 Type Rates

The Type Rates sub-tab shown in figure 8.74 displays the current bitrate of all the components of one selected type.

8.6.2.5 Services

The Services page displays information relative to each service present in the stream.

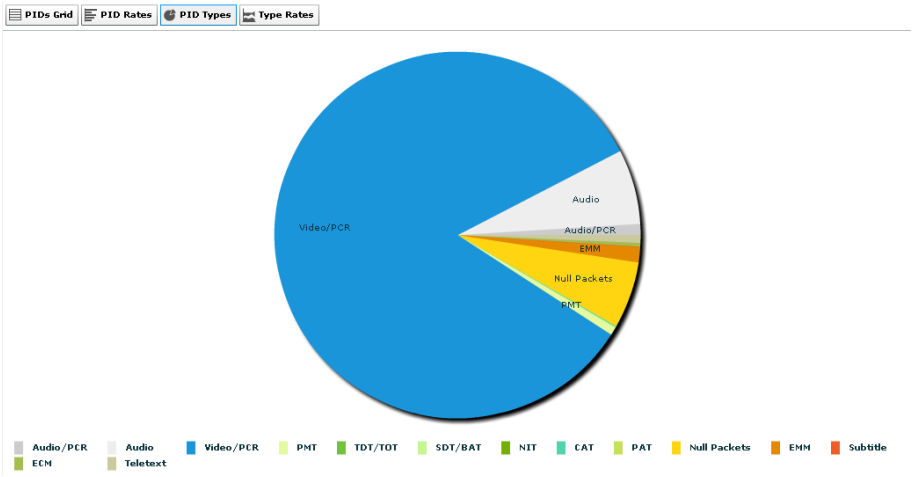


Figure 8.73 PID Details, types view

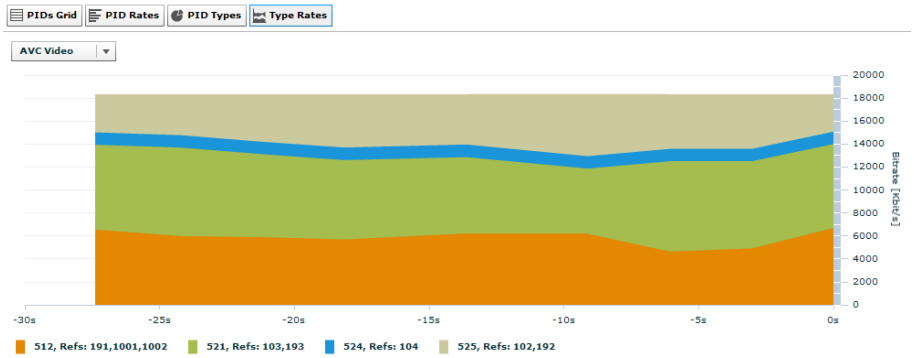


Figure 8.74 PID Details, type rates view

8.6.2.5.1 Service List

The Service List tab displays a list of services running in the selected input. Each service type is represented by a symbol colored to show the current alarm status of the service as shown in Figure 8.75. The service alarm status matches the most severe alarm severity of any alarm related to the service. When the service alarm changes, the unit may send a trap and/or put an entry in the alarm log. This alarm is called Program Severity Change (alarm id 1808) and is found in the Content folder for the TS alarms.

Sort by
: Selecting the Service ID or Name radio button sorts the list by service ID or service name, respectively.

Clicking on a service name (folder name) brings up a tab navigator to the right of the list containing more information about the selected service.

Service Details tab

The Details tab shows detailed information about the selected service. The service information may be presented in one or two sections. The first section, Service Details, is always present and consists of the following parameters:

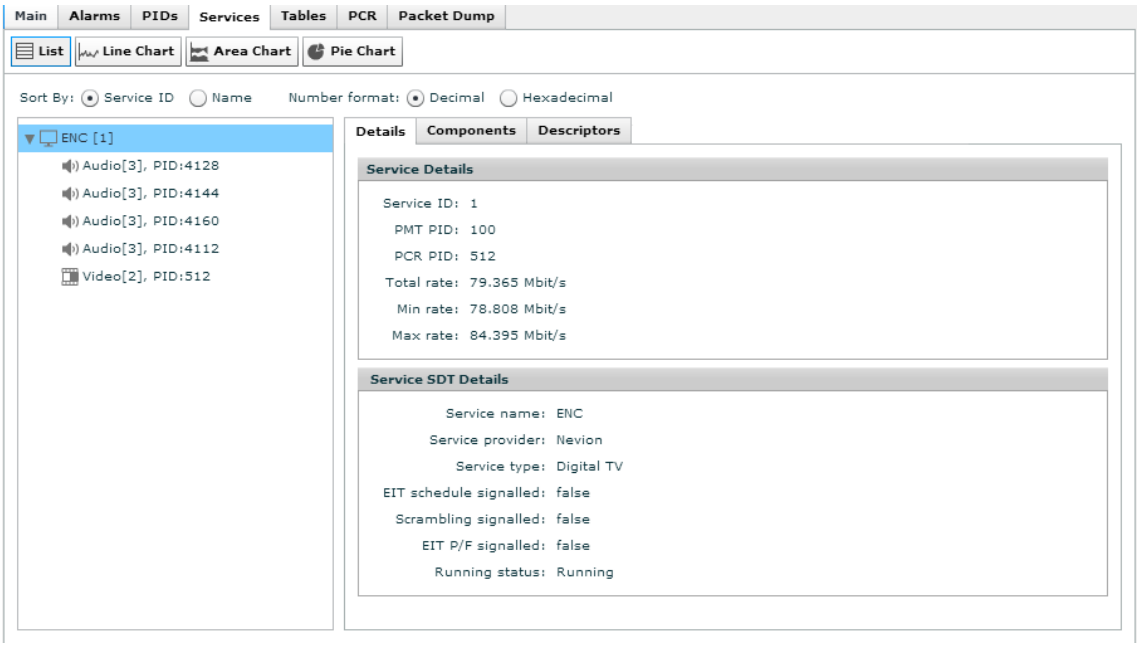


Figure 8.75 Service details overview when service list is not expanded.

Service ID
: The service id of the selected service.

PMT PID
: The program map table PID of the service.

PCR PID
: The PCR PID of the service.

Total rate
: The current bitrate of the service. The service bitrate is the sum of the bitrates of the PIDs pertaining to the service (PMT, PCR, ECMs and the component PIDs signaled in PMT). If PIDs are shared between services, the displayed sum of the bitrates of all services may exceed the total bitrate of the transport stream.

Min rate
: The minimum bit rate measured for this service since the last reset. Resets when the PID rates are reset.

Max rate
: The maximum bit rate measured for this service since the last reset. Resets when the PID rates are reset.

In DVB mode the second section, Service SDT Details, will be present only if the SDT table is present and analyzed. It consists of the following parameters:

Service name
: The name of the service.

Service provider
: The provider of the service.

Service type
: The type of service.

EIT schedule signaled
: Whether the EIT schedule information is signaled to be present for this service. This information is extracted from SDT actual.

Scrambling signaled
: Whether scrambling is signaled for the service. Interpretation of the Free_CA bit in SDT actual.

EIT P/F signaled
: Whether EIT present/following information is signaled to be present for this service. This information is extracted from SDT actual.

Running status
: The running status of the service as signaled in SDT actual.

Components tab

The Components shown in figure 8.76 tab displays detailed information about the components of the selected service, including:

PID
: The transport PID number.

Tag
: The component tag.

Type
: The component type.

Bitrate
: The current bitrate.

Min Rate
: The minimum bitrate.

Max Rate
: The maximum bitrate.

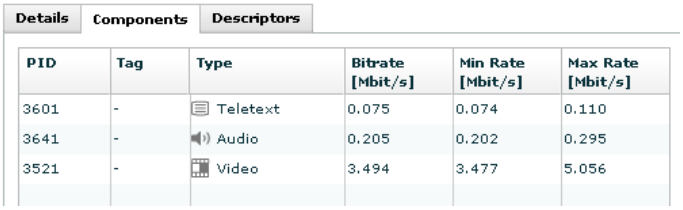


Figure 8.76 Service components overview

Descriptors tab

The Descriptors shown in Figure 8.77 tab displays the list of the PMT and SDT descriptors of the service.

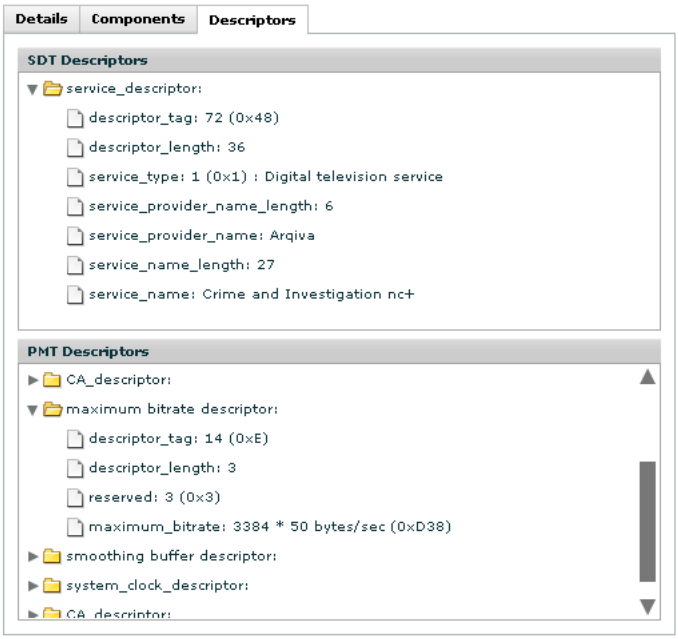


Figure 8.77 Service descriptors overview

Alarms tab

The alarms tab shows all active alarms which affects the alarm level of the service as shown in Figure 8.78. The alarms may be directly related to the service, or to one of the components of the service.

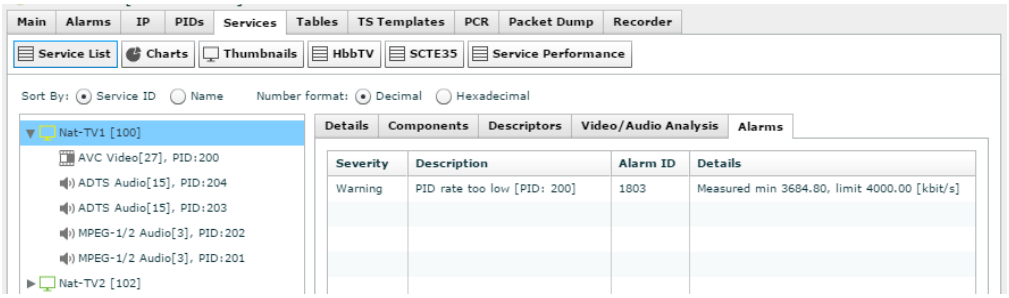


Figure 8.78 Service alarms

Component details

To list all components contained within a specific service click the arrow for the given service. The expanded view is shown in Figure 8.79.

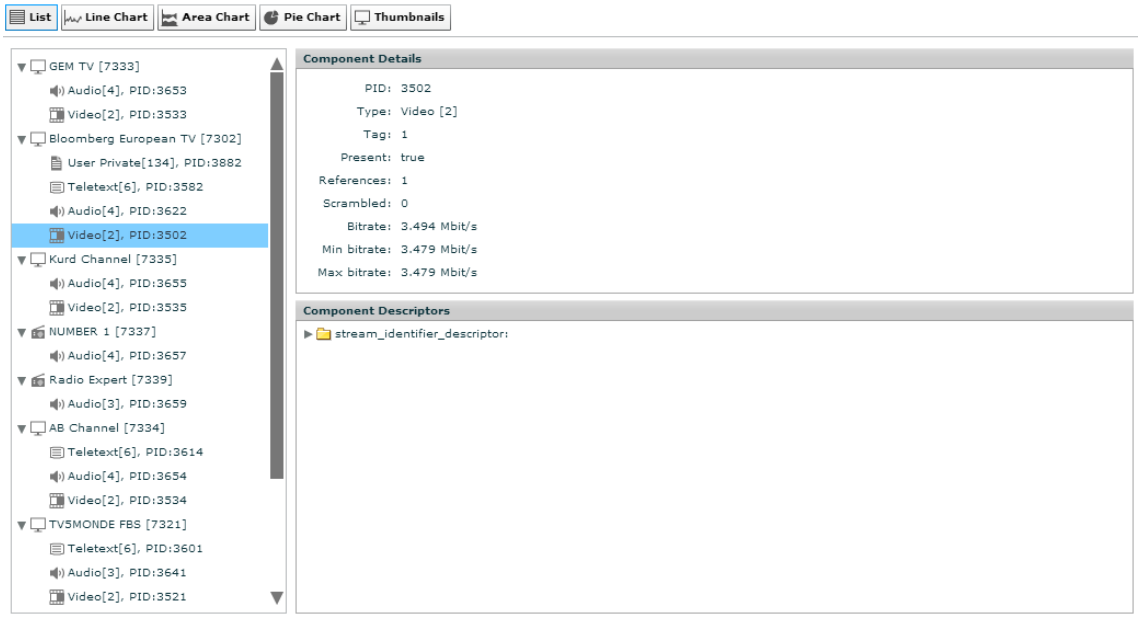


Figure 8.79 Service details full component overview

Each component is shown with the following information:

Component type symbol
: Symbol showing the kind of component.

Textual description
: A text description of the component type.

Type id
: The component type id.

PID
: The transport PID number.

Clicking on a component in the left hand list of services and components opens a Components Details view and a Component Descriptors view.

The Components Details view presents the following information:

PID
: The transport PID number.

Type
: The component type.

Tag
: The component tag.

Present
: Whether the component is currently present in the stream.

Reference
: The number of references of the component.

Scrambled
: The scrambling mode.

Bitrate
: The current bitrate.

Min Rate
: The minimum bitrate.

Max Rate
: The maximum bitrate.

The Components Descriptors lists all the descriptors associated with the selected component.

8.6.2.6 Tables

The Tables page shows detailed information about all the tables that are currently residing in the input SI database of the device. Accessing the related sub pages gives access to table contents right down to byte level.

Which tables being currently analysed by the device is also displayed.

"Tables" tab
: The button switches to a detailed view of the tables present on the input and analysed by the device.

"Settings" tab
: This button switches to a page showing what tables are being analysed.

"Table source settings" tab
: This button switches to a page allowing the user to configure non-default source PID of SI tables.

8.6.2.6.1 Tables

Figure 8.80 shows the table details in list view.

The left hand side of the page contains a tree showing the tables that are present on the input and analysed by the device. The tables belonging to a specific folder are displayed to the right by clicking on the folder.

Above the table the following information and buttons can be found:

Shown tables
: The number of table that fall into the chosen folder compared to the total number of tables.

Shown size
: The size(in bytes) of the tables that fall into the chosen folder compared to the total size of the tables.

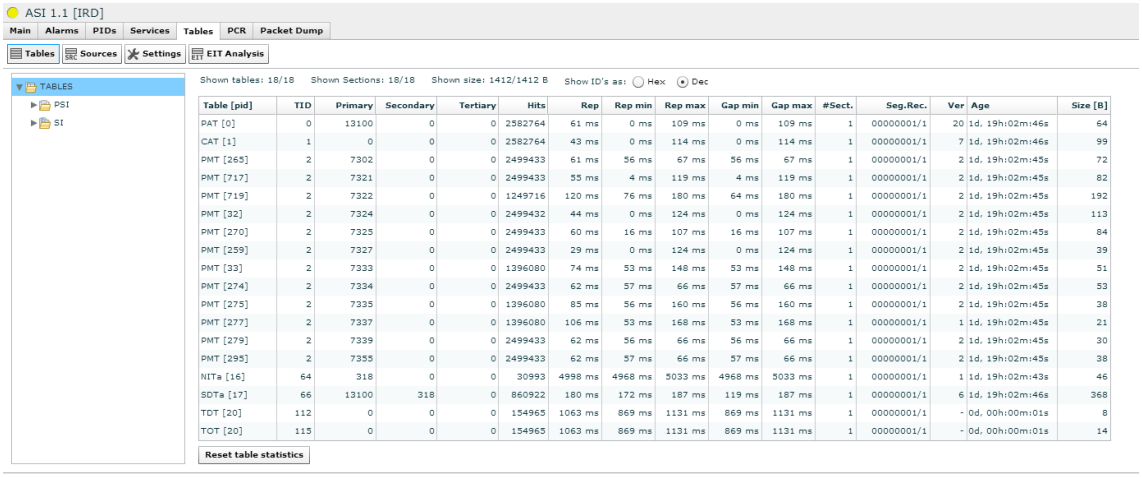


Figure 8.80 Table details, overview.

Show ID's as
: Configure to view id's and keys in hexadecimal or decimal notation.

The right hand side table of the sub page has the following columns:

Table
: The type of information table and (in braces, []) the PID containing it.

TID
: The table ID.

Primary
: The primary extension ID of the table. Hovering the mouse cursor over the value displays a tool tip describing the meaning of this key in the context of the table.

Secondary
: The secondary extension ID of the table. Hovering the mouse cursor over the value displays a tool tip describing the meaning of the secondary ID in the context of this table.

Tertiary
: The tertiary extension ID of the table. Hovering the mouse cursor over the value displays a tool tip describing the meaning of the key in the context of this table.

Ver
: This is the last received version of this table.

Age
: The time elapsed since the table was last updated. Selecting a single table from the tree to the left or double clicking a line within the table opens a view displaying the parameters of that table. The parameters are the same as are shown in the table view.

Selecting a specific table in the table tree on the left side of the "Table Details" pane presents the user with a tab view containing two tabs.

The first pane with label Details shows detailed information regarding the selected table. This pane re-iterates the details found in the TABLES column of the tree for this entry.

The second pane labelled "Decoded" allows exporting a detailed section dump. The text dump can be received as a new web page or saved to a file. When available all values are extended from bit values to their detailed type names.

To Browser
: Pops up a new browser window containing a text representation of the details found in the Decoded pane.

To File
: Pops up a standard platform Save As dialogue requesting the location to store a text representation of the details found in the Decoded pane.

Figure 8.81 shows the decoded table.

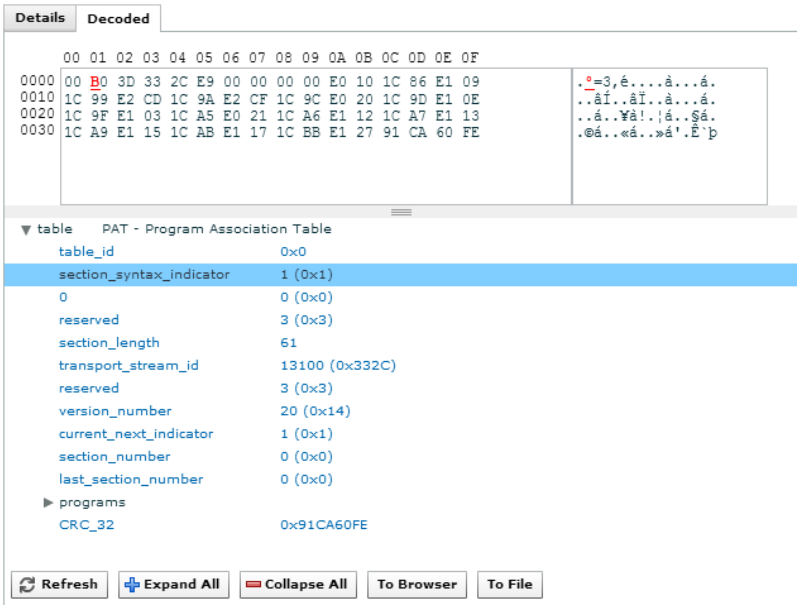


Figure 8.81 Table Details Decoded view

A debugger style hex dump of a table section and a detailed variable inspector that displays the parsed value of the table section.

By navigating the Dump tree, which makes up the bottom half of the decoded view, each series of bits in the table are parsed and displayed. If there is an error in the table the decoder will decode as many bytes as possible before failing.

8.6.2.6.2 Sources

This page allows you to configure non-standard input PID values for the section filtering of individual SI tables.

The page is shown in figure **8.82** and contains a grid with the following columns:

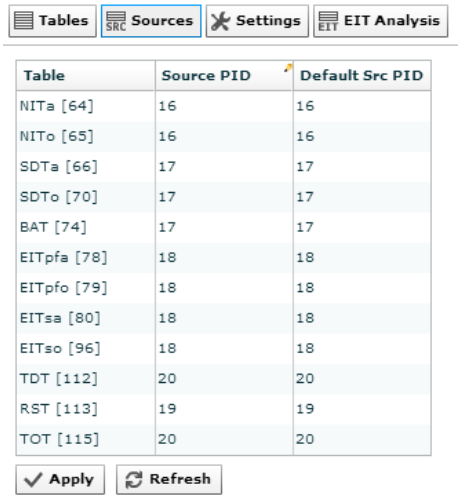


Figure 8.82 Non-standard table source PID configuration.

Table
: The table type to configure with its table ID in decimal in brackets.

Source PID
: The input PID to use in the section filter for this table ID. Click the grid cell to edit it. Edited fields are shown in yellow until applied.

Default Src PID
: The default PID used for this table type. Use this value if you want to go back to DVB compliant input filtering.

After making the changes in the grid press Apply to activate the changes. You can then go back to the table listing to see whether the expected tables are received on the new PID value.

Warning: Changing the PID values used in the input filtering must be performed with care. If you specify a PID that contains a high bandwidth PID it may cause the unit to malfunction.

8.6.2.6.3 Settings

In this sub page it is possible to select the table types to analyse. Each table type has a corresponding check box. EIT Actual and EIT Other are further configurable as they allow the number of days worth of data to be configured.

To commit changes to the settings on this page, click the Apply button located at the bottom of the page. Press Refresh to reload the settings which may have been changed by another user.

- To be able to see programs and program components you must analyse at least PAT and PMT.

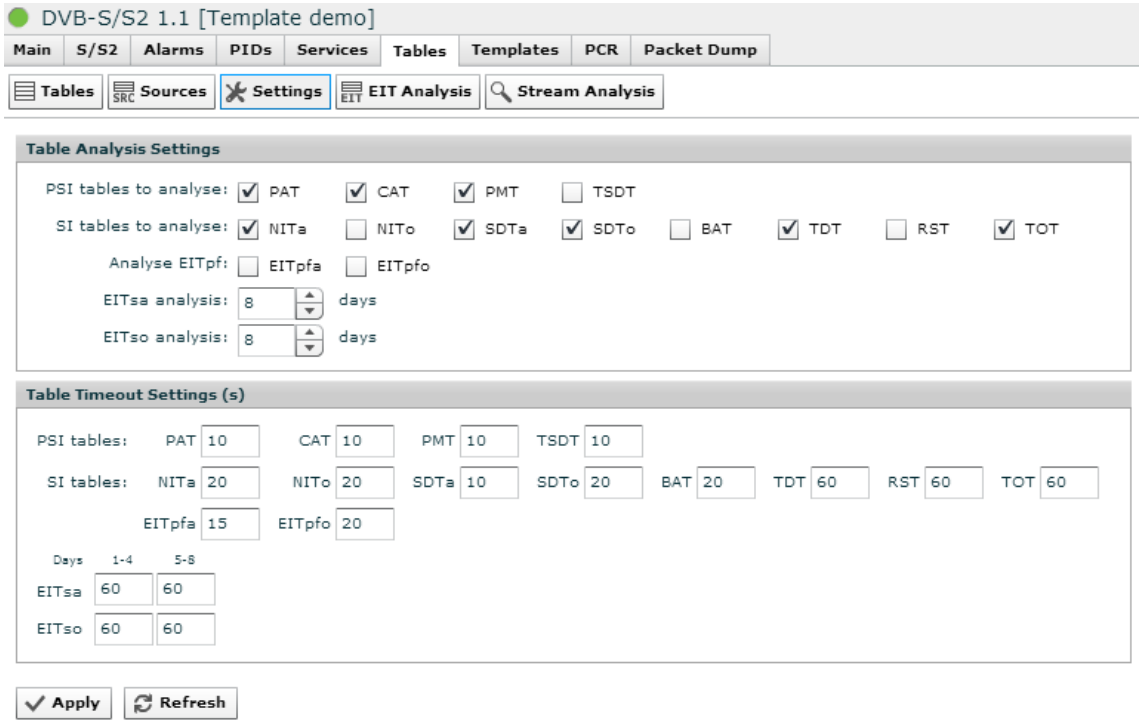


Figure 8.83 Table analysis configuration.

- To see the service name for the services you have to configure analysis of SDTa (SDT actual)
- In general alarms will not be generated for tables that are not configured for analysis.

Turning off analysis can free up CPU power and memory that may be used for other processing. E.g. if PID 18 is high bandwidth, but is not interesting for analysis, then it could be beneficial to disable EIT analysis (EITpfa, EITpfo, EITsa, EITso). In the Table Timeout Settings field it is possible to change the timeouts used when detecting the presence of each table. The values are specified in number of seconds.

Configuring larger time-out tolerances for tables that are occurring with non-standard repetition intervals can reduce the number of alarms generated. Right-clicking each timeout parameter and selecting Set to default resets the original value.

The timeout values are also used to generate Table missing alarms.

8.6.2.7 PCR

The PCR page allows you to view information about all the PCR PIDs that are currently received on the input. You can also perform PCR jitter analysis on a selected PCR PID. The first page contains a table showing all PCR PIDs currently received. It consists of the following columns:

PID
: This is the packet id.

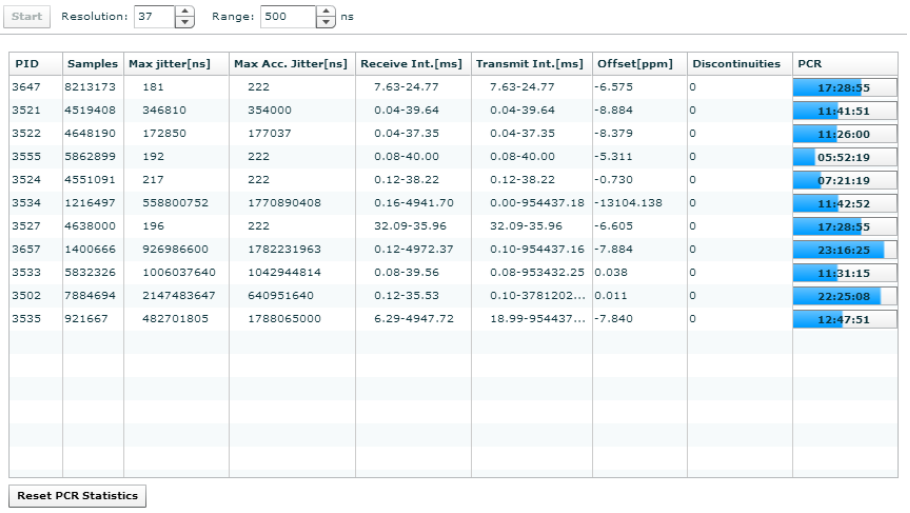


Figure 8.84 PCR PID List

Samples
: The number of Program Clock Reference samples received

Max Jitter [ms]
: This is the maximum overall jitter measured for this PID. The maximum overall jitter gives the jitter of the PCR stamps relative to the local time. Lock to external PPS to get a more precise result.

Max Acc. Jitter [ms]
: This is the maximum accuracy jitter measured for this PID. The accuracy jitter gives the jitter of the PCR stamps relative to the rate calculated using previous PCR stamps.

Receive Int. [ms]
: The minimum and maximum interval measured between each instance of the PCR PID in this stream. This measurement is done regardless of the PCR value found in the packet.

Transmit Int. [ms]
: The minimum and maximum interval between PCR values in this PID. This measurement is done purely by looking a PCR stamps, and is done regardless of local time. Should match the Receive interval for a good PCR signal.

Offset [ppm]
: This is an estimated offset in ppm (parts per million) of the incoming PCR clock as compared to the local 27MHz clock.

Discontinuities
: This is a counter that increments whenever a discontinuity is discovered in the incoming PCR values. Discontinuities are signal with a flag in the PCR field.

PCR
: This table shows the absolute PCR value. The absolute PCR value will wrap round to zero approximately every 26.5 hours.

Above the table is a button and two numeric inputs. To start a PCR jitter analysis selected a PCR PID from the table, and press the Start button. PCR jitter statistics are recorded and The Resolution and Range fields control the way the statistics are presented. The Range value determines the span of jitter values presented, the Resolution value determines the number of jitter value intervals to display. Refer to figure **Figure 8.86**.

Below the table is a button which allows you to reset the maximum jitter and the minimum and maximum intervals of all the PCR PIDs.

Pressing the Start button opens a page showing the status of the PCR jitter analysis.

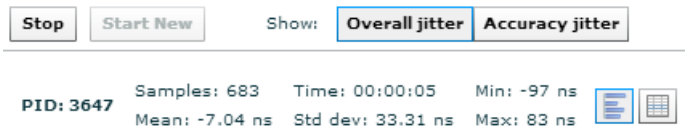


Figure 8.85 PCR Header

At the top of the page is a header. To the left in the header are two buttons. The Start New button is activated once the analysis has been stopped, and takes you back to the previous page. The Stop button stops the current analysis.

To the right of the buttons you can see which PID is currently being analysed, and status information for the current jitter measurement:

Samples
: This is the number of PCR samples registered so far.

Time
: This is the duration of the current measurement.

Mean
: This is the average jitter value.

Std dev
: This is the standard deviation of the measurements taken so far.

Min
: This is the minimum jitter value measured so far.

Max
: This is the maximum jitter value measured so far.

At the right end of the header are two buttons that you can use to view the measurements in two different ways.

The **Graph** View shows the PCR jitter values. Every jitter value recorded is placed in one of the intervals and the corresponding bar is updated. The vertical axis indicates the percentage of jitter values received. The horisontal axis shows the intervals; the label showing the mean value of each interval. By holding the mouse cursor over a bar, more information about the bar is shown.

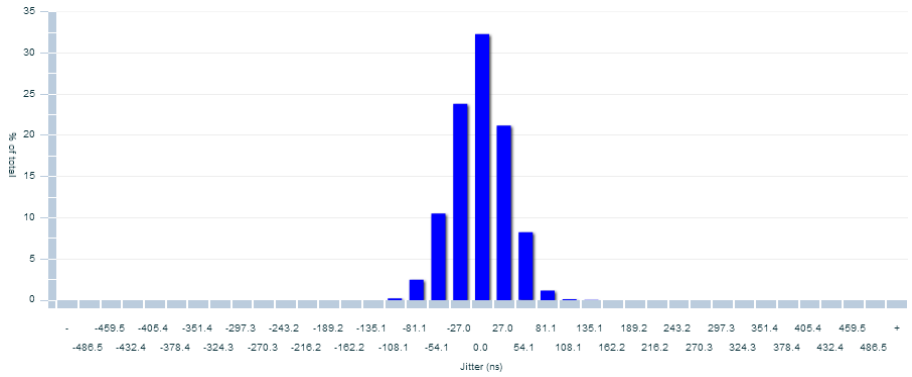


Figure 8.86 PCR Graph view

The **Table** view shows the exact same information as the graph view, but presented in a table. The Min and Max columns show the range of each interval. The Hits column shows the number of jitter values falling into a particular interval, and the Percentage column shows the percentage of the jitter values registered within this interval.

Min	Max	Hits	Percentage
-40.54	-13.51	1052	23.90
-13.51	13.51	1415	32.14
13.51	40.54	916	20.81
40.54	67.57	362	8.22
67.57	94.59	60	1.36
94.59	121.62	5	0.11
121.62	148.65	1	0.02
148.65	175.68	0	0.00
175.68	202.70	0	0.00
202.70	229.73	0	0.00
229.73	256.76	0	0.00
256.76	283.78	0	0.00
283.78	310.81	0	0.00
310.81	337.84	0	0.00
337.84	364.86	0	0.00
364.86	391.89	0	0.00

Figure 8.87 PCR Table view

8.6.2.8 Packet Dump

Note: This page is only displayed if the option Advanced monitoring is checked in the Main tab (cf. **Section 8.6.2.1**).

The packet dump page offers dumping the contents of a sequence of packets from a selected packet stream.

The first page contains a list of PIDs currently present on the input. To start dumping packets, select the PID you want to dump from the list, select the number of packets to dump and hit the Start button.

Clicking the Start button opens a new page showing the packets that are dumped. At the top of this page are two buttons. While the packet dump is running the Stop Dump button is activated

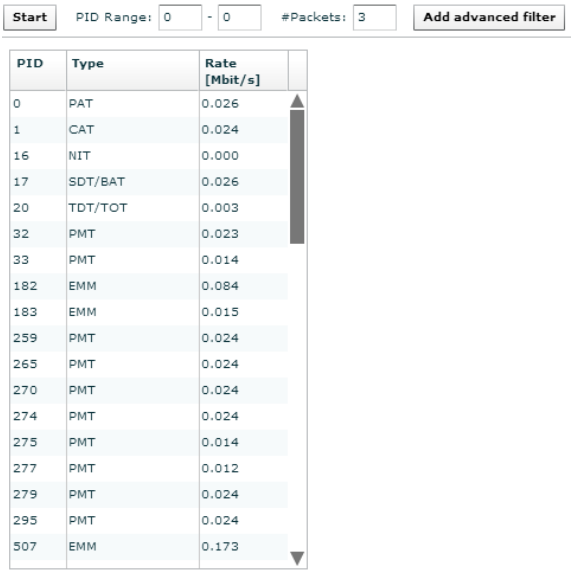


Figure 8.88 Packet Dump

Figure 8.89 Packet Dump Progress

and can be hit to terminate the packet dump. Once the packet dump is finished, either by dumping the specified number of packets or by hitting Stop Dump, the Start New button is activated and can be used to return to the previous page to start a new dump.

Below the two buttons is a text showing the current status of the packet dump. It shows the PID being dumped, the number of packets currently dumped and the total number of packets that has been requested. To the right of the text is an icon showing if the dump is still running.

The transport packet dump may be saved by clicking the Save Dump button in the GUI. This initiates a standard "Save file" dialogue.

When packet dump is ended the main part of the page contains a tab bar with three tabs.

The **Packets** tab contains a table listing all packets that have been dumped. The first column of the table is simply an index showing the packet number. The second column shows the time interval in seconds between that packet and the first packet that was dumped. The third column shows the time interval in seconds between that packet and the preceding dumped packet.

Selecting a packet in the list opens a more detailed view of that packet. At the top is a string showing the same details as presented in the table. Below this is the raw data of the packet, shown byte by byte. At the bottom is shown a decoded view of the packet Transport Stream header.

The **Delta first** tab shows a graph with the delta first value of all the dumped packets. This gives an indication of the packet rate variation over time of the selected packet stream.

The **Delta previous** tab shows a plot of the delta previous values of all the dumped packets. This gives another view of the rate variation over time of the packet stream.

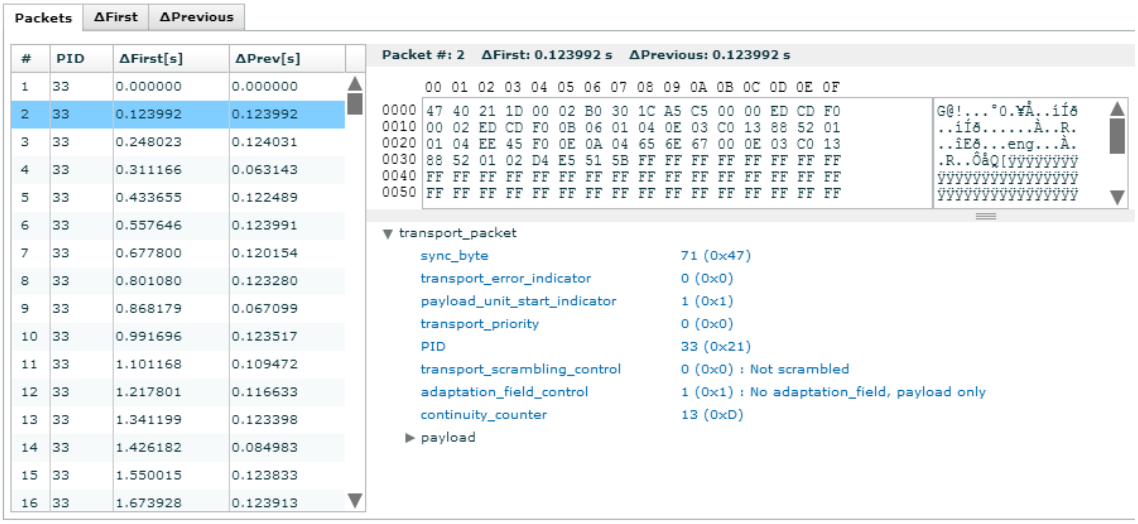


Figure 8.90 Packet Dump Packets

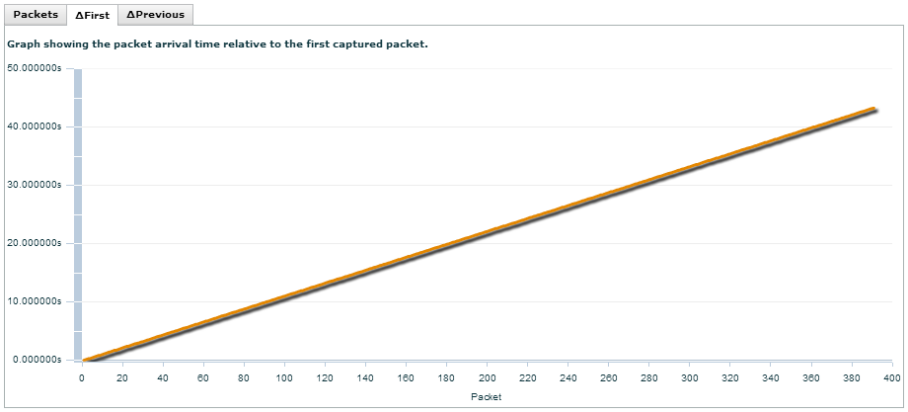


Figure 8.91 Packet Dump Delta First

Pressing the Add advanced filter brings up the dialog box shown in figure 8.93. In this dialog box, the user can add advanced filters to the packet dumping. By ticking the box at the top, saying Capture all packets after first filter match, all packets after the first filter match will be captured, even if they don't match the filter specified below.

The TS Header Filter and Adaptation Field Header Filter sections provide the user with a number of fields to specify the advanced filter for the packet dumping.

8.6.3 Audio Inputs

8.6.3.1 Audio-IP Input

The Audio-IP Input element represents an audio over IP stream received from the network. The stream may contain one or more audio channels that can be made available for internal routing and use in the device.

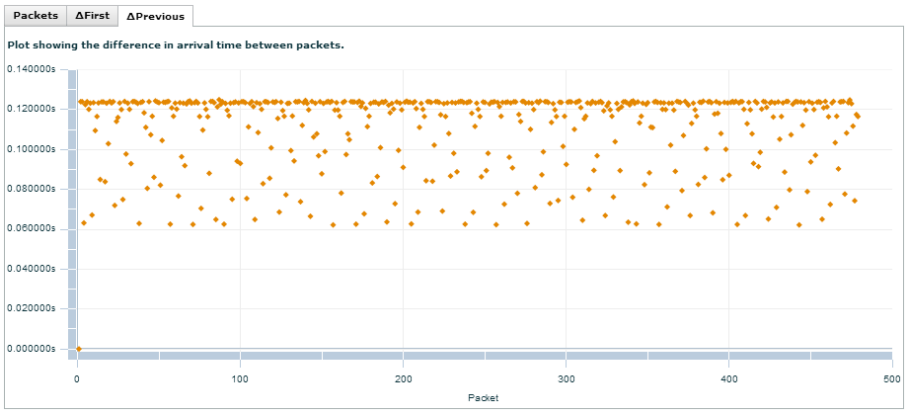


Figure 8.92 Packet Dump Delta Previous

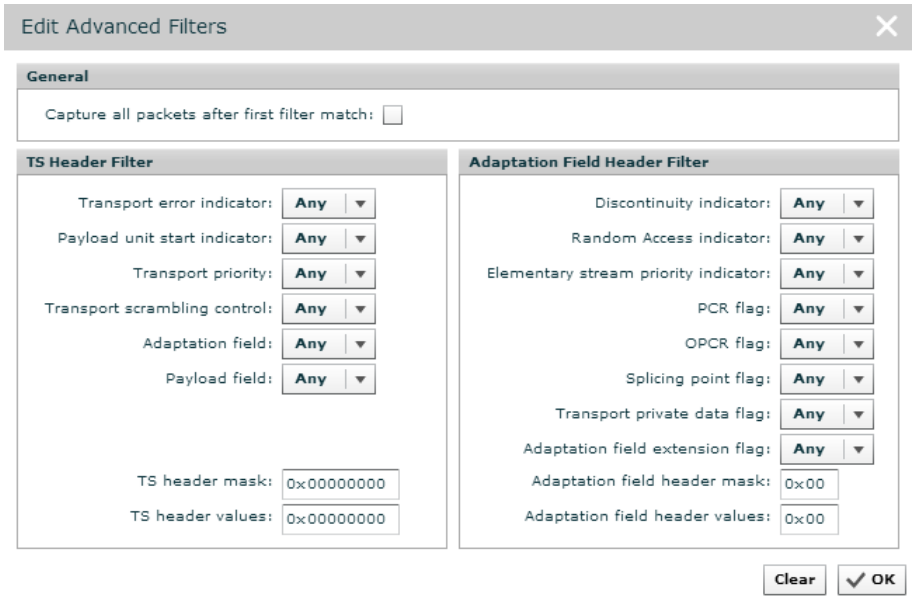


Figure 8.93 Edit advanced filters dialog box for packet dump tab.

The received audio RTP stream must conform to AES67-2015, meaning both the stream source and the receiving device must be locked to PTP. No adaptive rate recovery is supported in this version.

8.6.3.1.1 Audio-IP In - Main

The Audio-IP input Main tab is shown in figure 8.94. The most important configuration and status parameters are available on this page.

The Audio-IP Input Configuration section contains settings related to the audio stream:

Label
: A user configurable label. Is used as a tag in the user interface to ease navigation and stream identification.

Figure 8.94 Main tab for an Audio-IP input channel

Sample format
: The stream sample format bit depth. This parameter must be configured correctly to be able to receive a network stream. After this parameter has been configured, the receiver will automatically determine the packet length and audio channel count of the stream.

Warning: If the Sample format parameter is incorrectly configured, stream reception will not work, or erroneous audio data will be extracted and made available for routing in the device. Routing such erroneous audio to speakers or headphones may cause harm to equipment or hearing.

Max channels in stream
: The maximum number of audio channels per stream that should be supported. Streams with any number of audio channels below this value can be correctly received. If receiving a stream with a higher audio channel count, the available audio channels will be truncated to the configured value, making only the first channels of the stream available for use in the device.

Link offset (samples)
: The number of samples delay or offset between the originating source input time and playout

time in the receiving device. The value of this parameter must at least be 3x the packet length (samples) of the received stream or higher. Refer to AES67-2018 section 7.4 for an exhaustive explanation of this parameter and the realistic minimum value.

RTP TS offset
: Offset of the RTP Timestamp header field at the PTP Epoch. For SMPTE 2110-30/31 this value is defined to be zero, while in AES67 the value may be arbitrary and is signalled in the SDP describing the stream.

The Audio-IP Input Status section contains status related to the received audio stream:

Packet length
: The packet length of the currently received audio stream.

Channels in stream
: The audio channel count of the currently received audio stream.

Link offset (samples)
: The actual link offset value currently used. Refer to AES67-2015 section 7.4 for an exhaustive explanation of this parameter.

Current RTP SSRC
: The RTP SSRC value of the currently received audio stream.

The Audio Channel Info section contains status for the received audio channels:

The virtual LEDs in this view shows the status of the received audio channels, according to this coding:

- Grey: No audio present
- Transparent: Audio channel is present but audio sample contents indicate silence
- Green: Audio channel is present and contains audio samples with non-silence
- Yellow: Audio channel has an associated alarm
- Red: Audio channel is present but level is above peak threshold

The Flow X Configuration section contains settings related to the IP and UDP network layer:

Enable
: Check this box and press Apply to enable stream reception on this channel. If this box is unchecked, no audio stream will be received, and all alarms related to this Audio-IP In channel will be cleared.

Receive port
: UDP port to listen on. This parameter is used for both unicast and multicast reception.

Join multicast
: Whether to join a multicast stream, or only receive unicast traffic addressed to the device. If checked, the IP multicast group address configured in the text field will be received instead of unicast traffic.

Source interface
: Specify which Ethernet interface the incoming IP stream should be received on.

The Flow X Status section gives more details about the received RTP stream:

Alarm status
: Shows the alarm status of this specific IP flow. This only applies to flow X, and does not reflect the top level alarm status of the Audio-IP In channel.

Last RTP SSRC
: The RTP SSRC value last received on this IP flow.

RTP sequence errors
: The number of RTP sequence errors on this IP flow. Sequence errors may be caused by lost packets or packets received out of order. When receiving a healthy IP stream, this counter should be constant.

Total Ethernet rate
: The total Ethernet bitrate of the received IP flow, including all network headers.

Payload rate
: The payload bitrate of the received IP flow, excluding network headers. For the Audio-IP Input channel, this is the actual audio sample data rate.

8.6.3.1.2 Audio-IP In - Alarms

The Alarms tab lets the user configure specific filters and severity levels for the alarms associated with the Audio-IP Input channel. Refer to **Section 8.6.2.2** for an in-depth general explanation of alarm configuration of the device.

8.6.3.1.3 Audio-IP In - Monitor

The Audio-IP input Monitor tab allows the user to configure audio channel templates for alarm monitoring of channel presence, silence, peak and stuck peak level (tone detection). See **Section 8.9.2.3** for an explanation of the functionality.

Note that this functionality requires a special licence key.

8.6.3.1.4 Audio-IP In - IP

The Audio-IP input IP tab allows the user to set advanced configuration options for the IP reception. This includes configuration of the SIPS redundancy function. See **Section 8.6.4.1.3** for an explanation of the functionality.

8.6.3.1.5 Audio-IP In - Audio

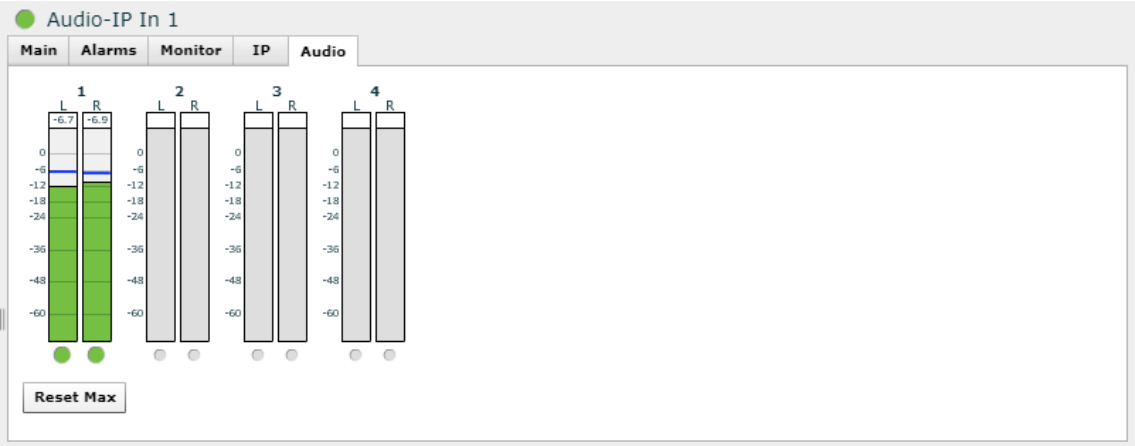


Figure 8.95 Audio tab for an Audio-IP In channel

The Audio-IP input Audio tab is shown in figure 8.95. Here basic audio meters showing the sample peak level for each audio channel in the received stream are shown.

At the top of the meters, the maximum sample peak level is indicated with a text label. A red overload indicator is also present at the top of the meter, to indicate that 0 dBFS has been reached. Both sample peak level and the overload indicator are sticky, and to reset them press the Reset Max button below the meters.

8.6.4 Video Inputs

8.6.4.1 Video-IP Input

The Video-IP Input element represents a video over IP stream received from the network.

The received video RTP stream must conform to SMPTE 2022-6. For use of seamless IP protection switching (SIPS), streams received must conform to SMPTE 2022-7.

8.6.4.1.1 Video-IP In - Main

The Video-IP input Main tab is shown in figure 8.96. The most important configuration and status parameters are available on this page.

The Video-IP Input Configuration section contains settings related to the video stream:

Label
: A user configurable label. Is used as a tag in the user interface to ease navigation and stream identification.

Mode
: Specify the most complex video standard that should be supported. This choice will affect what kind of licence that is required to enable the channel.

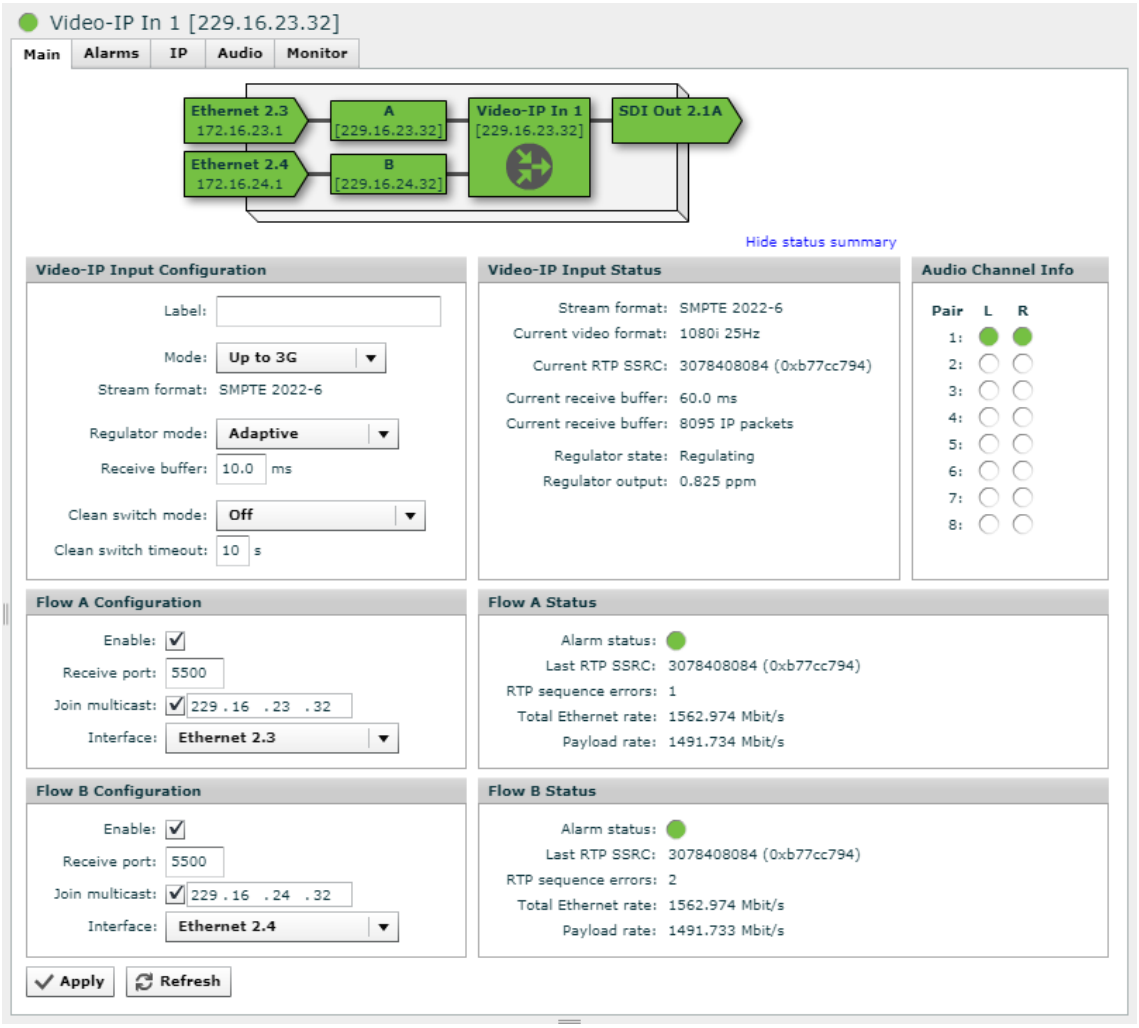


Figure 8.96 Main tab for a Video-IP input channel

Stream format
: Indicates which RTP stream format is used for carrying the video, e.g. SMPTE 2022-6.

Regulator mode
: Selection of IP receive buffer regulation mode.

- Adaptive: The playout rate of the buffer is regulated to keep the receive buffer filling at the specified level.
- PTP/VSF TR-04: The playout rate is fixed to the nominal rate of the video format present. This option requires both the device and the received stream to be locked to PTP. The Receive buffer parameter still determines the size of the IP buffer.

Receive buffer
: Buffer delay of the IP receive buffer. This must be configured to be higher than the max anticipated packet jitter on the IP network.

Clean switch mode
: Selection of IP clean switch mode.

- Off: No clean switch performed, receive buffer is resynchronized if input signal changes.
- Break Before Make: A clean-switch is performed when an existing input signal is removed and another signal is immediately re-connected. The signal that is being switched to must have the same format as the signal already present.

Note: Clean switch is only supported with Regulator mode set to PTP/VSF TR-04, in other words for PTP locked signals only. To achieve the clean switch, an additional video frame worth of delay is added to the configured Receive buffer size in this mode.

Clean-switch timeout
: The maximum time the clean-switch mechanism should allow reconnection of the next signal. After this period has passed, the channel will enter the sync loss state.

The Video-IP Input Status section contains status related to the received video stream:

Stream format
: The currently received RTP video stream format.

Current video format
: The currently detected video format that is received in the IP stream.

Current RTP SSRC
: The RTP SSRC value of the currently received video stream.

Current receive buffer
: The current actual IP receive buffer filling, measured in ms or IP packets.

Regulator state
: The state of the IP receive buffer regulator.

Regulator output
: The current deviation of the IP buffer playout rate from the nominal video format rate, as currently given by the buffer regulator.

The Audio Channel Info section contains status for the received audio channels:

The virtual LEDs in this view shows the status of the received audio channels, according to this coding:

- Grey: No audio present
- Transparent: Audio channel is present but audio sample contents indicate silence
- Green: Audio channel is present and contains audio samples with non-silence

- Yellow: Audio channel has an associated alarm
- Red: Audio channel is present but level is above peak threshold

The Flow X Configuration section contains settings related to the IP and UDP network layer:

Enable
: Check this box and press Apply to enable stream reception on this channel. If this box is unchecked, no video stream will be received, and all alarms related to this Video-IP In channel will be cleared.

Receive port
: UDP port to listen on. This parameter is used for both unicast and multicast reception.

Join multicast
: Whether to join a multicast stream, or only receive unicast traffic addressed to the device. If checked, the IP multicast group address configured in the text field will be received instead of unicast traffic.

Source interface
: Specify which Ethernet interface the incoming IP stream should be received on.

The Flow X Status section gives more details about the received RTP stream:

Alarm status
: Shows the alarm status of this specific IP flow. This only applies to flow A, and does not reflect the top level alarm status of the Video-IP In channel. When using SIPS/SMPTE 2022-7, the multiple flows that are received will have their own flow alarm status. If not green, indicated problems with reception on the specific IP flow.

Last RTP SSRC
: The RTP SSRC value last received on this IP flow.

RTP sequence errors
: The number of RTP sequence errors on this IP flow. Sequence errors may be caused by lost packets or packets received out of order. When receiving a healthy IP stream, this counter should be constant.

Total Ethernet rate
: The total Ethernet bitrate of the received IP flow, including all network headers.

Payload rate
: The payload bitrate of the received IP flow, excluding network headers. For the Video-IP Input channel, this is the actual video sample data rate.

8.6.4.1.2 Video-IP In - Alarms

The Alarms tab lets the user configure specific filters and severity levels for the alarms associated with the Video-IP Input channel. Refer to **8.6.2.2** for an in-depth general explanation of alarm configuration of the device.

8.6.4.1.3 Video-IP In - IP

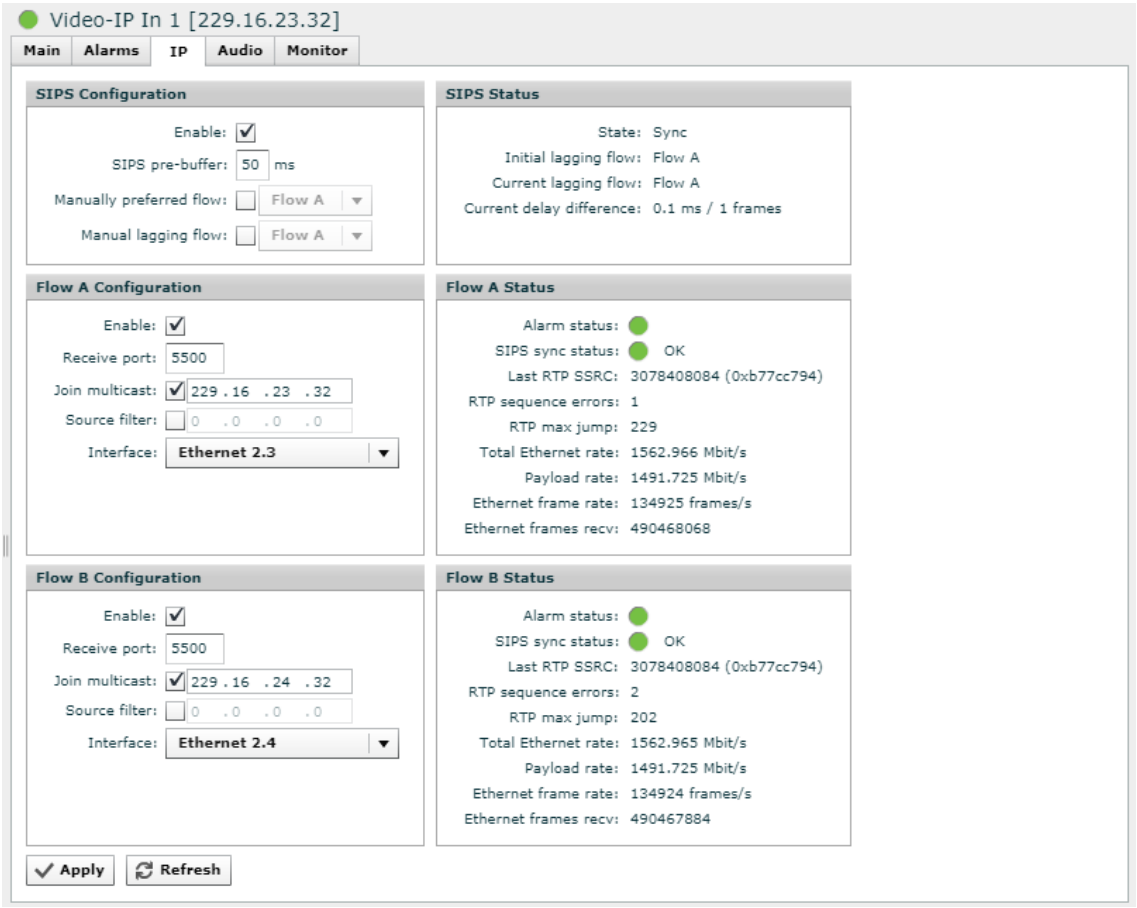


Figure 8.97 IP tab for a Video-IP input channel

The Video-IP input IP tab is shown in figure 8.97. Advanced configuration of the IP reception can be done here.

The SIPS Configuration section contains settings related to the video stream:

Enable
: Use Seamless IP Protection Switching for stream reception. Enabling this function will allow simultaneous reception of two redundant and RTP identical IP streams, and seamless merging of those for improved robustness against packet loss. The two received streams must comply to SMPTE 2022-7. If this function is disabled, only Flow A can be used for data reception.

Note: Note that the specific Enable parameter must be selected for both Flow A and Flow B for the seamless flow merge to be performed.

SIPS pre-buffer
: The maximum anticipated network delay difference between the received redundant IP flows.

Manually preferred flow
: If a specific IP flow should be preferred over the other, that flow can be selected here. This setting will influence the behavior of the receiver in the case where non-identical flows are received. If the setting is left disabled, the flow that has been longest present will decide which other flows are merged, namely the flows that are identical to the one present for the longest time.

Manual lagging flow
: If the IP flow that will have the highest network delay is deterministically known beforehand, that flow can be selected as the lagging flow manually with this option. This will minimize the receive buffer startup latency if not both flows are present when starting IP reception.

The SIPS Status section contains status related to the SIPS redundancy controller:

State
: The state of the SIPS controller.

Initial lagging flow
: The IP flow that was found to be lagging at initial receiver startup.

Current lagging flow
: The IP flow that is currently found to be lagging the most behind.

Current delay difference
: The currently measured differential latency between the leading and lagging IP flow.

The Flow A/B Configuration section contains settings related to the IP and UDP network layer:

Enable
: Check this box and press Apply to enable stream reception on this channel. If this box is unchecked, no video stream will be received, and all alarms related to this Video-IP In channel will be cleared.

Receive port
: UDP port to listen on. This parameter is used for both unicast and multicast reception.

Join multicast
: Whether to join a multicast stream, or only receive unicast traffic addressed to the device. If checked, the IP multicast group address configured in the text field will be received instead of unicast traffic.

Source filter
: When using multicast, whether to filter data coming from a specific IP source. This parameter must be used when receiving a stream on a Source Specific Multicast address, in the 232.x.x.x range.

Note: For the network to be able to do source specific multicast filtering, to e.g. reduce Ethernet link usage by doing IGMP snooping, IGMPv3 must be supported and running on the network.

Source interface
: Specify which Ethernet interface the incoming IP stream should be received on.

The Flow A/B Status section gives more details about the received RTP stream:

Alarm status
: Shows the alarm status of this specific IP flow. This only applies to the specific IP flow (A/B), and does not reflect the top level alarm status of the Video-IP In channel. When using SIPS/SMPTE 2022-7, the multiple flows that are received have their own flow alarm status. If not green, indicates problems with reception on the specific IP flow.

Last RTP SSRC
: The RTP SSRC value last received on this IP flow.

RTP sequence errors
: The number of RTP sequence errors on this IP flow. Sequence errors may be caused by lost packets or packets received out of order. When receiving a healthy IP stream, this counter should be constant.

Ethernet frames recv
: Total amount of Ethernet frames/packets received on this specific flow.

Total Ethernet rate
: The total Ethernet bitrate of the received IP flow, including all network headers.

Payload rate
: The payload bitrate of the received IP flow, excluding network headers. For the Video-IP Input channel, this is the actual video sample data rate.

8.6.4.1.4 Video-IP In - Audio

The Video-IP input Audio tab is shown in figure 8.98. Here basic audio meters showing the sample peak level for each audio channel in the received stream are shown.

At the top of the meters, the maximum sample peak level is indicated with a text label. A red overload indicator is also present at the top of the meter, to indicate that 0 dBFS has been reached. Both sample peak level and the overload indicator are sticky, and to reset them press the Reset Max button below the meters.

8.6.4.1.5 Video-IP In - Monitor

The Video-IP input Monitor tab allows the user to configure templates for alarm monitoring of video and audio. See Section 8.9.2.3 for an explanation of the functionality.

Note that this functionality only applies to SMPTE 2022-6 IP streams, and requires a special licence key.

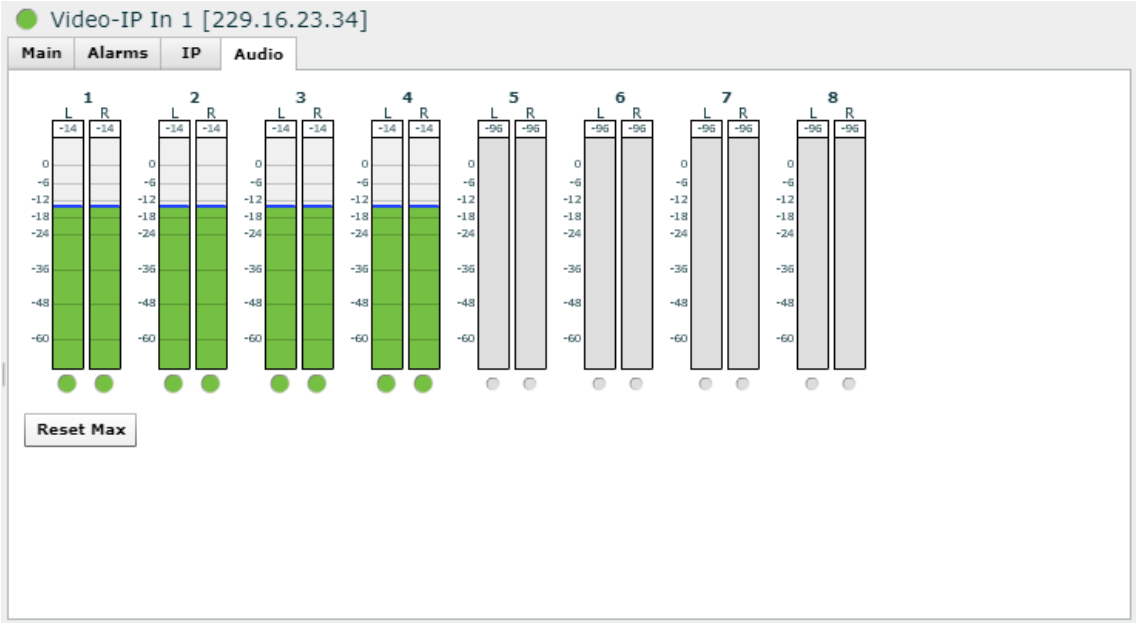


Figure 8.98 Audio tab for a Video-IP In channel

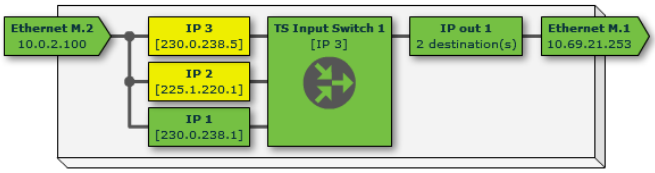


Figure 8.99 Ts Input switch data flow

8.7 Transforms

8.7.1 Input Switch

Input switch forwards data from a selected input to the output as presented in Figure 8.99. The input is selected from a set of connected inputs either by automatic logic or manually by a user. When operating in the automatic mode, switch selects the highest priority input matching the predefined conditions.

Input switch will generate an alarm notifying that a switch has been made and a new input has been selected. Another alarm is persistent and is raised when the switch cannot find a valid input matching user requirements. It is cleared when such input is found. Also, there is an alarm raised if a configurable number of inputs fall are no longer considered valid.

8.7.1.1 General settings

Input switch configuration and status is presented in three windows ordered by functional aspects. The *Input Switch Configuration* window provides a basic control over input switch.

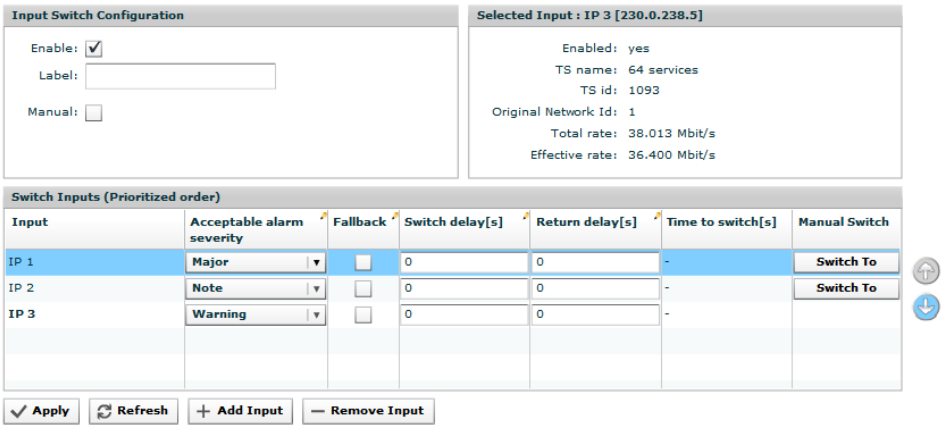


Figure 8.100 TS Input switch configuration

Label
: Custom user label.

Enable
: User can enable or disable the input switch logic and data transmission.

Manual
: If checked, only manual switching between inputs is possible.

Minimum valid inputs
: An alarm will be raised if the number of invalid inputs exceed this limit.

The *Selected Input* window present a short summary of the currently selected input.

Switch inputs are listed in the *Switch Inputs* table (see Figure 8.100) by order of priority. The first input on the list has the highest priority and the last input on the list has the lowest priority. Two inputs cannot have the same priority. Each input is described by a set of properties displayed in the input row. The properties affect the switch logic when switch operates in the automatic mode described below.

8.7.1.2 Add/Remove Input

To add an input to input switch, press "Add Input" button. The input is added at the bottom of the input list taking the lowest priority. The priority of the input can be changed by selecting the input in the table and pressing the up or down arrow located to the right of the table. The input is set to the selected priority after pressing the "Apply" button.

To remove an input, first select the input in the *Switch Inputs* table by pressing any field of the input row. The input is immediately removed after pressing the "Remove Input" button. When removing the currently selected input, switch will select a new input based on the automatic switch logic.

8.7.1.3 Automatic Mode

An input is described by a status which is either “valid” or “invalid”. It is consider to be “valid” if its alarm severity level is lower or equal to the selected “Acceptable alarm severity” level.

Considered the input priority list and the input status, input switch selects the input based on the following rules:

1. If the selected input becomes invalid wait the “Switch delay” seconds and select a valid input with the highest priority. The following two exceptions apply:
   - If there is no valid input on the switch, do not switch and raise the “Unable to switch” alarm.
   - If the selected input becomes valid within the “Switch delay” seconds do not switch.
2. If an input with the higher priority becomes valid and has the “Fallback” property set, select this input after the “Return delay” seconds. If the input becomes invalid within the “Return delay” seconds do not switch.
3. If the selected input has been deleted, select a valid input with the highest priority. If there is no valid input on the switch, select the input with the highest priority and rise the “Unable to switch” alarm.

A user can select an input manually by pressing the “Switch To” button in the automatic mode. However, after the switch operation is executed, input switch re-evaluates the selected input with respect to the presented rules and if a better input is found it switches to that input. For example, when switching to an invalid input while there is a valid input on switch results in the immediate switch to the valid input.

8.7.1.4 Manual Mode

In this mode the automatic switch logic is disabled and a user selects an input by clicking on the “Switch To” button in the “Manual Switch” column. The input is selected immediately after pressing the button. The input choice is recorded and preserved during a system reboot.

8.7.2 Descrambler

The descrambler module will descramble a BISS-1 scrambled signal using the DVB-CSA algorithm and generate a new Transport Stream. The Virtuoso supports multiple logical descramblers in a single unit. Creating extra descramblers are done by simply clicking Add Descrambler on the Transforms Overview page.

Connecting the output of the descrambler to another element is done by navigating the element you would like to connect, and select the descrambler module as the source for that element.

The descrambler page shows descrambler status summary, settings and a status information window. The descrambler status summary figure shows how the descrambler is inter-connected in the system. Clicking an item will take you to it’s own page. The status information box includes information about the generated Transport Stream. For each descrambler it is also possible to inspect the descrambled stream by clicking on Output TS in the navigator pane to the left.

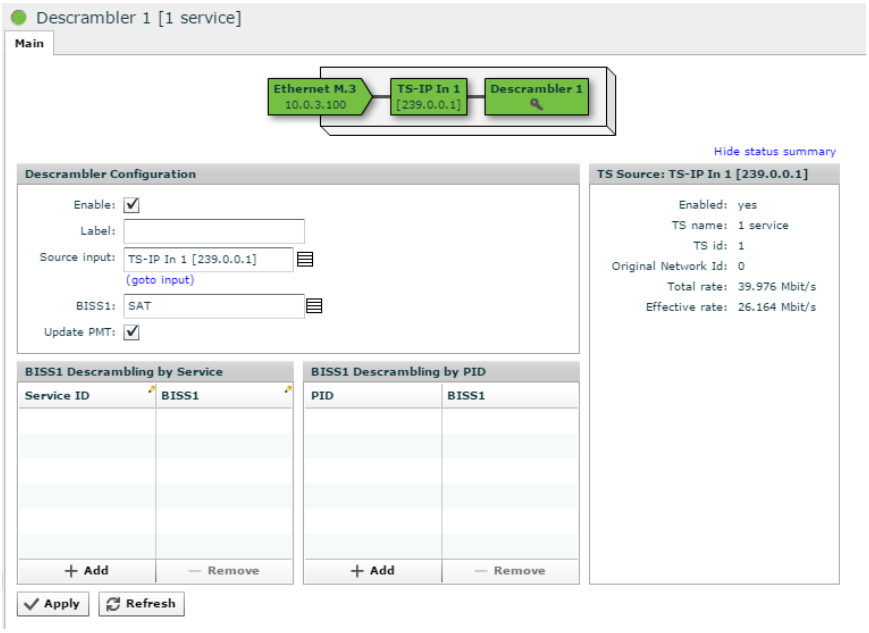


Figure 8.101 TS Descrambler

8.7.2.1 Settings

Enable
: When enabled the descrambler will generate a new transport stream. This will happen even if selecting No Descrambling under the BISS1 option.

Label
: Used configurable label for each descrambler module.

Source input
: Select which stream to descramble.

BISS1
: Select which BISS1 session word to use for descrambling. It is possible to have multiple session words defined on the unit, and multiple descramblers may use the same session word. Defining new session words is done by clicking on the BISS1 field, and then clicking the Set to new Session Word button.

Update PMT
: If checked the descrambler will remove BISS-1 scrambling descriptors from the PMT.

BISS1 Descrambling by service
: If different services are scrambled with different keys, each service can be assigned a different key here.

BISS1 Descrambling by PID
: If different PIDs are scrambled with different keys, each PID can be assigned a different key here.

8.7.3 Crypto Module

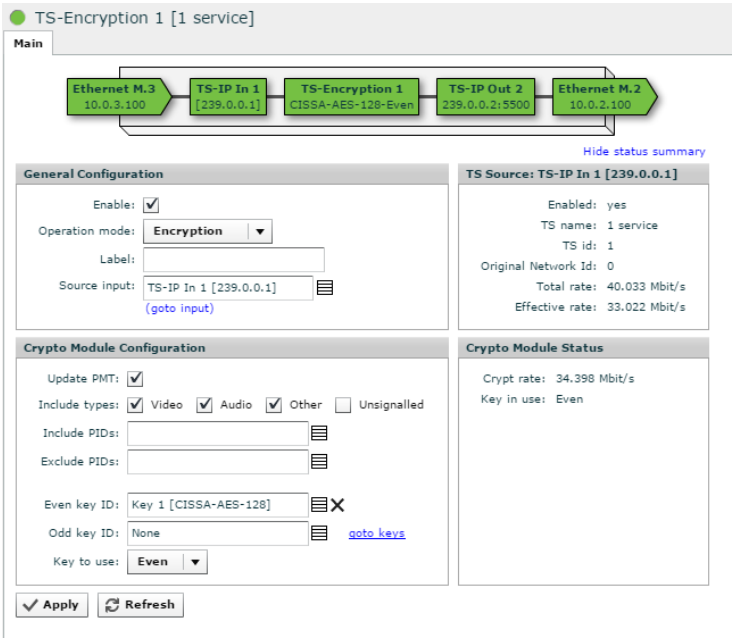


Figure 8.102 Cryptmodule

The cryptomodule will encrypt or decrypt transport stream using the DVB-CISSA algorithm. The Virtuoso supports multiple modules in a single unit. Creating extra modules are done by simply clicking Add CryptoModule on the Transforms Overview page.

Connecting the output of the module to another element is done by navigating the element you would like to connect, and select the cryptomodule as the source for that element.

For each module it is also possible to inspect result of the process by clicking on Output TS in the navigator pane to the left.

8.7.3.1 General configuration

Enable
: Check this box to enable the transport stream to flow through the module.

Operation mode

- Transparent: No processing is performed
- Encryption: The transport stream is encrypted
- Decryption: The transport stream is decrypted

Label
: Give the module a label to easily identify it in the user interface.

Source input
: Select the source of the module.

8.7.3.2 Crypto Module Configuration

Update PMT
: Check this box if the PMT shall be updated with new information about which PIDs are scrambled.

Include types
: Check the box of each type of content that shall be encrypted.

Include PIDS
: Option to manually specify which PIDs to process.

Exclude PIDs
: Option to manually specify PIDs that shall not be processed.

Even/Odd key ID
: Select which key shall be used from the drop down list. To add new keys go to the Encryption Keys page under Device Info.

Key to use
: Select if encryption shall be done with the Even or Odd key. For decryption the odd/even key is automatically selected.

8.7.3.3 Crypto Module Status

Crypt rate
: Shows the current bitrate of the encrypted/decrypted part of the transport stream.

Key in use
: Shows if even or odd key is in use.

8.8 Encoder/Decoder

The Encoder/Decoder page contains all information and settings of the present encoders and decoders.

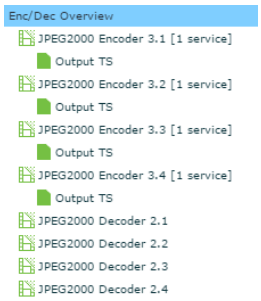


Figure 8.103 Codec page navigator bar for the Virtuoso.

The navigation list to the left shown in 8.103, lets the user select which encoder or decoder to view, or select Encoder/Decoder Overview to view a summary of all the inputs to the device. In addition the list also includes the input switchers and their corresponding inputs, if configured.

The labeling of the encoders and decoders is a combination of the user defined name of the input and the physical number of the respective encoder or decoder.

8.8.1 Encoder/Decoder Overview

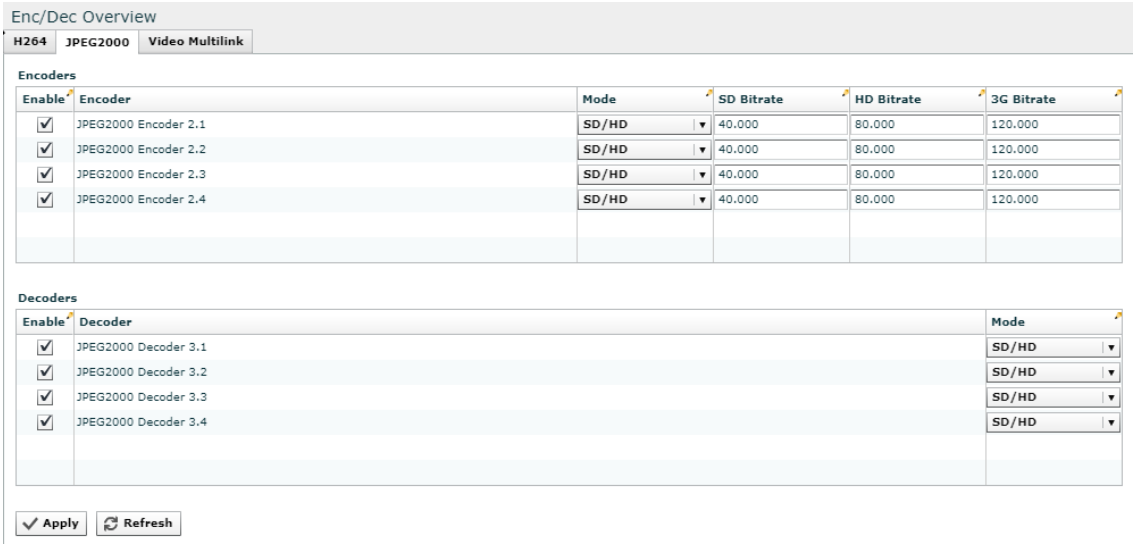


Figure 8.104 Encoder/Decoder overview page for the Virtuoso, showing all interfaces and their current status.

The Encoder/Decoder Overview page shows a graphical view of all the current encoders and decoders on the unit, as shown in figure 8.104.

The encoder/decoder page contains all the information and settings that are related to the encoder/decoder on the device, such as setting encoder/decoder configurations.

8.8.2 JPEG2000 Encoder

When a specific encoder or decoder is selected a page with information about that input is displayed. The top part of the page is common for all sub pages and shows the name and the current alarm status of the encoder.

Figure 8.105 JPEG2000 Encoder header

Holding the mouse cursor over the alarm status indicator brings up a tool tip displaying up to 30 of the current alarms (if any) on this particular input.

Beneath the name of the encoder is a tab navigator containing different sub pages with information about the selected encoder. The choices are:

Main
: This page shows a summary of the encoder configuration, including input audio streams and outputs.

Alarms
: This page lets the user view the status of all alarms on the encoder, and override the severity of these alarms.

ANC Config
: This page lets the user view the ANC settings of the encoder.

TS Config
: This page lets the user view the TS settings of the encoder, including PID settings.

Advanced
: This page lets the user view advanced settings of the encoder

In all sub-pages for a selected encoder a list of current alarms for that input is shown. The list is identical to the list displayed in the Current Status view, described in **Section 8.3.1**.

8.8.2.1 Main

Figure 8.106 Main

The Main page displays a block diagram ,and basic information of the encoder divided different sections

Looking at the input exampled in figure 8.106 a block diagram representation of the current decoder is given to provide a simple overview.

8.8.2.1.1 General Settings

This contains the configuration parameters which are common for all encoders:

Enable
: This shows whether the encoder is currently enabled. The encoder is enabled or disabled by clicking the check box and then Apply.

Mode

- SD: Only encodes SD formats.
- SD/HD: SD option, plus HD and 3G broadcast formats.
- SD/HD + Film: SD/HD option, plus film formats (2k, psf, 24p),

Label
: This is the user defined name of the encoder, which can be changed by typing a new label and hitting Apply. It is only used in the WEB GUI to identify the encoder.

Source
: Select the video source of the Encoder. Same source can be shared by multiple encoders.

TS bit rate (SD)
: This shows the SD bit rate used by the encoder in Mbit/s.

TS bit rate (HD)
: This shows the HD bit rate used by the encoder in Mbit/s.

TS bit rate (3G)
: This shows the 3G bit rate used by the encoder in Mbit/s.

8.8.2.1.2 Audio Stream

This shows a list of all the audio streams that are present on the selected encoder. Basic configuration of an audio stream can be performed directly in this section.

The list has 3 columns:

Enable
: Check to enable the current audio stream is enabled

PID
: Select which PID the audio stream will be assigned in the TS.

Bit Depth
: Select if audio should be transported with 20 or 24 bits per audio sample.

8.8.2.1.3 Encoder Status

Encoding
: Shows if encoder is current encoding.

Encoder state
: Shows the current state of the encoder.

Encoded frames
: Numbers of total encoded frames.

Video format
: Shows current format being encoded.

Framestore delay
: Shows current delay in the internal framestore (in ms).

Max compressed bitrate
: Shows maximum compressed bitrate. Value is calculated based on Video format, TS bitrate, audio and ancillary data settings.

8.8.2.1.4 Thumbnail

Check the Enable box to generate thumbnails of the video signal being encoded.

8.8.2.1.5 Destinations

Consist of a list of the outputs for the encoder. IP Destinations can be added or removed using the respective buttons.

8.8.2.2 VBI/ANC Config

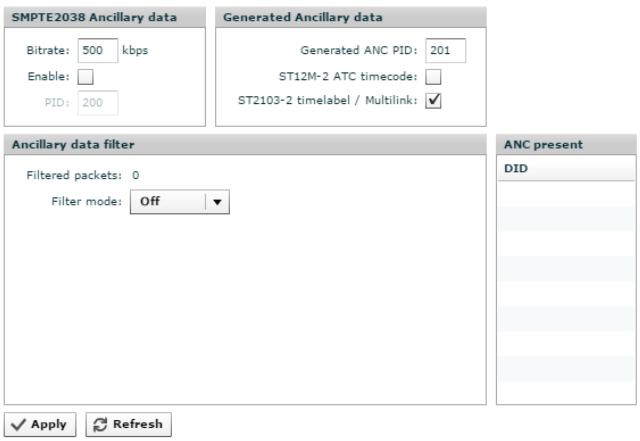


Figure 8.107 VBI/ANC Configuration

8.8.2.2.1 SMPTE 2038 Ancillary data

Bitrate
: Specify how much of the Transport Stream bitrate that should be allocated for Ancillary Data.

Enable
: Enable SMPTE 2038 Ancillary data transmission.

PID
: Specify which PID SMPTE 2038 should have.

8.8.2.2.2 Generated Ancillary data

Generated ANC PID
: Specify which PID the generated ancillary data should have.

ST12M-2 ATC timecode
: Inserts a ATC VITC timecode in the stream.

ST2102-2 timelabel / Multilink
: Inserts a timelabel used to synchronize multiple channels in a Multilink setup.

8.8.2.2.3 Ancillary data filter

To filter out Ancillary data packets, a filter can be applied. Select Include mode to only allow packets with the specified DID values, or select Exclude to filter out all packets with the specified DID values.

8.8.2.2.4 Anc present

Shows a list of the ancillary packets detected before the filter is applied.

8.8.2.3 TS Config

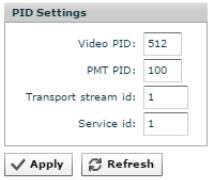


Figure 8.108 TS Configuration

8.8.2.3.1 PID Settings

Video PID
: Specify the PID for the video stream.

PMT PID
: Specify which PID the PMT table should have.

Transport stream id: Specify which transport stream ID that should be used.

Service id: Specify which service ID should be signalled in the SDT.

8.8.3 JPEG2000 Decoder

When a specific decoder or decoder is selected a page with information about that input is displayed. The top part of the page is common for all sub pages and shows the name and the current alarm status of the decoder.

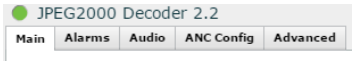


Figure 8.109 JPEG2000 Decoder header

Holding the mouse cursor over the alarm status indicator brings up a tool tip displaying up to 30 of the current alarms (if any) on this particular input.

Beneath the name of the input is a tab navigator containing different sub pages with information about the selected input. The choices are:

Main
: This page shows a summary of the decoder configuration, including status, thumbnail, input and outputs.

Alarms
: This page lets the user view the status of all alarms on the decoder, and override the severity of these alarms.

Audio
: This page lets the user view the audio settings of the decoder.

ANC Config
: This page lets the user view the ANC settings of the decoder.

Advanced
: This page lets the user view the advanced settings of the decoder.

In all sub-pages for a selected decoder a list of current alarms for that input is shown. The list is identical to the list displayed in the Current Status view, described in **Section 8.3.1**.

8.8.3.1 Main

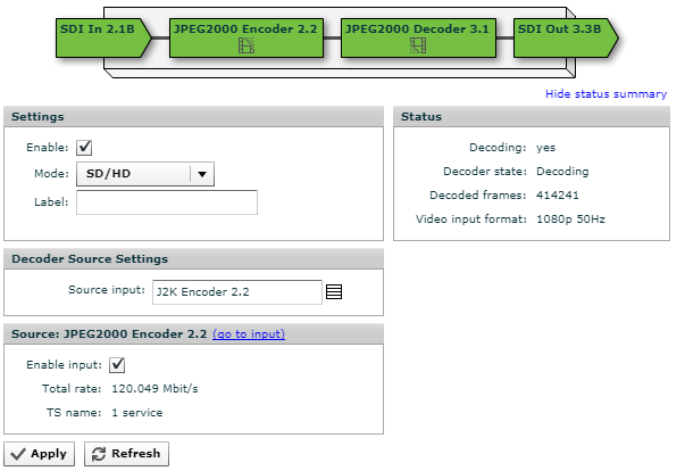


Figure 8.110 Main

The Main page displays a block diagram and basic information of the decoder divided in different sections.

8.8.3.1.1 Settings

Enable
: Enables the decoder.

Mode

- SD: Only decodes SD formats.
- SD/HD: SD option, plus HD and 3G broadcast formats.
- SD/HD + Film: SD/HD option, plus film formats (2k, psf, 24p),

Label
: This is the user defined name of the encoder. It is only used in the WEB GUI to identify the encoder.

Reference sync
: Check box to enable reference sync. Select correct refsync source, and a desired offset if required.

8.8.3.1.2 Decoder source settings

Source Input
: Select which ASI or IP Input that is the source to the decoder.

8.8.3.1.3 Status

Shows state of the decoder, current video format being decoded and number of frames decoded.

8.8.3.1.4 Thumbnail

Check the Enable box to generate thumbnails of the video signal being decoded, or the test signal if decoder is not decoding.

8.8.3.1.5 Source details

This box shows some information and settings for the currently selected source of the decoder.

8.8.3.2 Audio

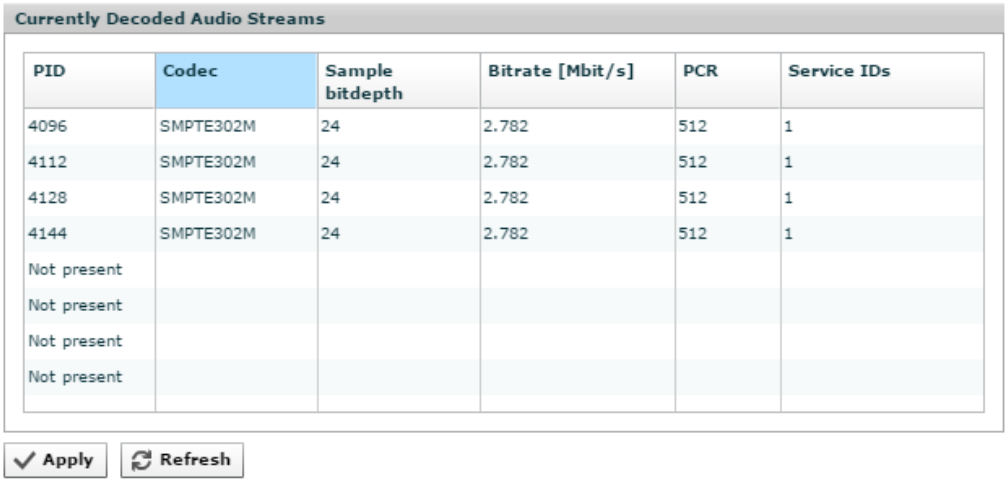


Figure 8.111 Audio Configuration

8.8.3.2.1 Currently Decoded Audio Streams

This is a list over the current decoded audio streams, including some extra information about PID, Audio Codec, which services reference the audio, TS bitrate and the referenced PCR.

8.8.3.3 VBI/ANC Config

8.8.3.3.1 SMPTE2038 Generic ANC

- Enable: Enable Ancillary data
- Current PID: Shows the current PIDs selected for SMPTE2038 Anc data (0 if no PID is found)

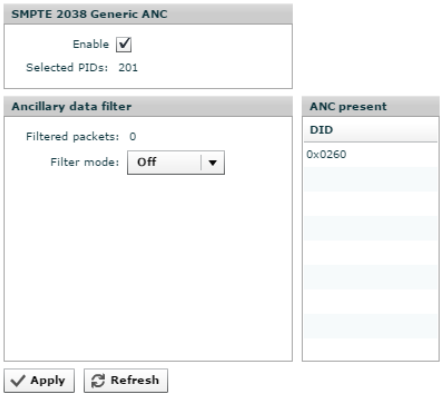


Figure 8.112 ANC Configuration

8.8.3.3.2 Ancillary data filter

To filter out Ancillary data packets, a filter can be applied. Select Include mode to only allow packets with the specified DID values, or select Exclude to filter out all packets with the specified DID values.

8.8.3.3.3 ANC present

Shows a list of the ancillary packets detected before the filter is applied.

8.8.4 TICO Encoder

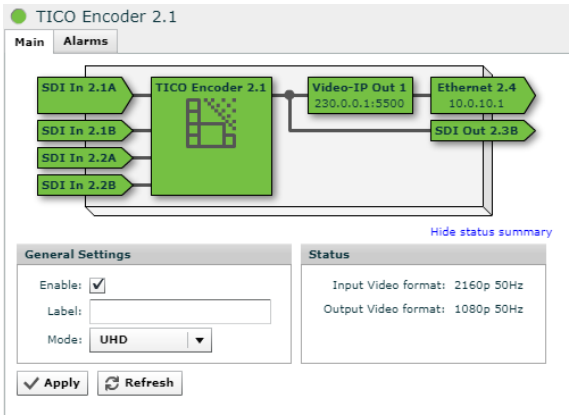


Figure 8.113 TICO Encoder

The TICO Encoder compresses a full-frame UHD picture with a factor of 1:4. The compressed codestream is mapped into the active picture region of a new HD/3G SDI stream. Both vertical and horizontal blanking (all ANC and Audio), is copied from the first SDI input, and mapped to the output. This ensures transparent Audio and Ancillary data transport. The resulting SDI (SDTI) output can both be sent out on SDI and over IP with the Video over IP Output element.

Mode
: Select if the encoder should operate in “UHD”, or “UHD+Film mode”. The ability to support Film-formats depends on loaded licences on the unit.

Input Video format
: Shows the current video format that is detected on the input (UHD format)

Output Video format
: Shows the video format of the compressed data stream on the output (HD/3G format)

8.8.5 TICO Decoder

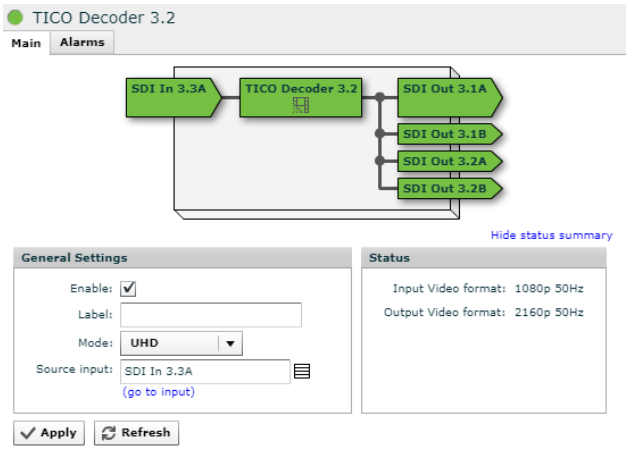


Figure 8.114 TICO Decoder

The TICO Decoder will extract the codestream from the active picture on the input. It will then decompress it into a full raster picture. All the SDI outputs will copy both the horizontal, and vertical blanking from the input to the output. This ensures tranparent Audio and Ancillary data transport.

Mode
: Select if the encoder should operate in “UHD”, or “UHD+Film mode”. The ability to support Film-formats depends on loaded licences on the unit.

Source input
: Select which input where the decoder should get its compressed stream from.

Input Video format
: Shows the current video format of the compressed stream (HD/3G format)

Output Video format
: Shows the video format of the resulting decoded video (UHD format)

8.8.6 H.264/AVC Encoder

When a specific encoder or decoder is selected a page with information about that input is displayed. The top part of the page is common for all sub pages and shows the name and the current alarm status of the encoder.

Figure 8.115 H.264/AVC Encoder header

Holding the mouse cursor over the alarm status indicator brings up a tool tip displaying up to 30 of the current alarms (if any) on this particular input.

Beneath the name of the encoder is a tab navigator containing different sub pages with information about the selected encoder. The choices are:

Main
: This page shows a summary of the encoder configuration, including input audio streams and outputs.

Alarms
: This page lets the user view the status of all alarms on the encoder, and override the severity of these alarms.

Video
: This page lets the user view the video settings of the encoder.

Audio
: This page lets the user view the audio settings of the encoder.

VBI/ANC Config
: This page lets the user view the VBI settings of the encoder.

TS Config
: This page lets the user view the TS settings of the encoder, including PID settings.

Scrambling
: BISS1 scrambling configuration.

Capture
: Full frame capture of the SDI input to the encoder.

Advanced
: This page lets the user view advanced settings of the encoder

In all sub-pages for a selected encoder a list of current alarms for that input is shown. The list is identical to the list displayed in the Current Status view, described in **Section 8.3.1**.

8.8.6.1 Main

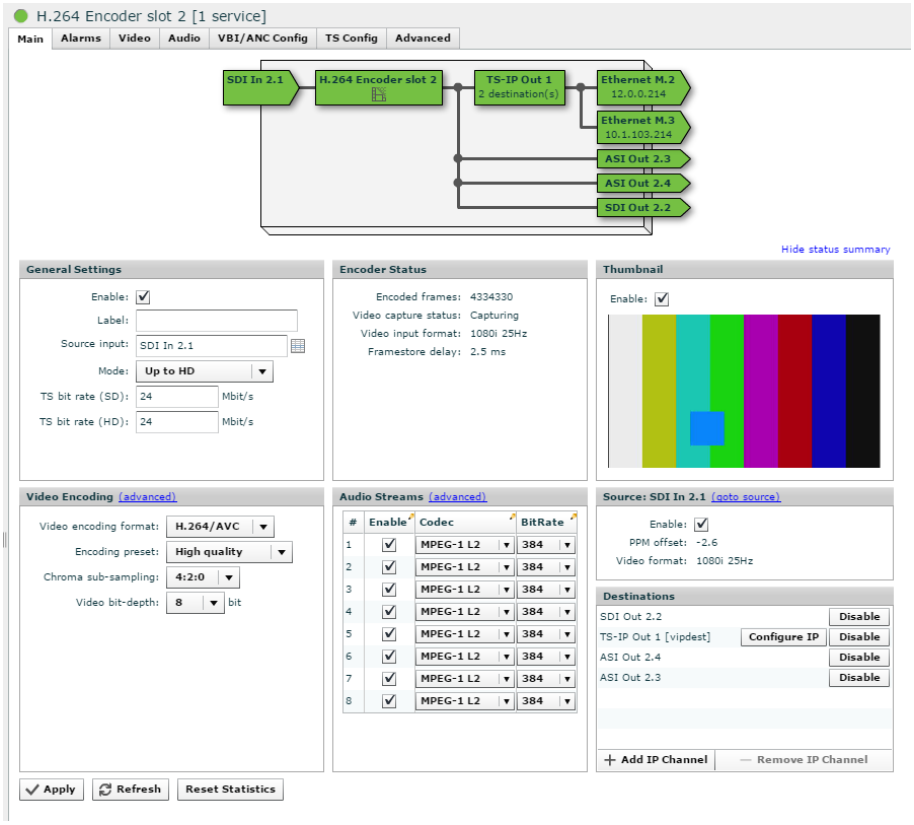


Figure 8.116 Main

The Main page displays a block diagram ,and basic information of the encoder divided different sections

Looking at the input exampled in figure 8.116 a block diagram representation of the current decoder is given to provide a simple overview.

8.8.6.1.1 General Settings

This contains the configuration parameters which are common for all encoders:

Enable
: This shows whether the encoder is currently enabled. The encoder is enabled or disabled by clicking the check box and then Apply.

Label
: This is the user defined name of the encoder, which can be changed by typing a new label and hitting Apply. It is only used in the WEB GUI to identify the encoder.

Mode
: To encode SD and HD signal, select mode Up to HD. When encoding 1080p50/59.94 3G-SDI

signal, two Encoder-cards are required. One of the cards need to be configured as Up to 3G, and the other card as 3G co-processor. The two cards needs to be positioned in Slots 1 and 2, or 3 and 4. In a 3G setup, connect SDI and ASI cables to the board configured with Up to 3G, as you would in HD. The 3G co-processor card does not require any cables connected to it.

TS bit rate (SD)
: This shows the SD bit rate used by the encoder in Mbit/s.

TS bit rate (HD)
: This shows the HD bit rate used by the encoder in Mbit/s.

8.8.6.1.2 Video Encoding

Video encoding format
: This shows the encoding format used by the encoder. The encoding format can be changed by selecting an option from the scroll down menu and then clicking Apply.

Encoding present
: This shows the encoding preset used by the encoder. The encoding preset can be changed by selecting an option from the scroll down menu and then clicking Apply.

Chroma sub-sampling
: This shows the chroma sub-sampling used the by encoder. The chroma sub-sampling can be changed by selecting an option from the scroll down menu and then clicking Apply.

Video bit-depth
: This shows the video bit-depth used by the encoder. The video bit-depth can be changed by selecting an option from the scroll down menu and then clicking Apply.

8.8.6.1.3 Audio Stream

This shows a list of all the audio streams that are present on the selected encoder. Basic configuration of an audio stream can be performed directly in this section.

The list has 3 columns:

Enable
: This shows whether the audio stream is currently enabled. The stream is enabled or disabled by clicking the check box and then Apply.

Codec
: This shows the codec used by the audio stream. The codec can be changed for the stream by selecting an option from the scroll down menu and then clicking Apply.

Bitrate
: This shows the bit rate used by the audio stream. The bit rate can be changed for the stream by selecting an option from the scroll down menu and then clicking Apply.

8.8.6.1.4 Encoder Status

Encoded frames
: Numbers of total encoded frames.

Video capturing status
: Shows if the encoder is currently capturing information.

Video input format
: Shows current format of the encoder input.

8.8.6.1.5 Thumbnail

Check the Enable box to generate thumbnails of the video signal being encoded.

8.8.6.1.6 Destinations

Consist of a list of the outputs for the encoder. IP Destinations can be added or removed using the respective buttons.

8.8.6.2 Video

This tab consist of different sections as shown in figure **8.117**.

8.8.6.2.1 Main Settings

Video encoding format
: This shows the encoding format used by the encoder.

Encoding present
: This shows the encoding preset used by the encoder.

Chroma sub-sampling
: This shows the chroma sub-sampling used the by encoder

Video bit-depth
: This shows the video bit-depth used by the encoder.

TS bit rate (SD)
: Configure the overall Transport Stream bitrate for SD formats, in Mbit/s.

TS bit rate (HD)
: Configure the overall Transport Stream bitrate for HD formats, in Mbit/s.

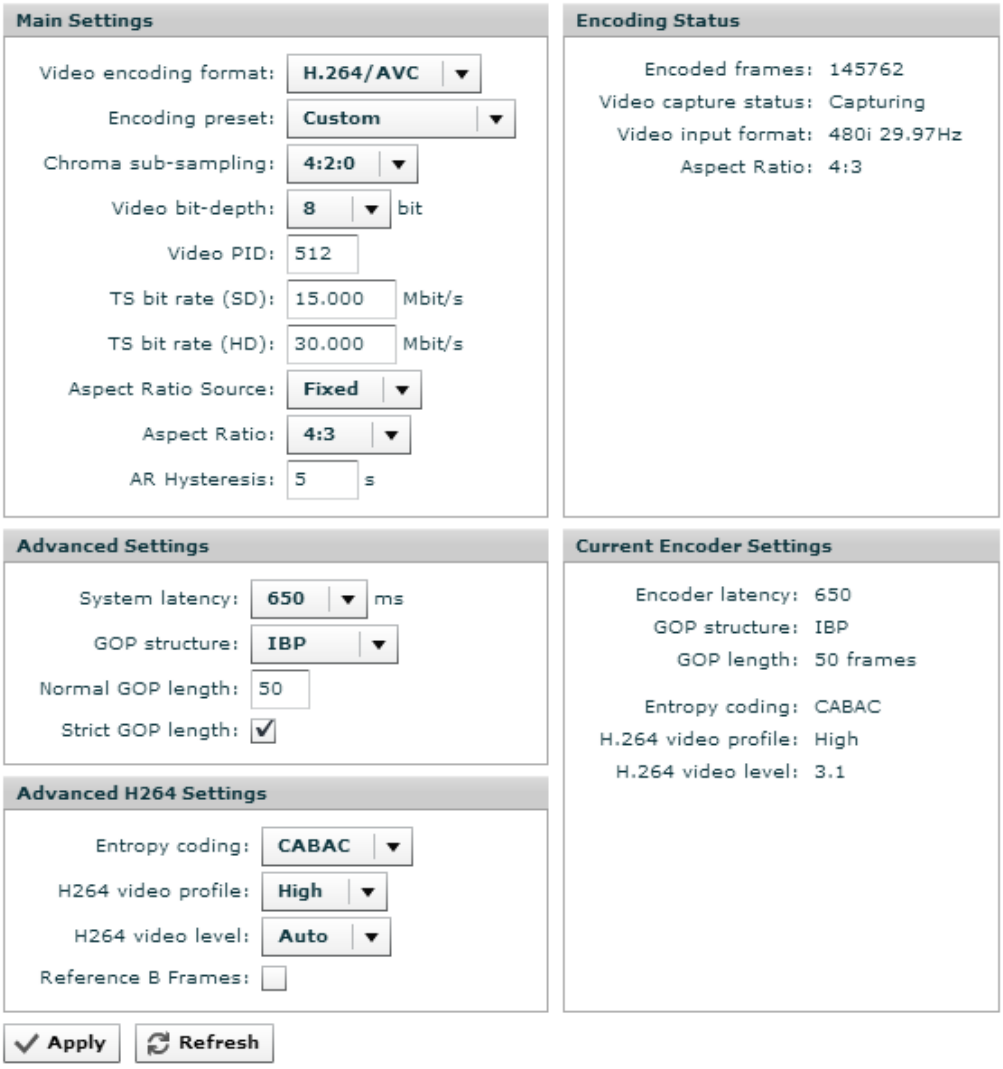


Figure 8.117 Video Configuration

8.8.6.2.2 Advanced Settings

This section is enabled when Encoding preset Custom is selected.

System latency
: This shows the system latency used by the encoder in miliseconds.

GOP structure
: Specify the desired GOP structure that will be used by the Encoder (if supported for the video format).

Normal GOP length
: Select the target GOP length used by the encoder. The actual GOP length may vary depending on Video content and scene changes.

Strict GOP length
: Check this box if the GOP length should never exceed the Normal GOP length.

8.8.6.2.3 Advanced H264/MPEG2 Settings

Advanced settings either for MPEG2, or H.264/AVC. Settings will change based on which codec is selected.

H264/MPEG2 video profile
: This shows the H264 video profile used by the encoder.

H264/MPEG2 video level
: This shows the H264 video level used by the encoder.

H264 Entropy encoding
: This shows the entropy encoding used by the encoder.

H264 Reference B Frames
: This shows whether the B frames are currently been referenced.

8.8.6.2.4 Encoding Status

Basic status information about the encoder

Encoded frames
: Numbers of total encoded frames.

Video capturing status
: Shows if the encoder is currently capturing information.

Video input format
: Shows current format of the encoder input.

8.8.6.2.5 Current Encoder Settings

Shows the current configuration used by the encoder.

8.8.6.3 Audio

Figure 8.118 Audio Configuration

This tab is consist of 5 sections as shown in figure 8.118.

The first field is Main Settings. This contains the audio configuration parameters of the selected encoders:

Enable
: Enable encoding for the selected audio stream.

Audio PID
: Configure the PID for the audio stream.

Source
: Select the source of the audio stream. The same source can be selected by several audio streams. If the source is not present in the SDI signal, silence will be encoded instead.

Codec
: This shows the encoding format used by encoder for the audio stream.

SMPTE302 bit depth
: Select between 16, 20 or 24 bits resolution. Selection only applicable when SMPTE302 coded is selected.

Bit rate
: Selection for the bit rate of the audio stream. Note, the bitrate is for the compressed audio, and does not include overhead like PES and TS headers.

Delay
: Specify delay for the audio channel in milliseconds. The delay is performed by adjusting the PTS in the transport stream. Some decoders will need to resync to take the delay into account.

Language Descriptor
: Specify the language descriptor that is used in the PMT table.

8.8.6.4 VBI/ANC Config

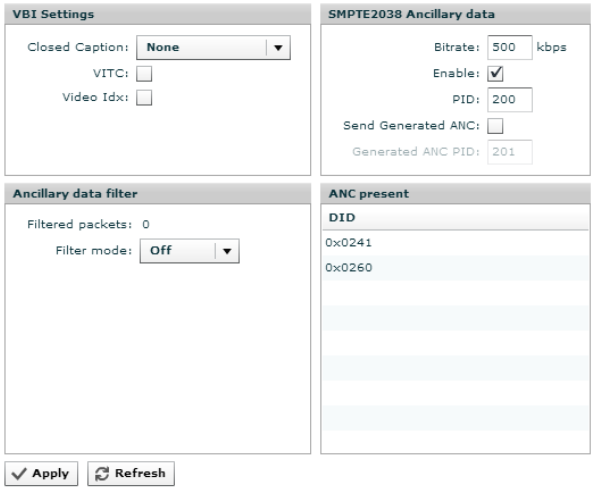


Figure 8.119 VBI/ANC Configuration

8.8.6.4.1 VBI Settings

Closed Caption
: Select the source for Closed Captioning.

VITC
: Enables processing of Vertical Interval Timecode (ST12M-1). (For ATC/ST12M-2 Timecode, use SMPTE2038 ancillary data).

Video Idx
: Enabled processing of Video Index with AFD information.

8.8.6.4.2 SMPTE 2038 Ancillary data

ANC Bitrate
: Specify how much of the Transport Stream bitrate that should be allocated for Anciallary Data.

Enable
: Enable SMPTE 2038 Ancillary data transmission.

PID
: Specify which PID SMPTE 2038 should have.

Send Generated ANC
: Enable SMPTE 2038 Ancillary data transmission of ancillary data generated by the SDI Input.

Generated ANC PID
: Specify which PID the generated ancillary data should have.

8.8.6.4.3 Ancillary data filter

To filter out Ancillary data packets, a filter can be applied. Select Include mode to only allow packets with the specified DID values, or select "Excludeto filter out all packets with the specified DID values.

8.8.6.4.4 Anc present

Shows a list of the ancillary packets detected before the filter is applied.

8.8.6.5 TS Config

8.8.6.5.1 PID Settings

Video PID
: Specify the PID for the video stream.

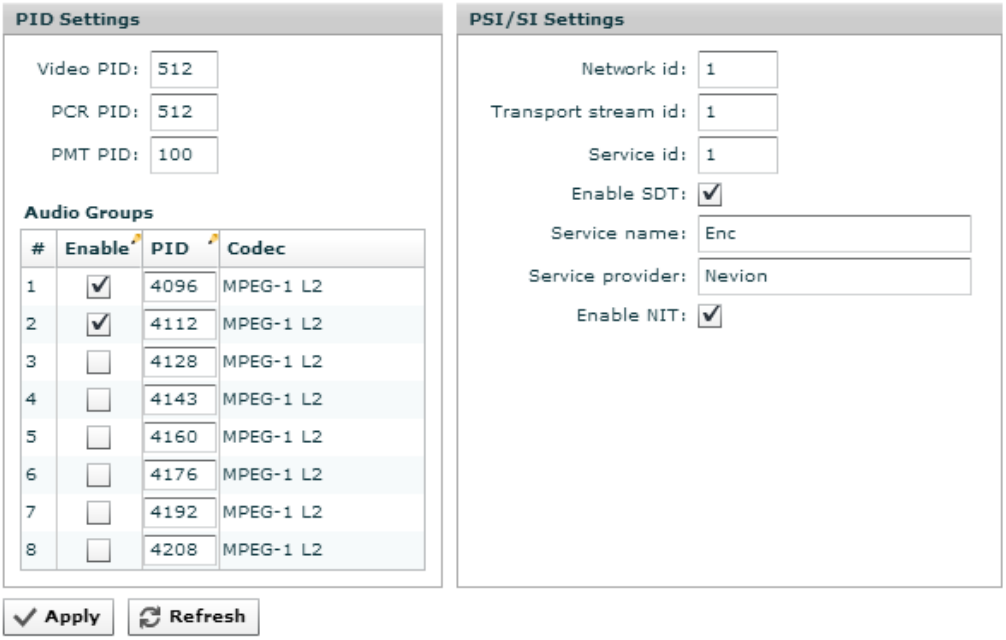


Figure 8.120 TS Configuration

PCR PID
: Specify the PID for the PCR. If different PID than video is selected, the PCR will be in it's own PID.

PMT PID
: Specify which PID the PMT table should have.

Audio Groups
: Select the PID for each audio stream.

8.8.6.5.2 PSI/SI Settings

This section allows the configuration and insertion of SDT and NIT packets according to PSI/SI specification.

Network ID
: Select the Network ID to be used.

Enable SDT
: Check this box to enable insertion of SDT packets

Service name
: Specify the service name used in the SDT packet.

Service provider
: Specify the service provider name used in the SDT packet.

Enable NIT
: Check this box to enable insertion of NIT packets.

8.8.6.6 Scrambling

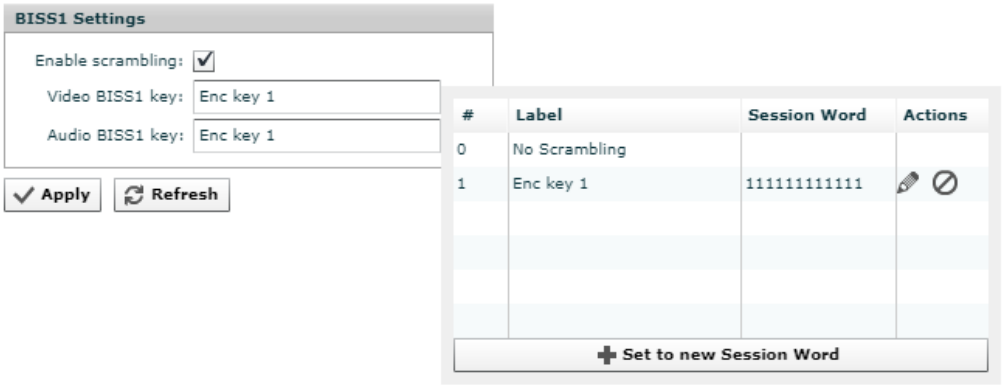


Figure 8.121 Scrambling Configuration

Enable
: Enable the scrambling by checking this box

Video BISS1 key
: Select which BISS1 key should be used to scramble the Video PID. Setting to No Scramble will disable the scrambling of the video. Press the Set to new Session Word to add a new BISS1 key.

Audio BISS1 key
: Same configuration as the video, but allows to use different BISS1 keys.

8.8.6.7 Capture

Captured image
: Shows the current captured image on the unit.

Capture button
: Press this button to capture a new image. The image will be ready for download in a few seconds.

Download button
: Press button to download the uncompress.yuv image from the unit. The image is in the format: 4:2:2 10 Bit, Big Endian, Packed with order UYVY. See 8.123 for how this is configured in Windows program YUView.

Figure 8.122 Capture Configuration

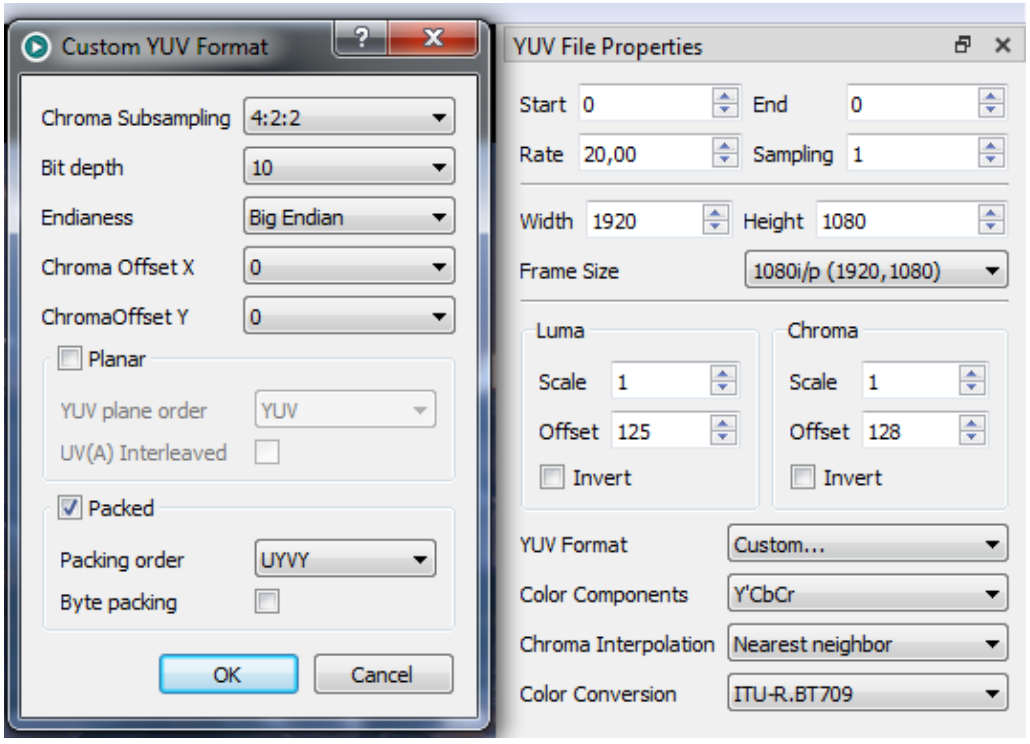


Figure 8.123 YUView Configuration

8.8.7 H.264/AVC Decoder

When a specific decoder or decoder is selected a page with information about that input is dis-

played. The top part of the page is common for all sub pages and shows the name and the current alarm status of the decoder.

Figure 8.124 H.264/AVC Decoder header

Holding the mouse cursor over the alarm status indicator brings up a tool tip displaying up to 30 of the current alarms (if any) on this particular input.

Beneath the name of the input is a tab navigator containing different sub pages with information about the selected input. The choices are:

Main
: This page shows a summary of the decoder configuration, including input audio streams and outputs.

Alarms
: This page lets the user view the status of all alarms on the decoder, and override the severity of these alarms.

Audio
: This page lets the user view the audio settings of the decoder.

VBI/ANC Config
: This page lets the user view the VBI settings of the decoder.

Advanced
: This page lets the user view the advanced settings of the decoder.

In all sub-pages for a selected decoder a list of current alarms for that input is shown. The list is identical to the list displayed in the Current Status view, described in **Section 8.3.1**.

8.8.7.1 Main

The Main page displays a block diagram and basic information of the decoder divided in different sections.

8.8.7.1.1 Settings

Enables the decoder, and allows selection between 100ms and 300ms latency mode. 300ms latency will provide higher picture quality.

3G Level B
: Output 1080p50/59.94 video as 3G-SDI Level B.

Use reference sync
: Check box to enable reference sync. Go to advanced settings by clicking the (Refsync config) link.

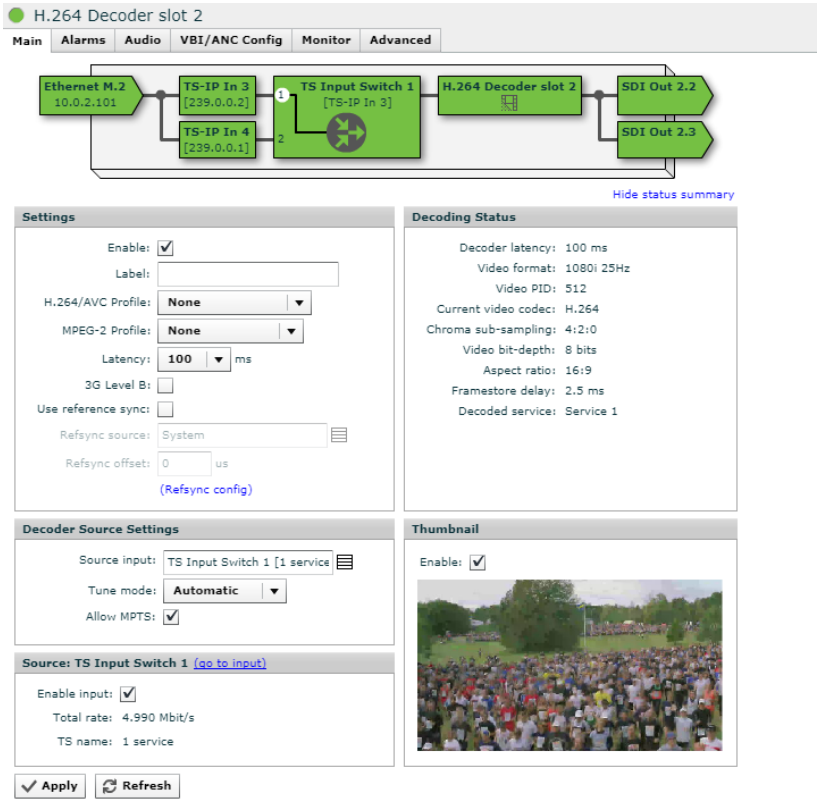


Figure 8.125 Main

8.8.7.1.2 Decoder source settings

Source Input
: Select which ASI or IP Input that is the source to the decoder.

8.8.7.1.3 Tune mode

8.8.7.1.4 Automatic

In automatic mode the decoder will automatically decoder the first service it finds. Check the Allow MPTS box if the decoder is allowed to decode a MPTS (Multiple Program Transport Stream) and always select the first service.

8.8.7.1.5 Service ID

In the Service ID mode to decode a specific service in a MPTS stream. Check the Auto failover box if the decoder shall switch to Automatic mode if the service is not found.

8.8.7.1.6 Manual

In the manual mode PCR, Video and Audio PIDs needs to be set manually. Make sure that both video and all the audio streams refer to the selected PCR. Check the box Unsignaled PIDs to allow decoding of PIDs that are not signaled in PMTs. When this box is checked, and the PIDs are no signaled, the codec types for the unsignaled pids needs to be specified.

8.8.7.1.7 Decoding status

Shows some information about the decoding of the current stream, including latency, video codec, chroma sub-sampling and video bit-depth.

8.8.7.1.8 Thumbnail

Check the Enable box to generate thumbnails of the video signal being decoded, or the test signal if decoder is not decoding.

8.8.7.1.9 Source details

This box shows some information and settings for the currently selected source of the decoder.

8.8.7.1.10 Destinations

Shows a list of the current destinations of the decoder. Example: SDI 2.2

8.8.7.2 Audio

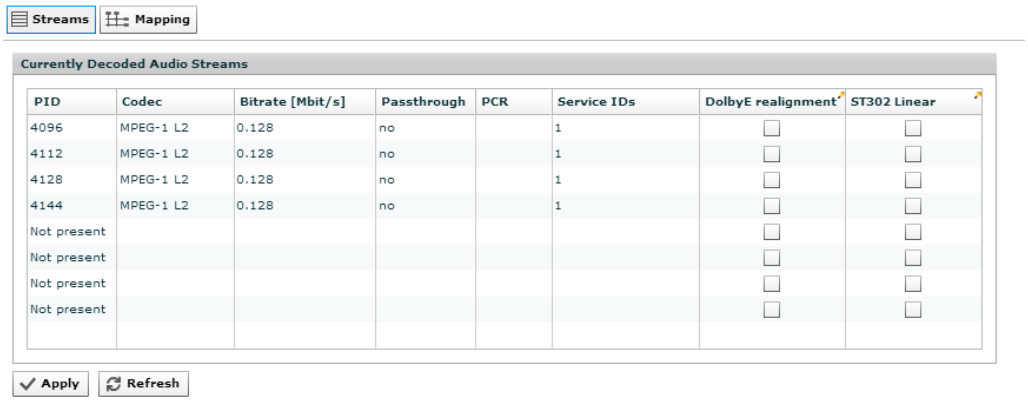


Figure 8.126 Audio Configuration

8.8.7.2.1 Currently Decoded Audio Streams

This is a list over the current decoded audio streams, including some extra information about PID, Audio Codec, which services reference the audio, TS bitrate and the referenced PCR. When in manual tune mode it is possible to manually configure the PID/codec of each stream.

DolbyE realignment
: Enable automatic re-alignment of DolbyE audio for the specific stream.

ST302 Linear
: Set the Linear PCM identification bit in the AES channel status information for ST302 streams. (Default is not set).

8.8.7.3 VBI/ANC Config

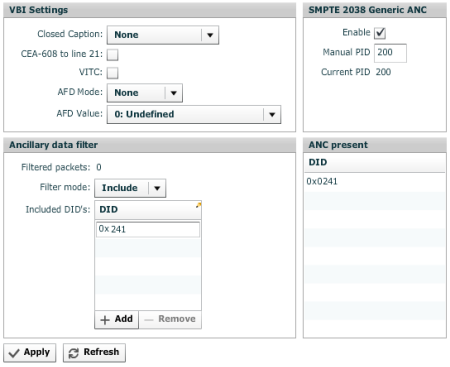


Figure 8.127 VBI/ANC Configuration

8.8.7.3.1 Vbi Settings

Closed Caption
: Select specification shall be used to insert the closed captions into VANC.

CEA-608 to line 21
: Check this box if CEA-608 shall be converted to Line 21 captioning for US-SD.

VITC
: Check this box to enable VITC insertion (ST12M-1).

AFD Mode

- None: No AFD insertion.
- Auto: Insert AFD if present in stream.
- Always: Always insert AFD. If AFD is not present in stream, use AFD Value.
- Override: Always insert AFD but override with AFD Value.

AFD Value
AFD value used in AFD Modes Always and Override.

8.8.7.3.2 SMPTE2038 Generic ANC

- Enable: Enable Ancillary data
- Manual PID: Specify which PID should be checked when in manual mode
- Current PID: Shows the current PID selected for SMPTE2038 Anc data (0 if no pid found)

8.8.7.3.3 Ancillary data filter

To filter out Ancillary data packets, a filter can be applied. Select Include mode to only allow packets with the specified DID values, or select Exclude to filter out all packets with the specified DID values.

8.8.7.3.4 ANC present

Shows a list of the ancillary packets detected before the filter is applied.

8.8.7.4 Encoders Alarms

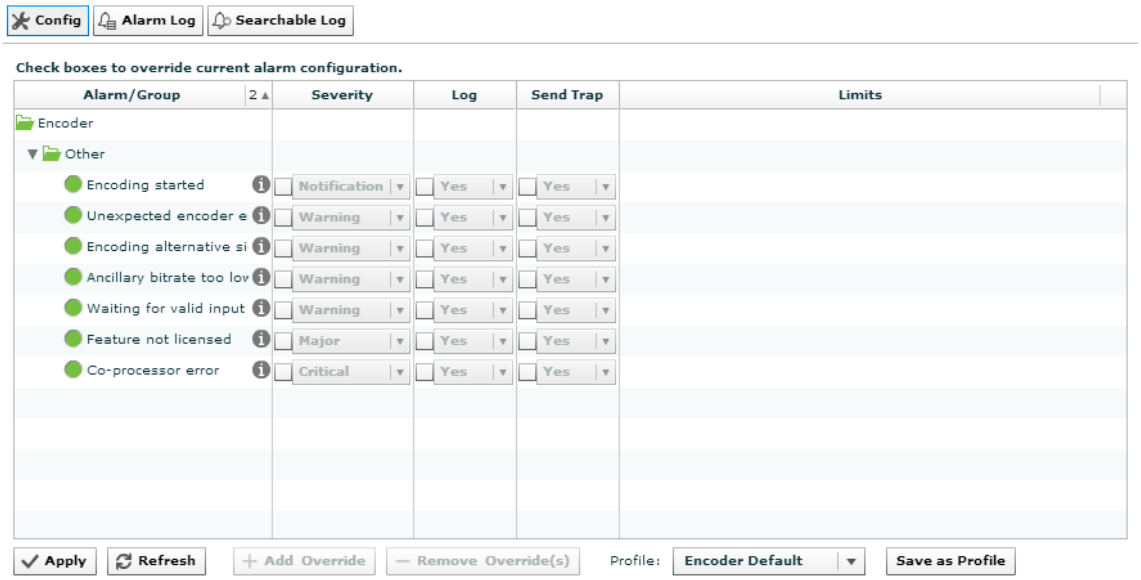


Figure 8.128 alarm configuration

The Alarms page lets the user configure and view the status of all alarms belonging to the selected. The page has two or three tabs at the top, depending on the type of. For Encoders, there are two tabs, Config and Alarm Log, which are present for all Encoders.

In figure 8.128 the Config page is shown. Note that the alarms are organised hierarchically and that only the branches in focus need to be expanded.

The alarm list is presented in a table with different columns, where the left most column shows the Alarm/Group which is where to navigate the alarm tree.

8.8.7.5 Decoders Alarms

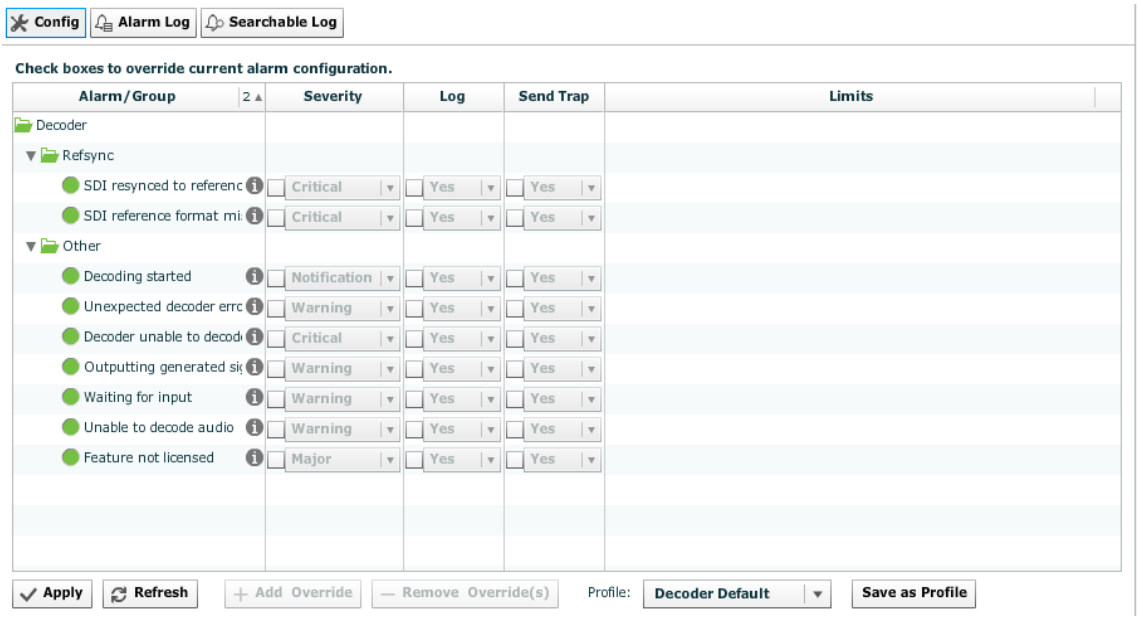


Figure 8.129 alarm configuration

The Alarms page lets the user configure and view the status of all alarms belonging to the selected. The page has two or three tabs at the top, depending on the type of. For Decoders, there are two tabs, Config and Alarm Log, which are present for all Decoders.

In figure 8.129 the Config page is shown. Note that the alarms are organised hierarchically and that only the branches in focus need to be expanded.

The alarm list is presented in a table with different columns, where the left most column shows the Alarm/Group which is where to navigate the alarm tree.

8.9 Common video pages

8.9.1 Video Advanced tab

The advanced configuration page is available on some Encoders, and either the Decoder or the SDI output connected to the decoder.

The Signal Loss Settings section contains configuration of what should happen in the event of an input signal sync loss:

Signal loss mode
: Specifies what should happen to the output stream in the event of source signal loss. Choosing either Test image or Freeze frame will ensure that there is a continuous valid output stream, no matter what happens to the input signal.

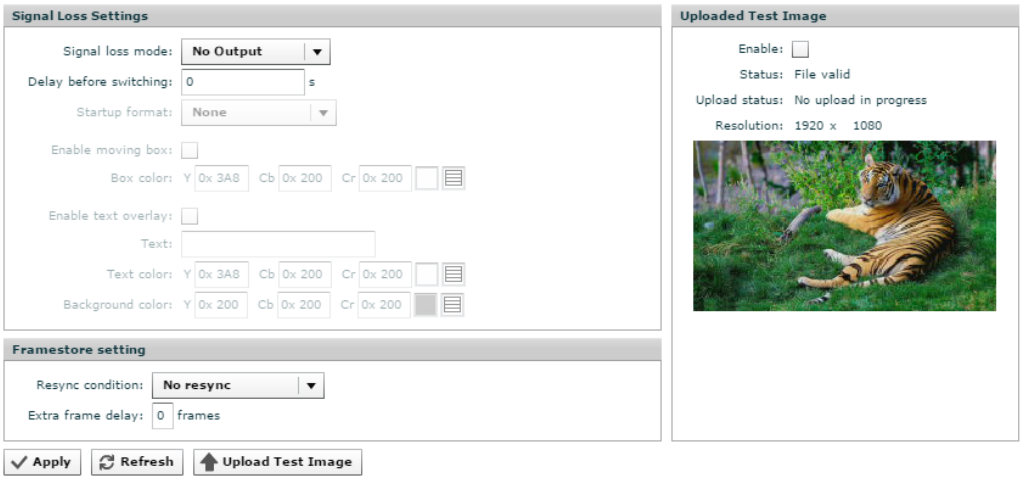


Figure 8.130 Advanced Configuration

Delay before switching
: When using Test image as the Signal loss mode, this delay specifies how many seconds the output should stay in Freeze frame mode before switching to the test image output. Leaving this at 0 s means that the test image is used immediately if input sync loss occurs. Specifying a value > 0 s so that the output first goes into the freeze frame mode, may give a gentler handling of e.g. spurious input sync losses, as a freeze frame in general will be less visible for a viewer than a predefined test image would be.

Startup format
: If enabling the channel without having a signal available on the selected input source, this parameter gives the video format for the internally generated test image that will then be transmitted. If no format is specified, there will be no output signal before some video format has been available on the selected input.

Enable moving box
: This parameter enables a moving box overlay on the output when in freeze frame or test image mode. This function is useful for determining whether or not there is a live signal arriving from this output at a downstream signal point.

Box color
: The color used for the moving box overlay.

Enable text overlay
: A user specified text label can be added to the output signal when the output is in Test Image mode.

Text
: A user defined custom text label to use for the Test Image overlay.

Text color
: The color to use for the custom text label above.

Test image pattern
: Several predefined test image patterns can be selected for use in the Test Image output mode. To get a uniform color over the entire picture, select the Flat field (user specified color) option.

Background color
: Background color fill when Flat field is selected as the Test image pattern.

The Framestore setting section contains the following configuration options:

Resync condition
: When not using the User reference sync, this option decides if the output should be resynchronized to achieve the lowest possible latency when the input is again available after a sync loss event. If it is desirable to keep a continuous output signal independent of the input signal, keep this option at No resync and use it with the Test Image or Freeze frame Signal loss mode.

Extra frame delay
: If more delay through the frame synchronizer than the minimum possible is required, up to 2 extra frames can be specified here.

The Uploaded Test Image section contains configuration for custom test signal images:

Enable
: Check this box to use a custom uploaded test image instead of an internally generated.

Status
: Shows the status for the custom test image.

Upload status
: Shows status for custom test image upload progress.

Resolution
: The pixel resolution of the currently uploaded test image.

To upload a new custom test image, press the Upload Test Image button on the bottom of the screen.

8.9.2 Video Monitoring tab

The advanced configuration page is available on some Encoders, and either the Decoder or the SDI output connected to the decoder.

8.9.2.1 Monitoring config

The configuration settings might vary depending on where the monitoring is placed.

Enable
: An overall enable/disable for all video monitoring.

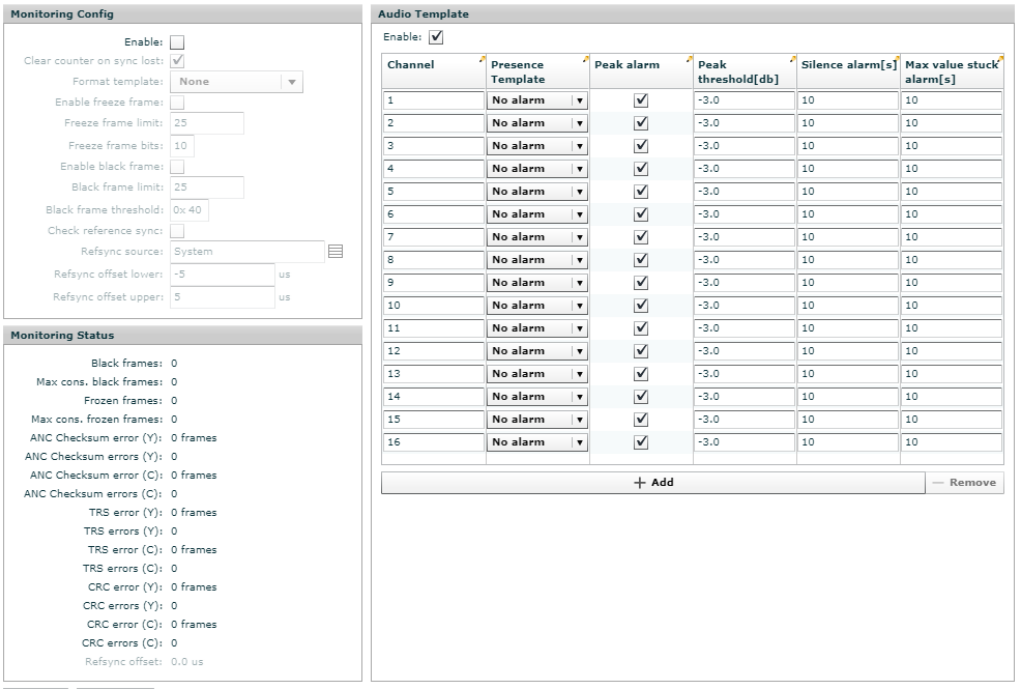


Figure 8.131 Monitoring configuration and status

Format template
: An alarm will be triggered if the video format does not match the configured format.

Black frame alarm
: Alarm is triggered when number of consecutive video frames where all active pixels are below the threshold is reached.

Freeze frame alarm
: Alarm is triggered when number of consecutive video frame where all the active pixels remains at the same value. It is possible to override how many bits of a pixels that should be checked. Ex: Set to 8 for 8 bit mode.

Reference sync
: Enable to verify if incoming signal is locked to a selected reference signal. Alarm will be triggered when the difference between them are outside the configured window.

8.9.2.2 Monitoring status

Shows counters and status for monitoring. Ex the number of video frames that have been below the black frame threshold.

8.9.2.3 Audio template

Add one entry per channel that shall be monitored. Note that the channels are indexed per mono-channel, not channel pair. Each channel can be configured with:

- The desired presence
- Enable peak threshold alarm, which will trigger if sample peak value is above the configured threshold.
- Number of seconds the audio can be silent before an alarm is triggered. Selecting a value of 0 will disable the alarm.
- Number of seconds the audio can be at the same maximum peak value before an alarm is triggered. Selecting a value of 0 will disable the alarm. The maximum sample value is samples 10 times per second.

8.10 Outputs

The Outputs page contains all information and settings that apply to the output ports of the device. The navigation list on the left hand side lets the user select which output to view, or to select Outputs Overview to view a summary of all the outputs on the device.

The labeling of the outputs is a combination of the user defined name of the output and the physical number of the output port.

8.10.1 Outputs Overview

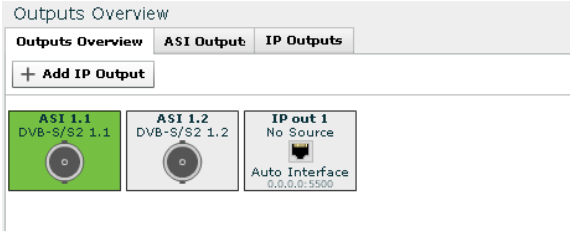


Figure 8.132 Outputs overview

The Outputs Overview page shows a graphical view of all the current outputs on the unit, as shown in **Figure 8.132**.

Note: Some ports have configurable direction, see **Section 8.4.3**.

Each output has a symbol referring to illustrate whether it is an ASI or IP, and each symbol is colored by its current alarm severity level. The output type is also written in the symbol box, along with its port numbering (as described in **Section 6.1** and the label or a generated service

description if no label is set. Mouseover on any output icon will give some configuration status, transport stream details and port specific details.

Pressing the Add IP input button adds a new IP input with an empty configuration and disabled.

8.10.1.1 ASI Outputs

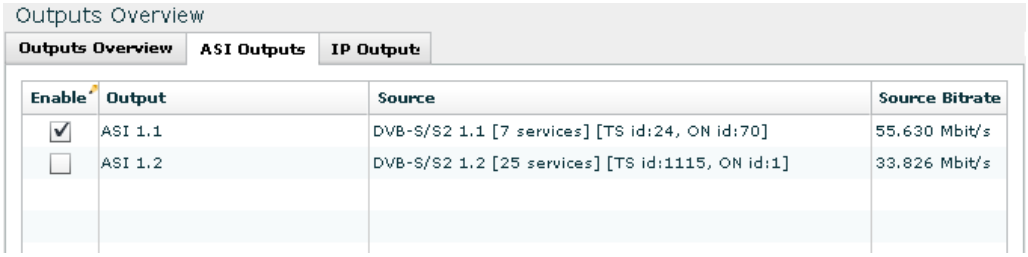


Figure 8.133 Outputs overview (ASI tab)

The ASI Outputs shown Figure 8.133 tab presents a list of all the ASI outputs with the following information:

Enable
: Enables/Disables the output.

Output
: The name of the output, consisting of the user defined label combined with the physical name of the port.

Source
: A summary of the source including the stream type, the number of services, the transport stream ID and the original network ID.

Source Bitrate
: The total bitrate of the transport stream currently transmitted, in Mbit/s.

8.10.1.2 IP Outputs

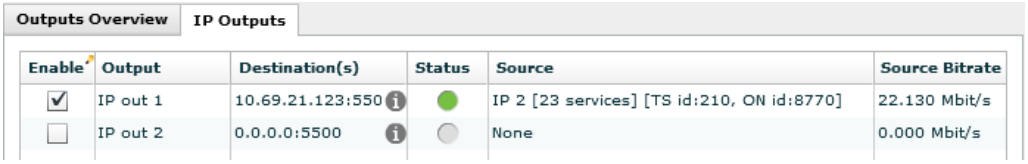


Figure 8.134 Outputs overview (IP tab)

The IP Outputs shown Figure 8.134 tab presents a list of all the IP outputs with the following information:

Enable
: Enables/Disables the output.

Output
: The name of the output, consisting of the user defined label combined with the physical name of the port.

Destination(s)
: The IP and port of the destination. Hovering over the "i" icon displays additional details about the stream such as the list of pids with name and bitrate.

Status
: The color of the icon indicates the current alarm severity level.

Source
: A summary of the source including the stream type, the number of services, the transport stream ID and the original network ID.

Source Bitrate
: The total bitrate of the transport stream currently transmitted, in Mbit/s.

8.10.2 TS Output

When selecting an output a new page on the right hand side with information about the selected output is displayed. The header of the page shows the current alarm status (if it is an IP output) and the name of the output. The list of tabs is dependent on what sort of output is selected (ASI, IP,...).

For an IP output, holding the mouse cursor over the alarm status indicator brings up a tool tip displaying up to 30 of the current alarms (if any) on this particular output.

8.10.2.1 Main tab

The Main tab presents general information about the output port settings. Its content is dependent on what sort of input is selected (ASI or IP).

8.10.2.1.1 Main (ASI output)

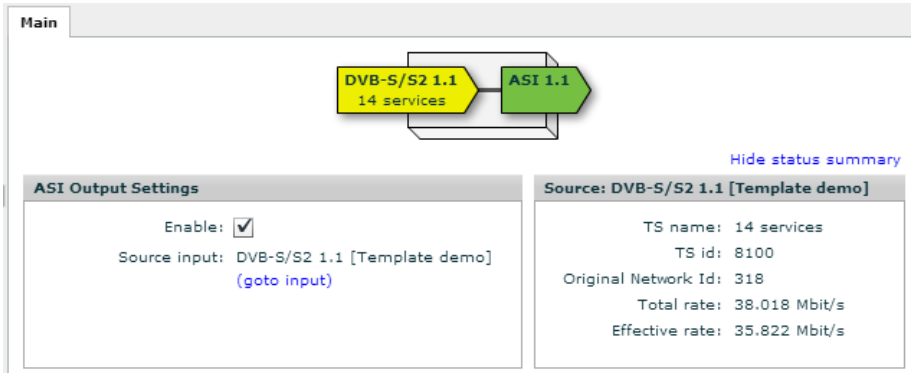


Figure 8.135 Main tab for ASI outputs

The Virtuoso has a fixed number of ASI output ports which depends on the hardware configuration. All the ASI outputs available (if any) are listed in the left panel. The Main page shown **Figure 8.135** lets the user configure the ASI port parameters on the selected Output.

The ASI Output Settings section lets the user configure the following parameters:

Enable output
: Enable or disable the output.

Source input
: Currently the ASI outputs are hard-wired, so the field is read-only and displays the type, port number and name of the source.

The Source section in the top right corner of the page gathers some important information about the selected source. The header of the section displays the type of stream, port number and name of the transport stream. The other information are:

TS name
: The name of the transport stream.

TS id
: The transport stream id.

Original Network id
: The original network id.

Total rate
: The total bitrate in Mbit per second.

Effective rate
: The effective bitrate (i.e. null packets being excluded) in Mbit per second.

8.10.2.1.2 Main (IP output)

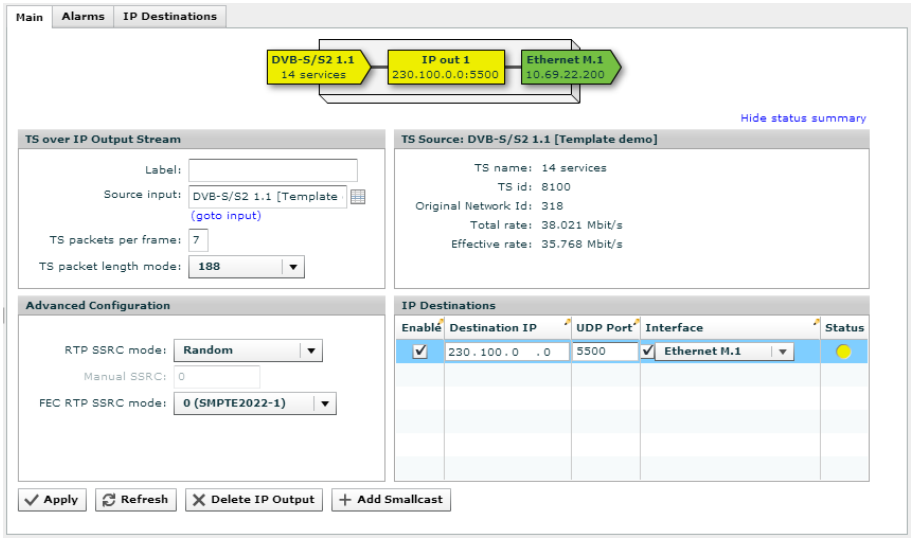


Figure 8.136 Main tab for IP outputs

The Main page shown **Figure 8.136** lets the user configure port level parameters on the selected Output.

Ts over IP Output Stream

The Ts over IP Output Stream section lets the user configure the following parameters:

Label
: A user-defined label for the selected output. The label is only used for presentational purposes.

Source input
: The source input (ASI or IP). A click on the field displays a table listing all the inputs. It is also possible to create directly a new input.

TS packets per frame
: Number of TS packets per IP frame.

TS packet length mode
: Number of bytes per TS packet. Available options:

  - 188: Source TS packet is truncated to 188 bytes.
  - 204 original: All 204 bytes from the source TS packet are output as they came in. If source was 188 bytes, 0xff is inserted above byte 188.
  - 204 pad: Source TS packet is truncated to 188 bytes, then padding of 0xff is added in byte 189 to 204.

Advanced Configuration

The Advanced Configuration contains the following parameters:

RTP SSRC Mode
: Select which mode to use in the SSRC field in the RTP header of the data stream. Available options:

  - 0 (SMPTE 2022-1)
  - Manual. If selected, the user is required to provide an RTP SSRC value.
  - Random

Manual SSRC
: RTP SSRC value. Only available if **Manual** is the selected mode for the previous field.

FEC RTP SSRC Mode
: Select which mode to use in the SSRC field in the RTP header of the FEC streams. Available options:

  - 0 (SMPTE 2022-1)
  - Random (RFC 3550)
  - Follow data stream

TS source

The TS Source section gathers some important information about the selected source. The header of the section displays the port number and name of the transport stream. The other information are:

TS name
: The name of the transport stream.

TS id
: The transport stream id.

Original Network id
: The original network id.

Total rate
: The total bitrate in Mbit per second.

Effective rate
: The effective bitrate (i.e. null packets being excluded) in Mbit per second.

IP Destinations

The IP Destinations section lets the user configure one or several destinations. It is possible to add/remove destinations from the list by pressing the buttons Add Smallcast/Remove Smallcast. For each destination, the parameters are:

Enable
: Enable/Disable transmission to the destination.

Destination IP
: The IP v4 address of the destination.

Destination port
: The port of the destination.

UDP port
: The port of the source.

Interface
: Configuration of the IP interface.

8.10.2.2 Alarms

The Alarms page, only present for IP outputs, lets the user configure and view the status of all alarms belonging to the selected output. The page functions exactly like the input alarms page (see **Section 8.6.2.2**).

8.10.2.3 IP Destinations

The IP Destinations tab (only present for an IP output) lists all the destinations for the selected IP output, and provides for each destination some informative and configuration capabilities.

Each destination can be enabled and disabled by using the enable checkbox located to the left of the destination. To add or remove a destination use the Add IP Destination or Remove IP Destination buttons.

8.10.2.3.1 Main

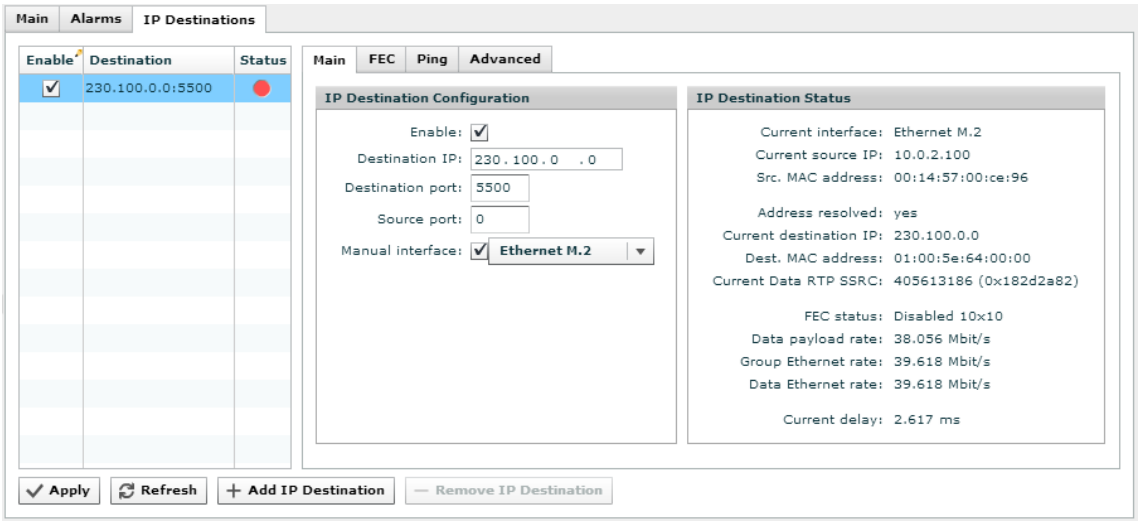


Figure 8.137 Main tab details

The Main tab is shown **Figure 8.137**.

IP Destination Configuration

The IP Destination Configuration section lets the user configure the destination that is selected in the left hand list.

Enable
: Enable/Disable transmission to the destination.

Destination IP
: The IPv4 address to transmit to.

Destination port
: The UDP destination port to use.

Source port
: The UDP source port to use.

Manual interface
: If checkbox is ticked, which specific IP interface the stream should be transmitted on.

If the checkbox is not ticked, the IP destination address will determine which interface the stream will be transmitted on, by routing according to the device's IP routing table. *Note: Automatic routing is not yet supported*.

Launch Delay Offset
: Configures the delay in number of milliseconds that is introduced in the transmission (output buffer delay).

IP Destination Status

The IP Destination Status section presents some detailed information about the destination. The following statuses are displayed:

Current interface
: The current IP destination interface used.

Current source IP
: Actual IP source address currently in use.

Src. MAC address
: Current source Ethernet MAC address.

Address resolved
: Whether the destination MAC address is resolved or not.

Current destination IP
: IP destination address currently in use.

Dest. MAC address
: Current destination Ethernet MAC address.

Current Data RTP SSRC
: Currently used RTP Synchronization Source identifier value.

FEC status
: The forward error correction status.

  See **Section 8.10.2.3.2** for more details.

Data payload rate
: The effective payload bitrate (excluding Ethernet/IP/RTP and FEC overhead) for the data stream.

Group Ethernet rate
: The total bitrate of the destination including protected data and FEC.

Data Ethernet rate
: The total bitrate of the transmitted data stream.

Current delay
: The current delay introduced in the signal from the input to IP output.

8.10.2.3.2 FEC

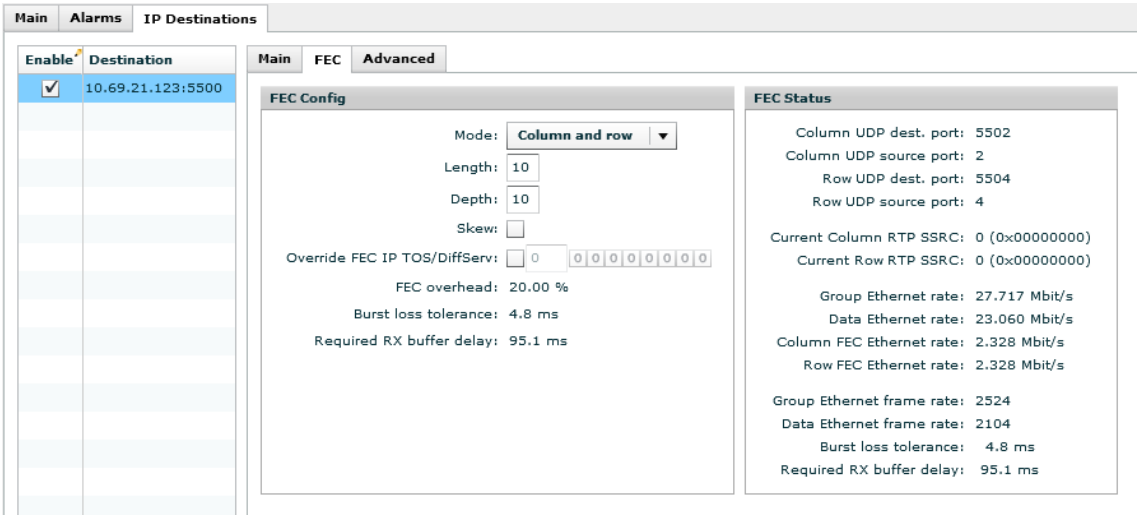


Figure 8.138 Forward Error Correction details

FEC Config

The FEC Config tab shown **Figure 8.138** lets the user configure the forward error correction parameters for the selected output destination. The parameters are:

Mode
: Selects the FEC mode. Available options:

- Disabled: No FEC.
- Column: Column only.
- Column and row: Both column and row.

Length
: Number of FEC columns to be used.

Depth
: Number of FEC rows to be used.

Skew
: Enables/Disables skew FEC mode.

Override FEC TOS/DiffServ
: Use manually configured IP Type-Of-Service / Differentiated Services for the FEC streams.

FEC overhead
: Expected FEC overhead expressed in % of data IP rate if the current settings where to be applied.

Burst loss tolerance
: Expected burst tolerance given the current data frame rate if the current settings where to be applied.

Required RX buffer delay
: Required RX buffer delay given the current data frame rate if the current settings where to be applied.

FEC Status

The FEC Status section displays some information related the use of forward error correction. The following statuses are provided:

Column UDP dest. port
: UDP destination used for transmitted FEC column stream.

Column UDP source port
: UDP source used for transmitted FEC column stream.

Row UDP dest. port
: UDP destination used for transmitted FEC row stream.

Row UDP source port
: UDP source used for transmitted FEC row stream.

Current Column RTP SSRC
: Currently used column FEC RTP SSRC value.

Current Row RTP SSRC
: Currently used row FEC RTP SSRC value.

Group Ethernet rate
: Total bitrate of the destination including protected data and FEC.

Data Ethernet rate
: Total bitrate of the transmitted data stream.

Column FEC Ethernet rate
: Total bitrate of the transmitted FEC column data stream.

Row FEC Ethernet rate
: Total bitrate of the transmitted FEC row data stream.

Group Ethernet frame rate
: Total Ethernet frame rate of the destination including protected data and FEC.

Data Ethernet frame rate
: Total Ethernet frame rate transmitted data stream.

Burst loss tolerance
: Burst tolerance given the current settings.

Required RX buffer delay
: RX buffer delay given the current settings.

8.10.2.3.3 RIPv2

Virtuoso provides support for building service redundancy in IP networks. The redundancy can be achieved by transmitting copies of the same service using two or more Virtuoso attached to the same network at different locations. The service is transported in the network by Source Specific Multicast (SSM) to all clients requesting it. It is carried by a single SSM channel identified by a source IP address and a multicast group number. When all cooperating Virtuoso use the same channel to transmit the same service, the SSM routing algorithm select the closest box as the service source for a given client. The distance between the client and the source is measured as the unicast path cost. Virtuoso can change the path cost by modifying routing database of the first hop router which distributes this information further in the network, thereby modifying SSM routes. For example, when one of Virtuoso observes that the stream it is transmitting has degenerated it announces high path cost. In response, SSM selects other box that has lower path cost to the client, thereby achieving source switchover.

To modify route database of the first hop router Virtuoso uses RIPv2. The configuration of RIPv2 is divided in two sections. The first section is located in the interface configuration and controls per interface RIPv2 behavior. The second section is located in the IP output configuration at the RIP tab. For ease of presentation, we start the description from per IP output configuration.

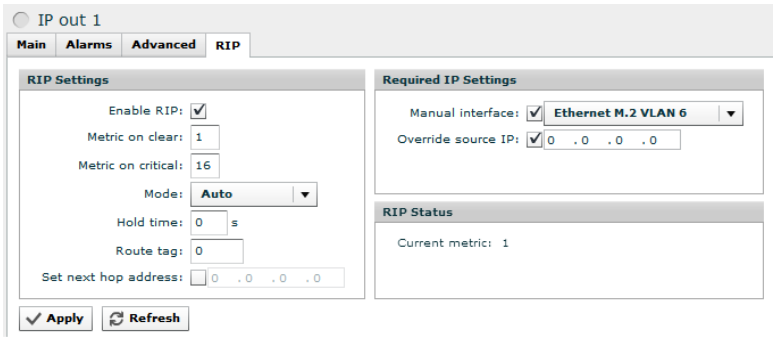


Figure 8.139 Per IP output RIPv2 settings

To enable service redundancy in an IP network for an IP stream, it is necessary that the stream is transmitted from more than one location over the same SSM channel. This implies that the source IP and multicast group address must be the same for all redundant copies of the stream. To achieve the common source IP address for all copies, Virtuoso enables a user to overwrite the source IP address of an IP stream. This creates effectively a virtual IP source for this IP stream which is sent through this box. To set up a route to this source Virtuoso transmits RIP messages to the first hop router that this source is reachable via Virtuoso.

The configuration of IP source is done via "Required IP settings" (see Figure 8.139) with the following options:

Manual interface
: Since the IP stream destination address is an IP multicast address, a user must select an interface for this IP stream.

Override source IP
: The source IP address must be specified for this IP stream. Together with the IP multicast group address it forms an SSM channel identifier that should be the same for all copies of the stream in the network.

The selected IP address for the IP stream should be a foreign address with respect to the network that the selected interface is attached to. When the selected IP source address belongs to the same network as the selected interface, is it not possible to setup a route for it at the first hop router, since it is directly reachable by this router.

The route description to the IP source that Virtuoso announces is controlled by *RIPv2 Settings* with the following options:

Metric on clear
: This field defines the path cost to the stream source which is announced when no critical alarm is active for the stream. The metric value is in the range of 1 to 16 where 16 means that the route is unavailable.

Metric on critical
: This field defines the path cost to the stream source which is announced when a critical alarm is active for the stream. The metric value is in the range of 1 to 16 where 16 means that the route is unavailable.

Mode
: To facilitate verification of the RIPv2 functionality, the RIPv2 module can be forced to transmit messages with the metric specific to the alarm state or clear state by selecting "Force alarm" or "Force clear" respectively. A user can restore the standard operation of the RIPv2 module by selecting the "Auto" option. In this mode the metric value carried by the RIP message is controlled by the current alarm level.

Set next hop address
: The first hop router receiving RIP messages assumes that the announced routes go via the network device that sends the messages. With this field a user can redefine the next hop IP for this stream as seen from the first hop router perspective. It should be noted that this field is marked as an "advisory" field by RFC2453. Thus, the provided next hop address can be ignored by some routers.

Route tag
: The field defines a route tag for the announced route.

Hold time
: In the situation when critical alarm is turned on and off rapidly, it can be useful to maintain the current route state until the situation stabilizes. With this field a user can specify the minimum time a defined route persist after the switch occurred.

The *RIP Status* window provides information about the currently transmitted metric value. The transmitted metric value can differ temporarily from the selected metric value due to hysteresis operation that is controlled with the hold time parameter.

The routing information generated for individual IP streams is aggregated on per interface basis and a single RIP message is generated. While the destination and transmission frequency of RIP

messages is defined by RFC2453, a user can redefine this parameters to tune the RIPv2 module behavior. Per interface configuration is accessible via *Advanced* settings at the network interface configuration presented in Figure 8.140.

8.10.2.3.4 Interface specific settings

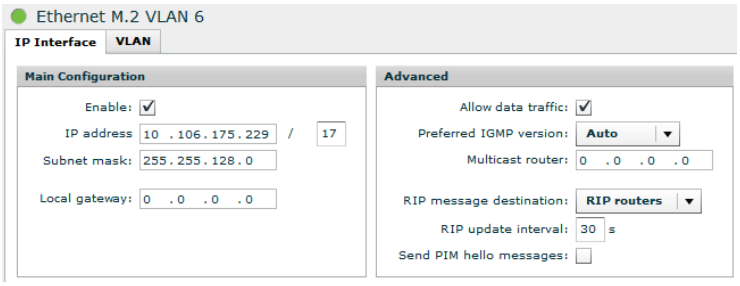


Figure 8.140 Per interface RIPv2 settings

The elements affecting RIPv2 behavior are following:

RIP message destination
: According to RFC2453, the standard IP multicast address for RIPv2 communication is 224.0.0.9 denoted as "RIP routers". A user can overwrite this setting and select other destination for RIP messages. When configured with "All routers" Virtuoso sends RIPv2 messages to 224.0.0.2 which is the standard multicast address which all routers listen on. For backwards compatibility with RIP version 1 a user can select "Broadcast" destination which sends RIPv1 messages to the local network broadcast address.

RIP update interval
: As defined in RFC2453, the RIPv2 process transmits routing updates every 30 seconds with an additional random variation of 5 seconds. This interval can be redefined by a user with this field. If other value than 30 second is selected no additional time variation is added. The interval resolution is 1 second.

Send PIM hello messages
: The standard behavior of a PIM multicast router is to forward packets to downstream multicast routers only if the packets originate from a local host or from a PIM capable router. However, IP stream source address must be a foreign address with respect to the network Virtuoso is attached to. Thus, packets composing the stream are regarded by the first hop router as originating from foreign network, in consequence of with the router discards them. To circumvent this problem Virtuoso can send "PIM hello" messages to the first hop router which registers it as a PIM router and will forward downstream all foreign packets originating from Virtuoso.

  The PIM hello messages assign the lowest Designated Router (DR) Priority (i.e. 0) to Virtuoso. This should prevent Virtuoso from being elected as DR for the local network. However, if all routers in the network have DR priority set to 0, the device with the lowest IP address is elected as DR. If Virtuoso is elected as DR, Protocol Independent Multicast will malfunction.

8.10.2.3.5 Ping

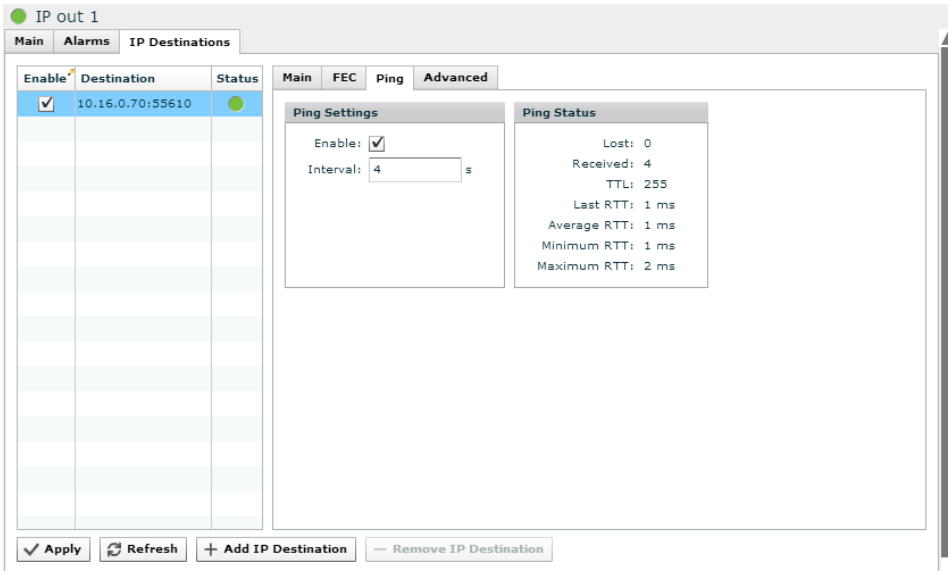


Figure 8.141 Output Ping Configuration

For the currently selected IP destination (selected to the left), the following Ping section can be used.

The Ping tab shown to the right, **Figure 8.141** lets the user configure the output ping configuration.

Ping Settings
: Here the user can click to enable the ping and set the time interval in seconds.

Ping Status
: This shows the user the current statistics for the active ping. This is also seen in **Section 8.5.1.1**.

8.10.2.3.6 Advanced

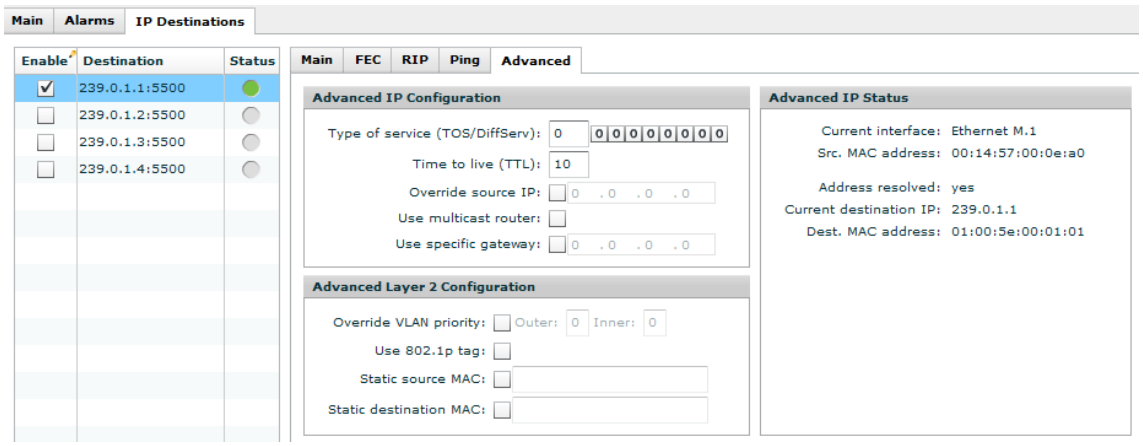


Figure 8.142 Advanced IP configuration details

The Advanced tab shown **Figure 8.142** let the used configure advanced IP configurations.

Advanced IP Configuration

The parameters accessible in the Advanced IP Configuration section are:

Type of service (TOS/DiffServ)
: Value of the Type-Of-Service / Differentiated Services in the IP header.

Time to live (TTL)
: Value of the Time-To-Live field in the IP header.

Override source IP
: Enable/disable and set a manual source IP address.

Use multicast router
: Send multicast streams to the MAC address of the configured multicast router of the interface instead of the multicast MAC address. For configuration of the multicast router address, see **Section 8.5.2.1**.

Use specific gateway
: Enables the use of one specific IP gateway/router for this specific stream. The Ethernet frames will be forwarded to this router, instead of a local destination node or the Data gateway that is configured on the IP interface (see **Section 8.5.2.1**). Note that this address must be local to the IP network configured on the destination interface.

Advanced Layer 2 Configuration

The parameters accessible in the Advanced Layer 2 Configuration section are:

Override VLAN priority
: Override default VLAN priority values. Outer and inner VLAG tag can be configured.

Use 802.1p tag
: Forces the insertion of the 802.1p tag (with VID = 0x0) on non-VLAN interfaces.

Static source MAC
: Enables/Disables the use of a manually configured source Ethernet MAC address.

Static destination MAC
: Enables/Disables the use of a manually configured destination Ethernet MAC address.

Advanced IP Status

The Advanced IP Statuses section presents the same information as **Section 8.10.2.3.1**

8.10.3 SDI Output

When a specific SDI output is selected a page with information about that output is displayed.

Some outputs will have a more detailed status and configuration.

8.10.3.1 Simple SDI Output

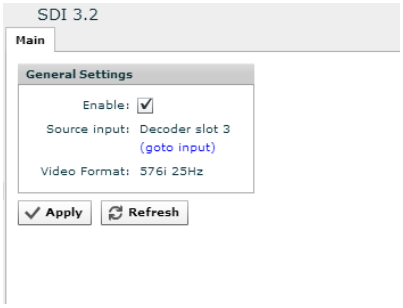


Figure 8.143 SDI Output Main

The Main page displays 1 section, as shown in figure 8.143.

The only field is SDI Output Settings. This contains the configuration parameters of the SDI output:

Enable
: This shows whether the SDI output is currently enabled. The SDI output is enabled or disabled by clicking the check box and then Apply.

Source Input
: This shows the source from the given output.

Video Format Input
: This shows the video format from the given output.

8.10.3.2 Advanced SDI Output

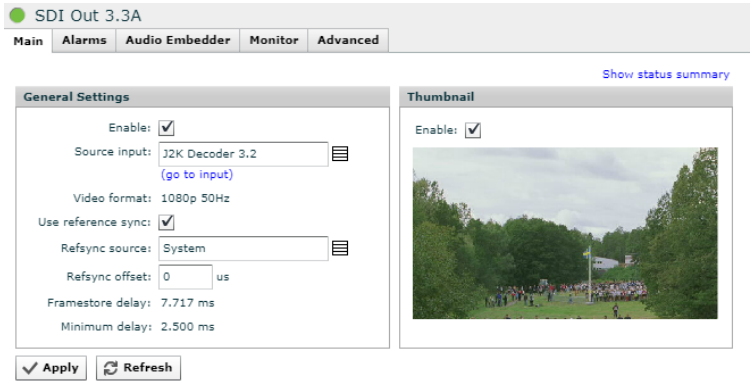


Figure 8.144 SDI Output Main

Figure 8.144 shows a more advanced SDI output with separate configuration. Here it is possible to configure source, reference sync, audio embedding, monitoring and sync loss configuration.

8.10.3.3 MADI Output

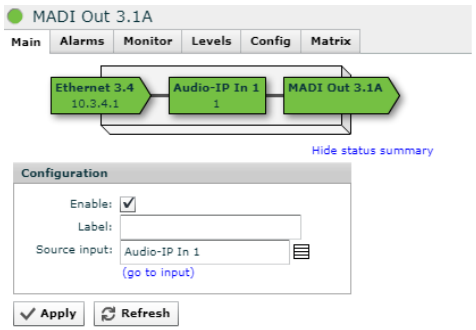


Figure 8.145 MADI Output

Figure 8.145 shows the MADI output configuration. Select the main source in the Source input box. The source of each channel can be configured separately under the Matrix tab. Audio gain,delay and polarity can be configured under the Config tab, while the Monitor tab gives configuration for audio silence and templates.

8.10.4 Audio Outputs

8.10.4.1 Audio-IP Output

The Audio-IP Out element represents an audio over IP stream transmitted on the network. The stream may contain one or more audio channels originating in the device.

In this version the only allowed source for the Audio-IP Out element is a Video-IP Out channel. This is to support operation as a VSF TR-04 transmitter, where AES67 streams are transmitted in sync with a SMPTE 2022-6 video stream. When a Video-IP Out is the source of the Audio-IP Out, the audio is taken from the output of the frame sync making it possible to use this function together with both synchronized and unsynchronized video sources - as they can be synchronized by the Video-IP Out frame synchronizer before being transmitted to the IP network.

8.10.4.1.1 Audio-IP Out - Main

The Audio-IP Out Main tab is shown in figure 8.146. The most important configuration and status parameters are available on this page.

The Audio over IP Output Stream section contains settings related to the network audio stream:

Label
: A user configurable label. Is used as a tag in the user interface to ease navigation and stream identification.

Audio source
: The source of the audio channels to be transmitted. Only Video-IP Out“ channels are valid sources.

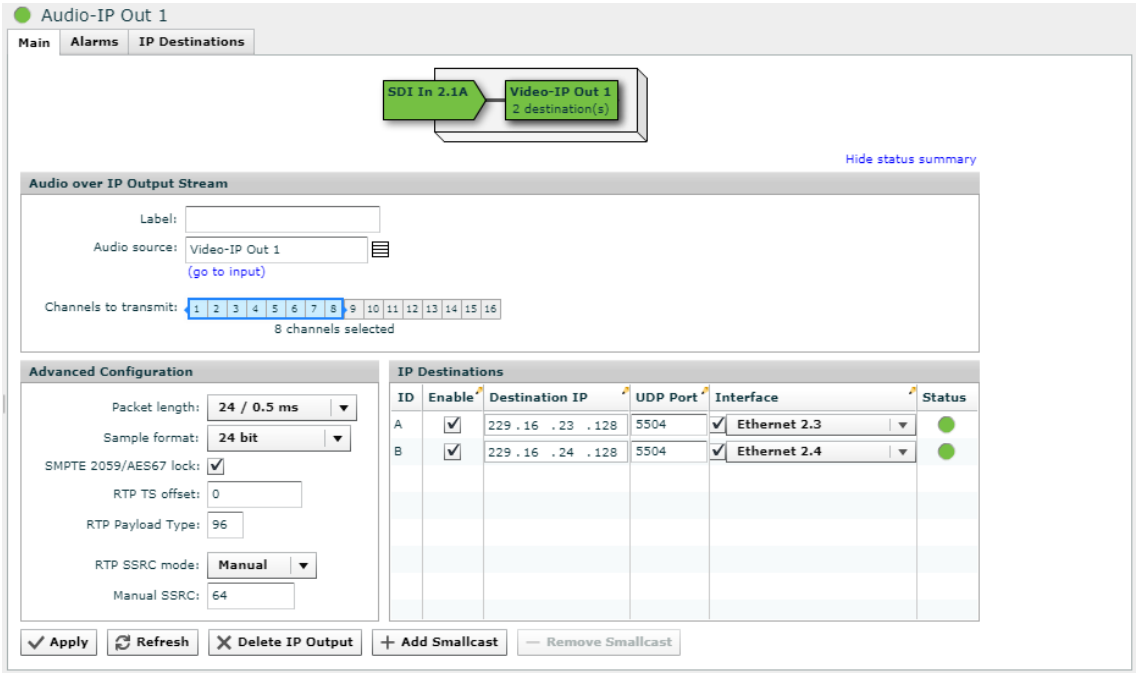


Figure 8.146 Main tab for an Audio-IP Output channel

Channels to transmit
: Selects which of the source's audio channels that should be transmitted as an audio over IP stream. Slide and resize to select channel count and which source audio channels to transmit. The number of channels transmitted affects the network packet length, and this parameter must therefore be configured together with the Packet length parameter - if one is increased, it might be required to lower the other.

The Advanced Configuration section contains advanced settings related to the transmitted audio over IP stream:

Packet length
: Number of samples that is packed into each RTP/IP packet. Measured in audio samples or ms (at 48 kHz), this parameter affects the minimum delay that can be achieved through the IP network. It also affects the packetization overhead due to the network headers, which have constant length independent of the number of samples in each packet.

Sample format
: The audio over IP stream sample format bit depth. Selecting 24 bit means the entire 24 bit audio sample is transmitted, but no AES3 meta data bits. If an application depends on transparent AES3 data, choose the 32 bit AM824 option. The 16 bit option is provided for compatibility, and may be used if network bandwidth must be kept low, and 16 bit audio is regarded as sufficient.

  For simplicity, it is recommended to choose one standard sample format that is used for all network audio streams in a facility, easing the configuration of receivers which then all can have a static Sample format configuration.

SMPTE 2059/AES67 lock
: Select this option to lock the RTP Timestamp field to PTP according to SMPTE 2059, SMPTE 2110-30 and AES67. Note that when using this option, the device must be configured to lock the system to a network Precision Time Protocol (PTP) source, and the Video-IP Out audio source must be configured with output reference sync, and with the sync source set to System. See **8.4.5.1** for info about how to configure a PTP clock.

Note: When this option is selected, no audio stream is transmitted unless the device is locked to a PTP network clock, or has been locked some time before, after the device was powered up.

RTP TS offset
: Configures the offset of the RTP Timestamp value measured at the PTP/SMPTE 2059 epoch. In AES67 this may be an arbitrary value, but in SMPTE 2110 this offset is mandated to be zero.

RTP Payload type
: The value of the Payload type field in the RTP header of the transmitted network audio stream. This can in most cases be left at the default value of 96 (dec), but other values between 96 and 127 (RTP dynamic payload type range) may be configured, e.g. for compatibility with other equipment or an organization's standard operating procedures.

RTP SSRC mode
: How the value of the SSRC field in the RTP header of the transmitted network stream is decided. The default behavior is to choose a new random 32 bit value every time the transmitter resynchronizes the output stream. This is in accordance with the RFC 3550 RTP specification. Under certain circumstances it may be desired to keep this value fixed, and in this case the Manual option can be selected.

Manual SSRC
: The actual decimal value to use for the RTP SSRC field, when RTP SSRC mode above has been set to Manual.

Up to four identical copies of the output network stream can be transmitted with different IP/UDP parameters. The IP Destinations section contains settings related to the IP and UDP network layer for each of these streams:

Enable
: Check this box and press Apply to enable transmission of this stream. If this box is unchecked, no audio stream will be transmitted.

Destination IP
: The destination IP address to transmit to. Either an IP unicast or an IP multicast address may be configured.

UDP Port
: Which UDP destination port to use. This parameter is used for both unicast and multicast reception.

Interface
: Specify which Ethernet interface to transmit the outgoing network stream on.

8.10.4.1.2 Audio-IP Out - Alarms

The Alarms tab lets the user configure specific filters and severity levels for the alarms associated with the Audio-IP Out channel. Refer to 8.6.2.2 for an in-depth general explanation of alarm configuration of the device.

8.10.4.1.3 Audio-IP Out - IP Destinations

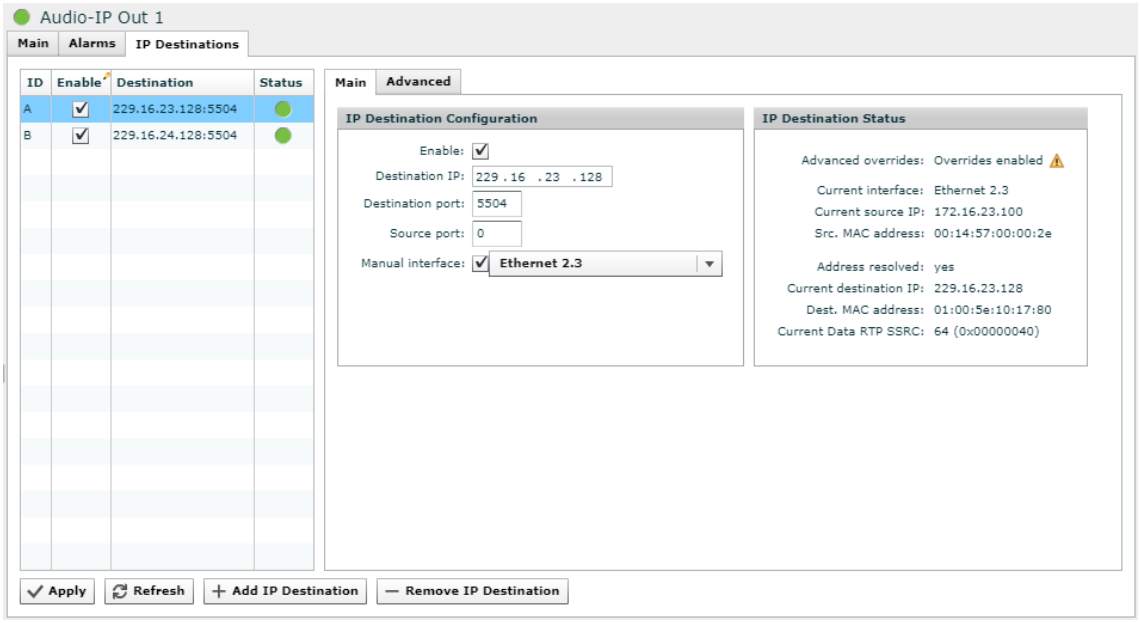


Figure 8.147 IP Destinations tab for an Audio-IP Output channel

The IP Destinations tab provides advanced configuration parameters of the outgoing IP network streams. The configuration is similar to the configuration for TS-IP Out, refer to 8.10.2.3 for a detailed explanation of the settings.

8.10.5 Video Outputs

8.10.5.1 Video-IP Output

The Video-IP Out element represents a video over IP stream transmitted on the network.

8.10.5.1.1 Video-IP Out - Main

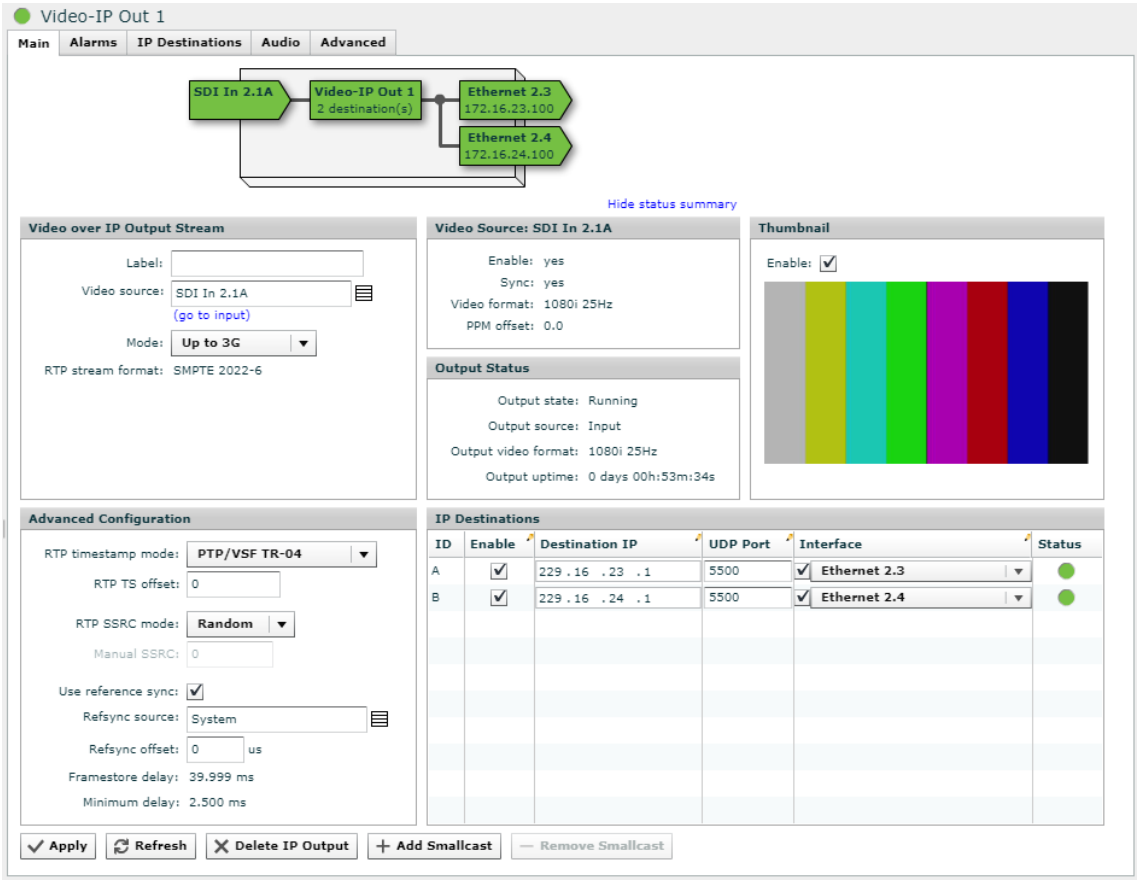


Figure 8.148 Main tab for a Video-IP Output channel

The Video-IP Out Main tab is shown in figure 8.148. The most important configuration and status parameters are available on this page.

The Video over IP Output Stream section contains settings related to the network video stream:

Label
: A user configurable label. Is used as a tag in the user interface to ease navigation and stream identification.

Video source
: The source of the video to be transmitted. Valid sources are SDI Inputs, Video-IP Inputs or Video input switches.

Mode
: Specify the most complex video standard that should be supported. This choice will affect what kind of licence that is required to enable the channel. This setting can also be used for limiting the maximum transmitted network bandwidth, providing safeguards for input signals with an unknown format.

RTP stream format
: The RTP stream format currently supported is SMPTE 2022-6.

The Advanced Configuration section contains advanced settings related to the transmitted video over IP stream:

RTP timestamp mode
: Configures how the Timestamp field in the RTP header of the outgoing stream should be set. Options are:

  - 2022-6 freerunning: 27 MHz freerunning RTP timestamp, updated each RTP/IP packet
  - PTP / VSF TR-04: 27 MHz RTP timestamp, frequency locked to PTP, with a constant offset at the PTP epoch, updated each RTP/IP packet

Note: When PTP/VSF TR-04 is selected, the RTP timestamp transmitted will not actually be locked to PTP and conform to SMPTE 2059 / TR-04, unless the device is locked to a PTP network clock, or has been locked some time before, after the device was powered up.

Note: To achieve the correct timestamping behavior when PTP/VSF TR-04 is selected, the device must be locked to a PTP network clock, or must have been locked some time before, after the device was powered up, and Use reference sync must be enabled on the Video-IP Out channel, using System as Refsync source. If the source signal is already locked to PTP, use the Refsync offset parameter to adjust the delay through the system.

RTP TS offset
: Configures the offset of the RTP Timestamp value measured at the PTP/SMPTE 2059 epoch. In TR-04 this may be an arbitrary value, but in SMPTE 2110 this offset is mandated to be zero.

RTP SSRC mode
: How the value of the SSRC field in the RTP header of the transmitted network stream is decided. The default behavior is to choose a new random 32 bit value every time the transmitter resynchronizes the output stream. This is in accordance with the RFC 3550 RTP specification. Under certain circumstances it may be desired to keep this value fixed, and in this case the Manual option can be selected.

Manual SSRC
: The actual decimal value to use for the RTP SSRC field, when RTP SSRC mode above has been set to Manual.

Use reference sync
: This option locks the output of the Video-IP Output's video frame synchronizer to a synchronization source independent of the source signal.

Refsync source
: Configures which sync source the frame synchronizer output should be locked to. Valid sources are video Sync In ports, SDI Inputs, or the System source. When using the System source, the frame start time will be deterministically locked to the absolute system time, and if the device is locked to PTP this means sync will be generated as specified in SMPTE 2059-1. See 8.4.5.1 for information about PTP configuration.

Refsync offset
: Specifies a positive or negative offset from the sync reference, measured in microseconds.

Up to four identical copies of the output network stream can be transmitted with different IP/UDP parameters. The IP Destinations section contains settings related to the IP and UDP network layer for each of these streams:

Enable
: Check this box and press Apply to enable transmission of this stream. If this box is unchecked, no video stream will be transmitted.

Destination IP
: The destination IP address to transmit to. Either an IP unicast or an IP multicast address may be configured.

UDP Port
: Which UDP destination port to use. This parameter is used for both unicast and multicast reception.

Interface
: Specify which Ethernet interface to transmit the outgoing network stream on.

8.10.5.1.2 Video-IP Out - Alarms

The Alarms tab lets the user configure specific filters and severity levels for the alarms associated with the Video-IP Out channel. Refer to 8.6.2.2 for an in-depth general explanation of alarm configuration of the device.

8.10.5.1.3 Video-IP Out - IP Destinations

The IP Destinations tab provides advanced configuration parameters of the outgoing IP network streams. The configuration is similar to the configuration for TS-IP Out, refer to 8.10.2.3 for a detailed explanation of the settings.

8.10.5.1.4 Video-IP Out - Audio

The Audio tab of the Video-IP Out channel has three sub-pages. In addition the Transparent SDI option is available at the sub page bar in the top rightmost corner.

Transparent SDI
: Activating this option will ensure fully transparent transport of the source SDI signal, and

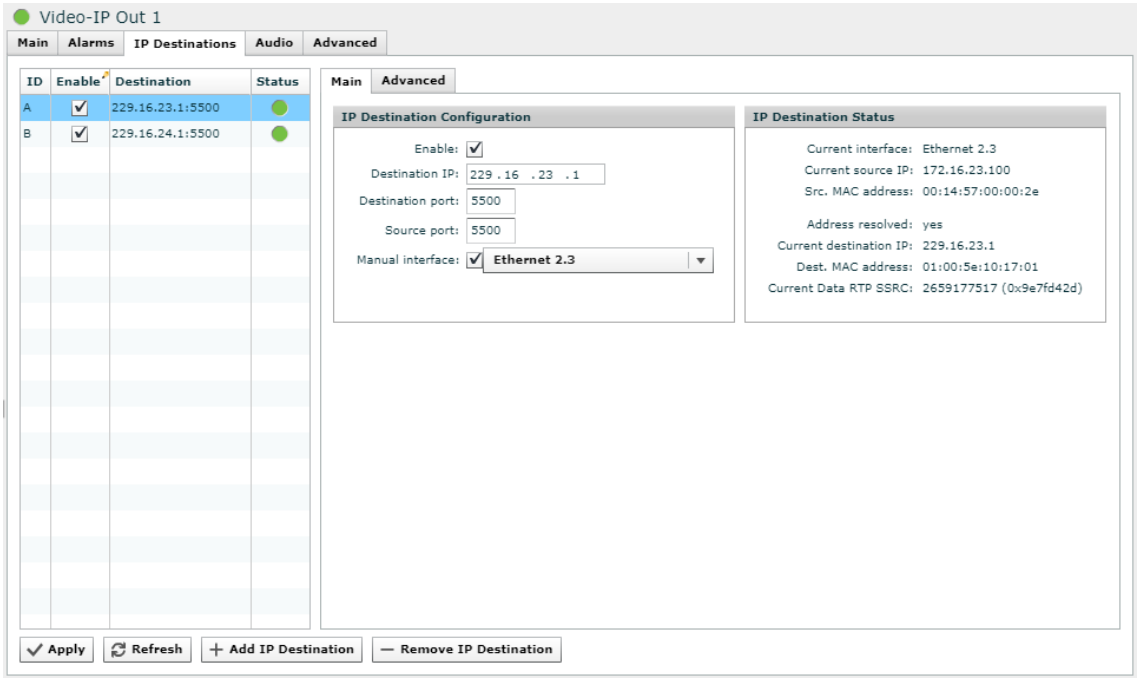


Figure 8.149 IP Destinations tab for a Video-IP Output channel

no audio embedding is performed. When using this option, advanced audio features such as levels, delay adjustment and the audio output remapping matrix are not available.

The Levels page shows the current and maximum sample peak value for each of the embedded audio channels. The measurement is done after the audio remapping matrix, and will therefore show the audio actually being embedded in the outgoing stream.

On the Config sub-page, a time delay measured in audio samples can be specified individually per mono audio channel. In addition, by deselecting the Enable checkbox beside any group of four mono channels, embedding of that ANC audio group can be disabled.

The Matrix sub-page is shown in **8.150**. On this page mono audio from any input in the same processing card/slot can be routed to any of the embedded audio channels of the outgoing video. This routing will also affect the audio going to an Audio-IP Out channel that may be using this Video-IP Out as it's audio source.

Note: When using the Video-IP Out as a source for an Audio-IP Out channel, the Transparent SDI option can NOT be used, as this would disable the audio going to the Audio-IP Out channel.

By clicking in the audio matrix while holding down the CTRL key, multiple consecutive channels can be routed diagonally.

The small virtual LEDs by the matrix audio input and output channels show the current status of that channel. The colour codes used are the same as audio indicators other places in the user interface:

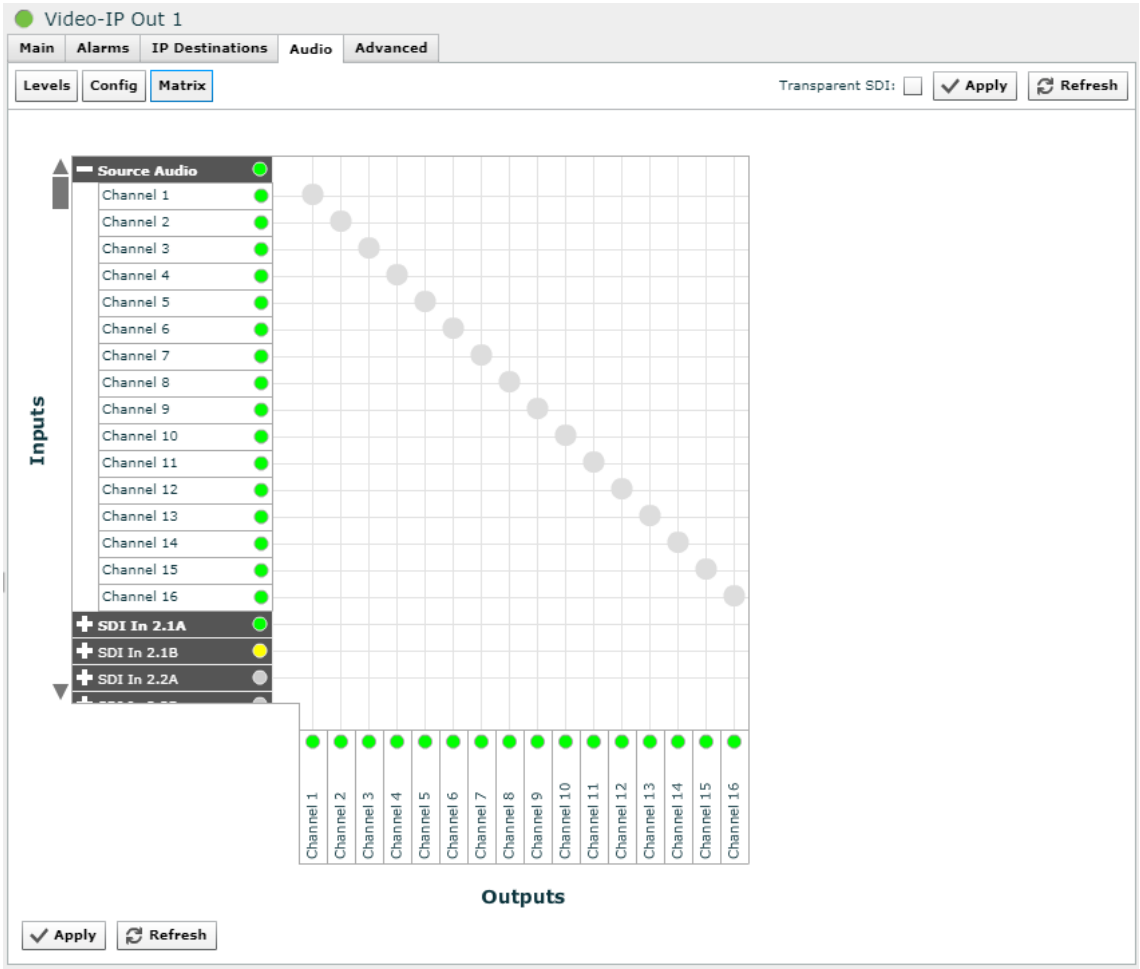


Figure 8.150 Audio Matrix sub-page for a Video-IP Output channel

- Grey: No audio present
- Yellow: Silent audio present
- Green: Non-silent audio present

9 SNMP

The product supports SNMP – Simple Network Management Protocol – for remote control and supervision, as well as Trap/Notification sending to external NMS systems. SNMP uses an extensible design, where management information bases (MIBs) describe the structure of the management data of a device subsystem. The primary purpose of SNMP is to export alarm and status information, but a range of MIBs related to configuration settings are also supported.

9.1 SNMP agent characteristics

The SNMP agent supports the SNMPv2c (Community based SNMPv2) protocol. All custom MIBS are written in SMIv2 format. The SNMP agent accepts both SNMPv1 and SNMPv2 messages and uses the normal UDP sockets for communication and listens for requests at UDP port 161.

The community strings and trap settings can be setup from Product info/SNMP Settings/SNMP Config (cf. **Section 8.4.7**).

SNMP Traps

The products support sending of SNMP traps (also called notifications) to multiple destinations. The current format of the trap messages itself is backward compatible with previous Nevion equipment for easy integration into existing NMS systems.

Both legacy SNMPv1 traps and SNMPv2 notifications are supported. It is however recommended to use the new SNMPv2 notification types for new deployments.

Refer to **Section 8.4.7** for setting the trap destinations.

9.2 MIB overview

This section describes the different modules used by the Virtuoso .

9.2.1 Supported standard MIBs

RFC1213-MIB
: MIB-II according to RFC1213.

9.2.2 Custom MIBs

For remote control and supervision using SNMP, the following set of MIBs is used:

NEVION-MIB
: Defines the top level MIB structure including the enterprise specific root node for device control (1.3.6.1.4.1.8768). Defined in `nevion.mib`.

NEO-TC-MIB
: Describes common textual conventions (data types etc.) used throughout the entire MIB set. Defined in `neo-tc.mib`.

NEO-DATA-2-VIURTUOSO-MIB
: Describes all the control and supervision parameters supported by the most recent Nevion products. It provides read and write access (when applicable) to any configuration or status parameters such as:

  - Device information
  - Table of current alarms
  - Network configurations
  - Control and supervision of any service delivered by the device. Defined in NEO-DATA-2-VIURTUOSO-MIB.mib .

NEO-DATA-MIB
: All the objects defined in this module are obsolete. Although still supported by the products for backward compatibility, it is not maintained and should not be used for any current implementation. All the definitions in this module have a mapping to `NEO-DATA-2-VIURTUOSO-MIB` which replaces `NEO-DATA-MIB` (cf. section Mapping of `NEO-DATA-MIB` into `NEO-DATA-2-VIURTUOSO-MIB` below for more details).

VIGW-BASE-MIB
: Is the current module describing the notifications. Its curious name and root node (1.3.6.1.4.1.22909) come from the fact that this module is backward compatible with oldest equipment from Nevion equipment. Defined in `nevion-legacy-traps.mib`.

Note: Currently, the nodes defined in this file are not accessible for reading or writing. They are only present for defining the notifications.

9.2.3 How to use the MIB

Note: In the remaining of this section we refer to NEO-DATA-2-Virtuoso-MIB as `NEO-DATA-2-XXXX-MIB` since this paragraph is general to all the newest Nevion products.

Structure of NEO-DATA-2-VIURTUOSO-MIB

`NEO-DATA-2-VIURTUOSO-MIB`, containing all the configuration/status parameter of a unit, is the place to look for when the user wants to read a field or set a configuration field in a unit. This module, containing several thousands of parameters, can seem quite intimidated at first. The object of this paragraph is to formalize the mapping of the internal representation of the data in Nevion's products (accessible with `http://w.x.y.z/txp_get_schema`) into the `NEO-DATA-2-VIURTUOSO-MIB`.

The challenge of mapping a multidimensional structure (internal representation of data in Nevion products) into a mono-dimensional one (SNMP) has been solved in the following manner. Any internal array A containing a group of scalar data S and a group of complex data C (inner arrays or collection of scalar/complex data) is mapped to:

- a table containing the group S with the keys of the parent tables preceding its own keys (let us suppose it is called `xTable`),
- a parent OID called `xSubTable` containing the group C. The mapping of the elements of C follows the same rules as above (recursively).

While this formalization may seem fairly complex, the mapping becomes intuitive with a bit of practice.

Special consideration

When accessing the instances of a virtual table which has an index of type UTF8StringKey, as specified in the textual convention, the size of the string must precede the string itself even in the case where it is the last index of the OID. Note also that the user must ensure that the OIDs are less than 128 sub-identifier long.

Mapping of NEO-DATA-MIB into NEO-DATA-2-VIURTUOSO-MIB

The reason why NEO-DATA-MIB became obsolete is that some NMS had unjustified restrictions applying to the values forming the OIDs (typically any value greater than 31 bit would be truncated). To avoid any integration problem, we decided to replace NEO-DATA-MIB by `NEO-DATA-2-VIURTUOSO-MIB` which maps all the OIDs defined in NEO-DATA-MIB into a 16 bit space. The mapping is defined by the following rules:

- The flags at bits 31, 30 and 29 is moved to bits 15, 14, 13 respectively,
- the reserved value 0xFFFFFF (RowStatus object) is mapped to the reserved value 0x1FFF,
- the reserved value 0xFFFFFE (RpcTrigger node) is mapped to the reserved value 0x1FFE,
- the 12 least significant bits remain the same.

9.3 Alarm/status related SNMP TRAPs

All TRAP messages are defined in VIGW-BASE-MIB. This section describes each trap message.

9.3.1 The main trap messages

The main (SNMPv2) trap messages are defined under the `unitNotifications` node in VIGW-BASE-MIB. The messages are described briefly in **Table 9.1**.

9.3.2 Severity indications

All alarm event traps (i.e. all traps defined in **Table 9.1** except `unitAlarmStatusChanged`) contain a severity field which is encoded according to the definition below:

Table 9.1 List of SNMPv2 traps

`unitAlarmStatusChanged`	This trap is sent when the top level unit alarm status (indicated by the `unitAlarmStatus` variable) changes. The trap indicates both the old and new alarm level. Transmission of this trap type can be enabled/disabled through configuration.
`unitAlarmAsserted`	This trap is sent when an internal alarm is raised. No `subid3` information is included. A corresponding `unitAlarmCleared` trap is sent when the alarm cause is cleared.
`unitAlarmCleared`	This trap is sent when an alarm condition previously indicated with `unitAlarmAsserted` is cleared.
`unitAlarmEvent`	This trap is sent when an alarm event (with no on/off state) is generated. No corresponding "cleared" message is expected for these traps. A typical example is an event like "User logged in".
`unitDetailedAlarmAsserted`	This trap is a more detailed version of `unitAlarmAsserted`. `subid3` information is included in addition to the basic parameters defined in `unitAlarmAsserted`.
`unitDetailedAlarmCleared`	This trap is sent when an alarm condition previously indicated with `unitDetailedAlarmAsserted` is cleared.
`unitDetailedAlarmEvent`	This is a more detailed version of `unitAlarmEvent`. `subid3` information is included in addition to the basic parameters defined in `unitAlarmEvent`.

Severity	Description
1	Cleared
2	Indeterminate
3	Warning
4	Minor
5	Major
6	Critical

9.3.3 Alarm event fields

A description of the fields in the alarm event traps is presented in **Table 9.2**. Most of the fields are entries from the `unitEventHistoryTable`. The instance identifier for each variable binding corresponds to the index in this table. This index is of kind `CircularLog` and will wrap around at 2^{32}.

Table 9.2.a Variables in SNMPv2 traps and their meanings

Field	Description
`unitEventSeverity`	This field indicates the severity of the alarm, 2-6. 1 will never be used, as this condition is indicated by transmitting a `unitAlarmCleared` message.

Table 9.2.b Variables in SNMPv2 traps and their meanings

Field	Description
`unitEventAlarmType`	This is an integer that describes the alarm type. Please refer to alarm documentation for description. From this type, one can extract the actual meaning of the `subid1` and `subid2` values in the message.
`unitEventAlarmId`	A unique identifier for this alarm type. Refer to alarm documentation in the user manual for values.
`unitEventAlarmName`	A fixed name corresponding to the alarm id.
`unitEventRefNumber`	This field is provided to easily match asserted/cleared alarms. In the cleared alarm it is set to the same number as in the asserted alarm.
`unitEventSubId1`	The first subidentifier to identify the source of the alarm. For products with single base boards it is typically set to a fixed value (0 or 1) and can be ignored.
`unitEventSubId2`	This field's purpose is dependent on the alarm type (alarm id). For some alarms it is not used and set to zero. For other alarms, it may e.g. indicate the channel/port number for the entity that generated the alarm.
`unitEventSubId3`	This field provide an even more detailed description of the alarm source. This field is only present in the "detailed" type of trap messages (`unitDetailedAlarmAsserted`, `unitDetailedAlarmEvent`). It's usage is dependent on the alarm ID. For example, in transport stream related alarms, `subid3` is used to indicate the PID value that caused the alarm.
`unitEventSourceText`	A textual description of the source of the alarm. This is typically a textual description of the `subid1` and `subid2` fields. For example, for transport stream related alarms, the text indicates the name (with label) of the port that generated the alarm.
`unitEventSubId3Label`	This field is fixed and indicates the label (meaning) of the `subid3` field, contained in the `unitEventSubId3` variable. It is intended to make it easy to log the alarm.
`unitEventDetails`	This is a generic text string that contains more details related to the alarm event. It's usage and content is dependent on the alarm ID.
`unitProdName`	This field provides the name of the product emitting the trap.
`unitAlarmStatus`	This variable contains the new, top level alarm status of the unit *after* the condition leading to this trap message. It may be used to quickly update the top level status for the device after receiving the trap message.

9.3.4 Matching of on/off traps

As mentioned previously, a `unitAlarmCleared` message is sent after a `unitAlarmAsserted` message and a `unitDetailedAlarmCleared` message is sent after a `unitDetailedAlarmAsserted` message.

The "cleared" event contains exactly the same identifiers as the "asserted" trap. This includes the alarm ID, `subid1`, `subid2` and `subid3` fields. This set of four identifiers uniquely identifies the source of an alarm.

A more easy way to match the traps is by using the `unitEventRefNumber` field. This is a simple integer that is the same in an "asserted" trap and in a "clear" trap.

10 Preventive Maintenance and Fault-finding

This chapter provides the schedules and instructions, where applicable, for routine inspection, cleaning and maintenance of the Virtuoso, to be carried out by the operator of the unit.

10.1 Preventive maintenance

10.1.1 Routine inspection

This equipment must never be used unless all the cooling fans are working. They should be checked when the unit is switched on and periodically thereafter.

10.1.2 Cleaning

- Remove power from the unit.
- Clean the external surfaces of the Virtuoso with a soft cloth dampened with a mixture of mild detergent and water.
- Make sure that the unit is completely dry before reconnecting it to a power source.

10.1.3 Servicing

Warning: Do not attempt to service this product as opening or removing covers may expose dangerous voltages or other hazards. Refer all servicing to service personnel who have been authorised by Nevion.

In case of equipment failure unplug the unit from the power and refer servicing to qualified personnel with information of the failure conditions:

- The power supply cord or plug is damaged
- Liquid has been spilled or objects have fallen into the product
- Product has been exposed to rain or water
- Product does not operate normally when following the operating instructions
- Product has been dropped or has been damaged
- Product exhibits a distinct change in performance

10.1.4 Warranty

The Virtuoso is covered by standard Nevion warranty service for a period of 24 months following the date of delivery.

The warranty covers the following:

- All defects in material and workmanship (hardware only) under normal use and service.
- All parts and labour charges
- Return of the repaired item to the customer, postage paid.
- Customer assistance through Nevion Customer Service Help Line

The warranty does not cover any engineering visit(s) to the customer premises.

10.2 Fault-finding

The objective of this chapter is to provide sufficient information to enable the operator to rectify apparent faults or else to identify where the apparent fault might be. It is assumed that fault-finding has already been performed at a system level, and that the fault cannot be attributed to other system components.

This manual does not provide any maintenance information or procedures which would require removal of covers.

Warning: Do not remove the covers of this equipment. Hazardous voltages are present within this equipment and may be exposed if the covers are removed. Only Nevion trained and approved service engineers are permitted to service this equipment.

Caution: Unauthorised maintenance or the use of non-approved replacement parts may affect the equipment specification and will invalidate any warranties.

If the following information fails to clear the abnormal condition, please contact your local reseller or Nevion customer care.

10.2.1 Preliminary checks

Always investigate the failure symptoms fully, prior to taking remedial action. The operator should not remove the cover of the equipment to carry out the fault diagnosis. The following fault-finding tasks can be carried out:

- Check that the PSU LED is lit. If this is not lit, replace external equipment, power source and cables by substitution to check that these are not defect.

- Confirm that the equipment hardware configuration is suitable for the purpose and that the unit has been correctly connected.
- Confirm that inappropriate operator action is not causing the problem, and that the equipment software set-up is capable of performing the required functionality.
- Check that the fans are unobstructed and working correctly.

When the fault condition has been fully investigated, and the symptoms are identified, proceed to fault-finding according to the observed symptoms. If the fault persists, and cannot be rectified using the instructions given in this manual, contact Nevion Customer Support. Switch off the equipment if it becomes unusable, or to protect it from further damage.

10.2.2 PSU LED not lit / power supply problem

Power fault-finding

1. Check the Power LED.
   - Is the LED unlit, but the unit still working properly?

     Yes
     : The Power LED itself is probably at fault - Call a Service Engineer.

     No
     : Proceed to next step

2. Check the Power Source.
   - Connect a piece of equipment known to work to the power source outlet. Does it work?

     Yes
     : The problem lies within the Virtuoso or the power cable. Proceed to next step.

     No
     : The problem lies with the power source. Check building circuit breakers, fuse boxes and the source outlet. Do they work? If the problem persists, contact the electricity supplier.

3. Check Power Cable.
   - Unplug the power cable and try it in another piece of equipment. Does it work?

     Yes
     : The problem lies within the Virtuoso. Call a Service Engineer.

     No
     : The problem lies with the cable. Replace the cable.

The PSU does not have any internal user changeable fuses.

10.2.3 Fan(s) not working / unit overheating

This equipment has forced air cooling and must not be operated unless all cooling fans are working. In the event of overheating problems, refer to the sequence below.

Caution: Failure to ensure a free air flow around the unit may cause overheating.

Fan fault-finding

1. Check fan rotation.
   - Inspect the fans located at the sides of the unit. Are the fans rotating?

     Yes
     : Check that the unit has been installed with sufficient space allowed enclosure for air flow. If the air is too hot, additional cooling may be required

     No
     : Possible break in the DC supply from the PSU module to the suspect fan(s). Call a Service Engineer.

10.3 Disposing of this equipment

Dispose of this equipment safely at the end of its life time. Local codes and/or environmental restrictions may affect its disposal. Regulations, policies and/or environmental restrictions differ throughout the world; please contact your local jurisdiction or local authority for specific advice on disposal.

10.4 Returning the unit

Before shipping the Virtuoso to Nevion, contact your local Nevion reseller or Nevion directly for additional advice.

1. Write the following information on a tag and attach it to the Virtuoso.
   - Name and address of the owner
   - Model number
   - Serial number
   - Description of service required or failure indication.
2. Package the Virtuoso.
   - The original shipping containers or other adequate packing containers must be be used.
3. Seal the shipping container securely, and mark it FRAGILE.

Appendix A Glossary

1000Base-T
: The term for the electrical Gigabit Ethernet interface. This is the most common interface for Gigabit Ethernet. Most Gigabit-enabled PCs and equipment support this interface.

3G-SDI
: 3Gbit High Definition - Serial Digital Interface. 3G-SDI, consisting of a single 2.970 Gbit/s serial link, is standardized in SMPTE 424M that can replace the dual link HD-SDI.

ARP
: Address Resolution Protocol. A protocol used to "resolve" IP addresses into underlying Ethernet MAC addresses.

ATSC
: Advanced Television Systems Committee. An American organisation working with standardisation of digital television broadcasts, primarily in the US but also in Asia and other parts of the world.

DiffServ
: Differentiated Services. A mechanism used on layer 3 - e.g. the IP layer - to differentiate between traffic of various types. DiffServ is based on the ToS field and provides a mechanism for the network to give e.g. video traffic higher priority than other traffic (for example Internet traffic).

DVB
: Digital Video Broadcasting. The European consortium defining standards for transmission of digital TV broadcasts, primarily in Europe.

DVB ASI
: Digital Video Broadcasting Asynchronous Serial Interface. A common physical interface for transmission of MPEG2 Transport Streams (i.e. MPEG2-compressed video) over a serial interface, typically coaxial cables.

DWDM
: Dense Wavelength Division Multiplexing. A mechanism to increase the bandwidth available in an optical fiber by adding extra signals using different optical wavelengths (colours).

Ethernet
: Originally a 10 Mbit/s shared medium network type developed by Xerox. Later transformed into an official standard. Nowadays, most Ethernet networks are based on full duplex connections over twisted pair cables. Ethernet switches in the network take care of routing Ethernet frames between nodes. The speeds now supported are 10 Mbit/s, 100 Mbit/s and 1000 Mbit/s. 10Gigabit/s Ethernet networks are now emerging.

FEC
: Forward Error Correction. A mechanism to protect data transmission by adding redundant information. Increasing the amount of redundant data will enable the receiver to correct more errors (i.e. regenerate lost packets) in case of network data loss.

HD-SDI
: High Definition - Serial Digital Interface. Also known as ANSI/SMPTE SMPTE 292M-1998. A specification describing how to digitize and transmit uncompressed high definition video signals. The typical bit rate of an HD-SDI signal is 1485 Mbit/s.

HDTV
: High Definition Television. Television standard(s) that provide(s) improved picture resolution, horisontally and vertically, giving clearer and more detailed TV pictures.

HTTP
: HyperText Transfer Protocol. The fundamental protocol used on the Internet for transmission of WEB pages and other data between servers and PCs.

ICMP
: Internet Control Message Protocol. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation.

IGMP
: Internet Group Management Protocol. IGMP is a protocol used to manage multicast on the Internet. For a host (receiver unit) to receive a multicast, it needs to transmit IGMP "join" messages in the right format. Three versions exist. IGMPv2 is commonly used today, but IGMPv3 is the next step.

JPEG2000
: A wavelet-based image compression standard. It was created by the Joint Photographic Experts Group committee with the intention to supersede their original discrete cosine transform-based JPEG standard. JPEG2000 can operate at higher compression ratios without generating the characteristic 'blocky and blurry' artifacts of the original DCT-based JPEG standard.

Meta-data
: Meta-data is descriptive data that is "tagged" to a movie or audio clip. Meta-data is essential for the broadcaster.

MPEG-2
: Moving Picture Experts Group 2. The compression standard used today on most satellite and cable TV digital broadcasts. MPEG-2 also includes standardisation of data transport of video using other compression techniques, and other types of information.

MPLS
: Multi-protocol Label Switching. A Quality of Service mechanism for IP networks that allows IP packets to flow along a predefined path in a network, improving the reliability and robustness of the transmission.

MPTS
: Multi Program Transport Stream. MPEG2 transport stream that carry multiple TV/Radio services.

Multicast
: An IP mechanism that allows transmission of data to multiple receivers. A multicast can also have several transmit sources simultaneously. In video applications, multicast is typically used to distribute a video signal from a central source to multiple destinations.

MXF
: Material eXchange Format is a container format for professional digital video and audio media defined by a set of SMPTE standards.

NMS
: Network Management System. A system used to supervise elements in an IP network. When a device reports an alarm, the alarm will be collected by the NMS and reported to the operator. NMS systems typically collect valuable statistics information about the network performance and can provide early warning to the operator of network issues.

PCR
: Program Clock Reference. A sampled 27 MHz video clock used in MPEG2 Transport Streams. The primary purpose of the PCR is clock synchronisation of transmitter and receivers.

PID
: Packet Identifier. An 11 bit field in an MPEG2 transport packet defining a logical channel. 8192 unique logical channels may coexist in one network.

PSI/SI
: Program Specific Information / Service Information. These are information tables (metadata) carried in MPEG2 transport streams in addition to video and audio. The information carried is typically service/program IDs, program names and conditional access information.

QAM
: Quadrature Amplitude Modulation. A digital modulation type that is used for transmission of digital TV signals over cable networks (e.g. DVB-C) or terrestrial networks (e.g. DVB-T).

QoS
: Quality of Service. A common term for a set of parameters describing the quality of an IP network: Throughput, availability, delay, jitter and packet loss.

QPSK
: Quadrature Phase-Shift Keying. A modulation type frequently used for transmission of digital TV signals.

RIP2
: Routing Information Protocol v2. A protocol used between network routers to exchange routing tables and information.

RSVP
: ReSerVation Protocol. A Quality-of-service oriented protocol used by network elements to reserve capacity in an IP network before a transmission session takes place.

RTP
: Real-time Transfer Protocol. A protocol designed for transmission of real-time data like video and audio over IP networks.

SD-SDI
: Standard Definition Serial Digital Interface. Also known as ANSI/SMPTE 259M-1997 or ITU-R BT.656. A specification describing how to digitize and transmit uncompressed standard definition video signals. The typical bit rate of an SD-SDI signal is 270Mbit/s.

SDI
: Serial Digital Interface. Used to describe both HD-SDI and SD-SDI input and output ports.

SDP
: Session Description Protocol. A protocol describing multimedia communication sessions for the purposes of session announcement, session invitation, and parameter negotiation. SDP is typically used to describe an ongoing multicast; for example the type of compression used, IP addresses etc.

SDTI
: Serial Data Transport Interface. A mechanism that allows transmission of various types of data over an SDI signal. This may be one or more compressed video signals or other proprietary data types. The advantage of SDTI is that existing SDI transmission infrastructure can be used to transport other types of data.

SDTV
: Standard Definition Television. The normal television standard/resolution in use today.

SFP
: Small Form-factor Pluggable module. A standardized mechanism to allow usage of various electrical or optical interfaces to provide Gigabit Ethernet. Several types of SFP modules exist: Single mode fiber modules for long-distance transmission and multi mode fiber modules for shorter distances. SFP is also known as “mini-GBIC”.

SIP
: Session Initiation Protocol. The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, used for controlling multimedia communication sessions such as voice and video calls over IP. The protocol can be used to create, modify and terminate unicast or multicast sessions consisting of one or several media streams.

SNDU
: Sub Network Data Unit. Protocol Data Units (PDUs), such as Ethernet Frames, IP datagrams, or other network-layer packets used for transmission over an MPEG-2 Transport Multiplex, are passed to an Encapsulator. This formats each PDU into an SNDU by adding an encapsulation header and an integrity check trailer. The SNDUs are fragmented into one or a series of MPEG-2 Transport Stream (TS) packets and sent over a single TS logical channel.

SNMP
: Simple Network Management Protocol. A fundamental and simple protocol for management of network elements. Commonly used by Network Management Systems and other applications.

SNTP
: Simple Network Time Protocol is an Internet protocol used to synchronize the system clocks of computers to a time reference. It is a simplified version of the protocol NTP protocol which is overcomplicated for many applications.

SPTS
: Single Program Transport Stream. MPEG2 Transport Stream that contains a single program/service.

TCP
: Transmission Control Protocol. A "reliable" protocol above the IP layer that provides automatic retransmission of datagrams in case of packet loss, making it very robust and tolerant against network errors. TCP is the fundamental protocol used in the Internet for WEB traffic (HTTP protocol). TCP is indented for point-to-point communication; TCP cannot be used for communication from one node to many others.

TCP/IP
: A common term used for the Internet protocol suite, i.e. the set of protocols needed for fundamental IP network access: TCP, IP, UDP, ARP etc.

ToS
: Type of Service. This is a field in the header of IP datagrams to provide various service types. It has now been "taken over" and reused by DiffServ.

Transport Stream (TS)
: The common name for an MPEG2 Transport Stream. A bit stream used to carry a multiplex of packets, each identified by a unique Packet Identifier (PID) defining a logical channel. A PID stream typically represents a video or an audio service.

UDP
: User Datagram Protocol. An "unreliable" protocol above the IP layer that also provides port multiplexing. UDP allows transmission of IP data packets to several receiving processes in the same unit/device. UDP is used in multicast applications.

Unicast
: Point-to-point connection. In this mode, a transmit node sends e.g. video data direct to a unique destination address.

VLAN
: Virtual Local Area Network, a network of units that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN.

Watermarking
: A mechanism to "stamp" video content with unique marks, making it possible to trace the origin of illegaly distributed content. Watermarks are invisible to the viewer.

XML
: eXtensible Markup Language. A common self-describing text-based data format. Used for many purposes: Meta-data, configuration files, documents, etc. The readability of the format has made it very popular and is now the basis of many types of WEB services.

Appendix B Technical Specification

B.1 Physical details

B.1.1 Full-width version

Height	43 mm, 1U
Width	448 mm excluding fixing brackets
Overall width	485 mm including fixing brackets
Depth	424 mm excluding connectors
Overall depth	443 mm including connectors
Approximate weight	6.5 kg (Fixed) or 7.5 kg (Modular)
Rack-mount case	19 inch width, 1 U height

B.2 Environmental conditions

Table B.1 Environmental specification

Operating temperature	0 to +50 °C
Storage temperature	-20 to +70 °C
Relative humidity	5 % to 95 % (non-condensing)
Handling/movement	Designed for fixed use when in operation

B.3 Power

B.3.1 AC Mains supply

Table B.2 AC Power Supply Specification

Chassis type	Fixed	Modular
Rated voltage	100-260 VAC	100-260 VAC
Rated frequency	50/60 Hz	50/60Hz
Rated current	2.0 A	3.3A
Max nominal power consumption	156 W	300W

B.4 Input/output ports

B.4.1 HD-SDI port

Table B.3 HD-SDI Port Specification

Type	[L] HD-SDI, Coaxial cable
Connector type	BNC 75 Ω socket
Signal	Compliant with ANSI/SMPTE (292M-1998)
Line rate	1,5 Gbit/s
Max cable length (Belden 1694A)	160m
Safety status (UK)	SELV

B.4.2 DVB ASI port

Table B.4 ASI Port Specification

Type	ASI-C, Coaxial cable
Connector type	BNC 75 Ω socket
Signal	Compliant with ETSI EN 50083-9 (DVB A010 rev.1)
Line rate	270 Mbit/s +/- 100 ppm
Data rate	0.1 - 213 Mbit/s
Packet length	188 or 204 bytes
Max cable length (Belden 8281 type)	300 m typical

B.4.3 Ethernet ports

Table B.5 Ethernet Port Specification

Type	10/100/1000Base-T Ethernet
Connector type	RJ45

B.4.4 SFP+ Ethernet ports

Table B.6 Ethernet SFP+ Port Specification

Type	10 Gigabit Ethernet
Connector type	Enhanced Small Form-Factor Pluggable (SFP+) slot to carry copper or optical SFP+, compatible with approved modules conforming to the Specification for Enhanced Small Form Factor Pluggable Module SFP+ (July. 6 2009).

B.4.5 Serial USB interface

Table B.7 USB port specification

Type	USB 1.1
Compatibility	Compatible with USB 2.0
Connector type	Mini USB Connector

B.5 Alarm ports

B.5.1 Alarm relay/reset port specification

Table B.8 Alarm Relay and Reset Port Specification

Connector type	9-pin D-sub Male
Relay rating	0.1 A max, 50 VDC max
Relay minimum load	10 μA at 10 mVDC
Reset activation time	8 seconds

Table B.9 Alarm Relay and Reset Port Pin Out

PIN	Connection
1	Relay 2 - Closed on alarm (NC)
2	Relay 2 Common
3	Relay 2 - Open on alarm (NO)
4	Prepared for +5 V Output
5	Ground
6	Alarm Relay - Closed on alarm (NC)
7	Alarm Relay Common
8	Alarm Relay - Open on alarm (NO)
9	Optional Reset Input

B.6 Compliance

B.6.1 Safety

The equipment has been designed to meet the following safety requirements: **Table B.10**.

Table B.10 Safety requirements met.

EN60950 (European)	Safety of information technology equipment including business equipment.
IEC 60950 (International)	Safety of information technology equipment including business equipment.
UL 1950 (USA)	Safety of information technology equipment including business equipment.

B.6.2 Electromagnetic compatibility - EMC

The equipment has been designed to meet the following EMC requirements:

EN 55022 and AS/NZS 3548 (European, Australian and New Zealand)
: Emission Standards Limits and methods of measurement of radio frequency interference characteristics of information technology equipment - Class A.

EN 61000-3-2 (European)
: Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

EN 50082-1 (European)
: Generic Immunity Standard Part 1: Domestic, commercial and light industry environment.

FCC (USA)
: Conducted and radiated emission limits for a Class A digital device, pursuant to the Code of Federal Regulations (CFR) Title 47-Telecommunications, Part 15: radio frequency devices, sub part B -Unintentional Radiators.

B.6.3 CE marking

The CE mark indicates compliance with the following directives:

89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility.

73/23/EEC of 19 February 1973 on the harmonisation of the laws of the Member States relating to electrical equipment designed for the use within certain voltage limits.

1999/5/EC of March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity.

B.6.4 Interface to “public telecommunication system”

The equipment is not constructed for electrical connection directly to a “public telecommunication system”. None of the signals shall be connected directly from the unit to a “public telecommunication system” leaving the building without using some kind of interface in between such as a telecom terminal, switch or similar unit. Such kind of buffer is required to achieve a protective electrical barrier between the “public telecommunication system” and the unit. This electrical barrier is required to achieve protection against lightening or faults in nearby electrical installations.

Appendix C Forward Error Correction in IP Networks

The normal operational mode of the public internet is that IP packets are forwarded using a "best effort" strategy implying that packets may occasionally be lost due to excessive load. To regulate the transport rate of an IP session a transmitting host will at session start ramp up the speed until the receiver starts to loose packets. The receiver will send acknowledgments as it receives packets. In the case of packet loss the source will re-transmit a packet and slow down transmission rate to a level where packets are no longer lost. This is inherent in the commonly used protocol TCP (Transmission Control Protocol).

In an IP network for broadcast signals however, this mode of operation becomes impractical since packet delay from source to receiver resulting from re-transmission amounts to three times the normal. It is also impractical for multicast as each individual receiver would need to request re-transmissions, which in itself inflicts a bandwidth increase in a channel at the edge of overflow. Accordingly, all broadcast related IP traffic use UDP (User Datagram Protocol). Here no retransmission is included, which means that all data must be delivered in a safe manner at first attempt.

C.1 IP stream distortion

Distortions that influence the performance of an IP video transport system, in addition to packet loss, are packet delivery time variations (jitter), and packets arriving out of order. It should be noted that a single bit error occurring within an IP packet will result in the loss of the complete packet. As IP packets and Ethernet physical link layers normally go hand in hand, IP packets will be discarded if a single bit error occurs in transmission. The Ethernet link layer is secured with a cyclic redundancy check (CRC). An Ethernet frame with bit error(s) will be discarded by the first IP switch or router because the CRC check fails.

Furthermore, multiple packets may be lost during short periods due to congestion. As an IP packet contains close to 1500 bytes, or about 5% of a video frame for a video stream running at 5 Mbit/s, a lost IP packet will result in visible impairments.

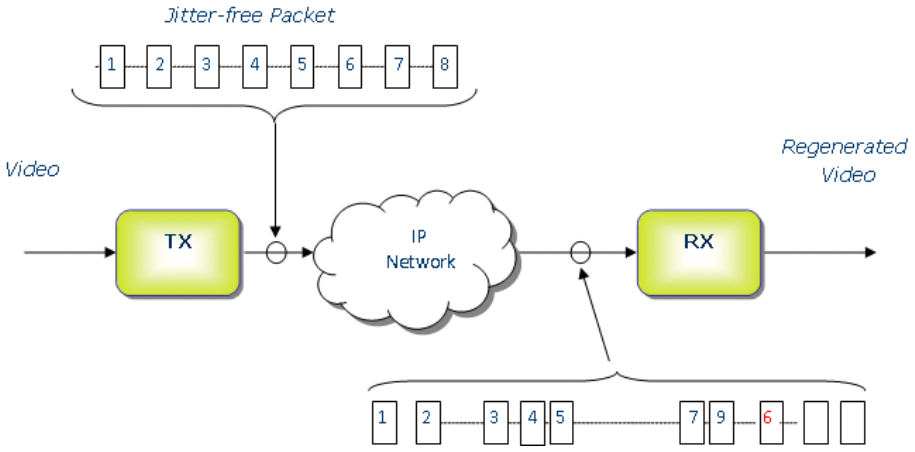


Figure C.1 Impairments of an IP packet stream

In **Figure C.1** distortions of an IP stream are visualised. The even stream of packets originating from the Tx node is modified in traversing the IP network. At the input of the Rx node the IP stream is distorted in the following ways:

- The packet spacing is no longer even
- The position of packet #6 has been shifted
- Packet #8 is missing

A properly designed IP node will handle the first two within certain limits; the input buffer size will determine the amount of jitter that can be tolerated and the time to wait for a delayed or out-of-order packet before it is deemed lost. Lost packets, however, are not recoverable unless special measures are taken.

C.2 Standardisation

All since streaming of broadcast services in IP networks began the insufficient reliability of IP links has been an issue, and methods to improve performance have been devised. Due to lack of standardisation many proprietary implementations and different solutions have been put into use by equipment manufacturers. The PRO-MPEG organisation has taken the initiative to achieve a common standard for transport of video over IP. These have been published as Code of Practice (COP) #3 and #4. COP#3 considers compressed video in the form of MPEG-2 Transport Stream, while COP#4 considers uncompressed video at 270Mbit/s and higher. The IP protocol stack proposed is RTP/UDP/IP. This work has been taken over by the Video Services Forum (VSF) (`http://www.videoservicesforum.org`). VSF has in cooperation with SMPTE successfully brought the COP#3 and COP#4 further and COP#3 is now finalised as SMPTE 2022-1 **[9]** and 2022-2 **[8]**. SMPTE 2022-1 focuses on improving IP packet loss ratio (PLR) performance using forward error correction techniques.

C.3 FEC matrix

SMPTE 2022-1 specifies a forward error scheme based on the insertion of additional data containing the result of an XOR-operation of packet content across a time window. By reversing the operation it is possible to reconstruct single lost packets or a burst of lost packets. The degree of protection may be selected to cover a wide range of link quality from low to heavy loss at the expense of increased overhead and delay.

SMPTE 2022-2 specifies use of RTP protocols and hence all packets have a sequence number. Thus, a receiver will be able to determine if a packet has been lost. There should be no cases of packets arriving containing bit errors as packets with checksum errors are discarded at the Ethernet layer. A FEC packet containing a simple XOR-sum carried out over a number of packets at the transmitter allows the receiver to compute one lost packet by redoing the XOR process over the same packets and comparing the results with the XOR FEC packet. This allows for the regeneration of one lost packet in an ensemble of N payload packets plus one FEC packet. If two or more packets in the ensemble are lost it is not possible to regenerate any of them. Packet loss in IP systems have a tendency to come in bursts (due to congestion). Therefore the FEC XOR calculation is not done on adjacent packets; rather packets at a fixed distance are used. This can be visualised by arranging the packets in a two dimensional array and inserting them in rows in the same order as they are transmitted.

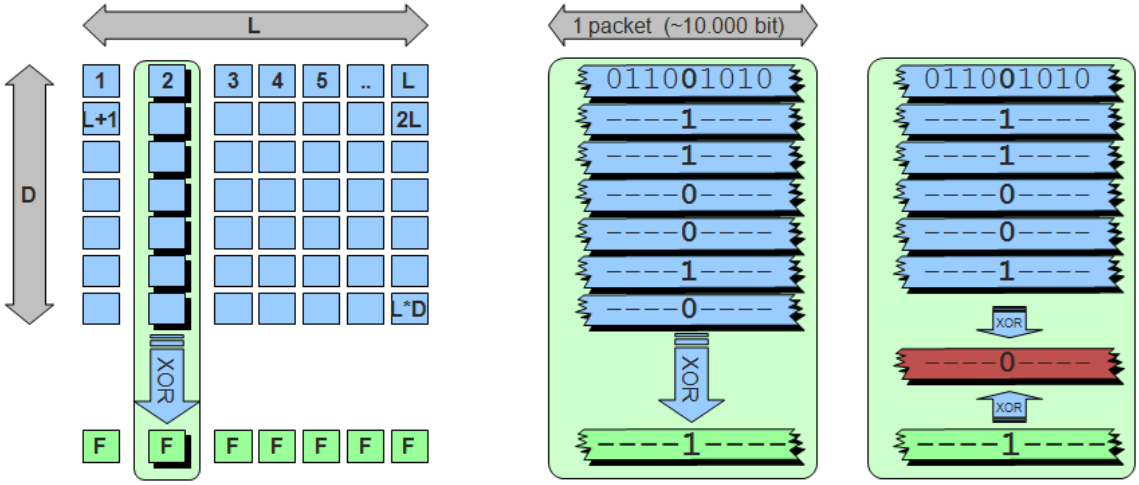


Figure C.2 IP packet FEC calculation matrix

Figure C.2 shows LxD consecutive IP packets arranged in a matrix. The FEC checksum is calculated over the columns, which means that the distance between two packets used in an XOR calculation is L. An XOR sum is calculated for each *bit position* of all the packets of a column. The checksums for all bit positions constitute the FEC checksum, and is inserted in a FEC packet which is sent in addition to the payload packets. There will be one FEC packet associated with each column, and it is therefore possible to regenerate as many packets as there are columns in the matrix.

In the right-most panel of **Figure C.2** the case is shown where a packet in the last column position has been lost. The packet may then be regenerated (shown in red) by performing XOR addition over all remaining packets in that column, including the FEC packet. This is the default FEC mode of SMPTE 2022-1.

However, it is not possible to correct more than one error in a column. To increase the error correction capability the specification gives the option to also include FEC over the rows. By combining the two FEC calculations it is now possible to handle more complex packet loss distribution patterns and correct up to L+D lost packets.

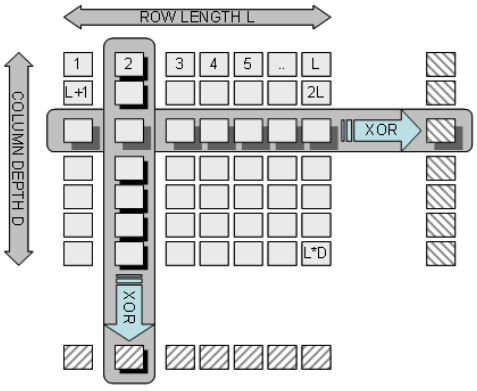


Figure C.3 Two-dimensional FEC calculation matrix

Figure C.3 shows this arrangement. Here, checksums are also calculated for the packets in each row. This gives rise to another D FEC packets, which again means increased overhead.

A drawback with a rectangular matrix arrangement is that all column-FEC packets need to be transmitted at nearly the same time as all column-FEC packets are generated when the last row of the matrix is being completed. Thus when transmitting the last row of payload packets the packet rate must be doubled in order to also send the FEC packets without generating extra payload packet delay. In itself this may cause temporary network overload with packet loss as a result. The specification [9] imposes some rules how FEC packets should be interleaved with payload packets to avoid excessive jitter and ensuring compatibility between equipment from different manufacturers. One method is to offset the FEC columns, one example is shown in Figure C.4, which also provides additional advantages.

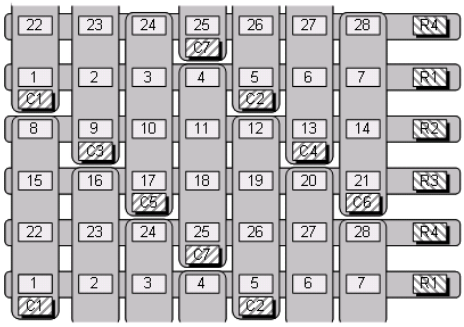


Figure C.4 FEC matrix with column offset

Column offset leads to column FEC packets being generated at a more regular rate and it is possible to transmit packets with a shorter delay than with a rectangular matrix. Offsetting the columns also increases the capability to regenerate longer bursts of lost packets; the length depending on the column and row length ratio.

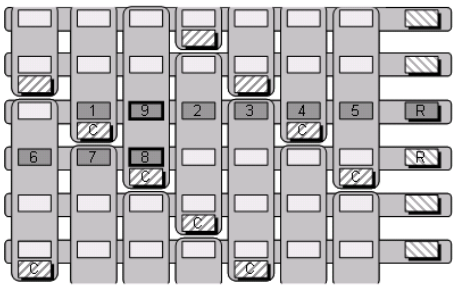


Figure C.5 Offset FEC matrix with missing packets

Figure C.5 shows an offset matrix with missing packets. The numbered items indicates packets lost. The figure shows that column offset may increase the capability to correct longer bursts of lost packets. In this example 9 consecutive packets are lost. Even if the row length is only 7 packets, all the 9 lost packets are reconstructed. The packets are numbered in the order they can be recovered. Packets marked 8 and 9 are protected by the same column FEC packet and are recovered by the row FEC packets after recovery of packets 1 through 7.

If more than one packet is lost in a row or a column of a matrix, the possibility to recover it depends on packet location. **Figure C.6** shows this.

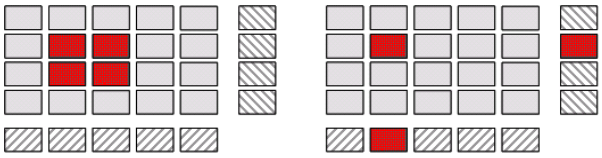


Figure C.6 Uncorrectable error patterns

The red-coloured packets are lost in transmission. The pattern to the left normally results in 4 unrecoverable payload packets. However, if two of the lost packets are FEC packets, then only 2 payload packets will be lost. The pattern to the right will result in one lost payload packet.

The specifications allow several parameter combinations for the FEC stream generation. The FEC matrix sizes can in principle be chosen at will to suit the operational conditions. Operators may easily be confused by the number of options, and it is not straightforward to choose the optimal FEC setting for a given scenario. For compatibility reasons SMPTE 2022-1 specifies that an MPEG-2 to IP network adapter should handle a minimum matrix size of 100 IP packets, and that row length or column depth should not exceed 20. Also the shortest column length allowed is 4.

C.4 Transmission aspects

The RTP protocol must be used if FEC shall be added to the IP payload. In order to provide compatibility between equipment handling application layer FEC and equipment without that capability FEC data is transmitted using UDP port numbers different from that of the payload. Column FEC is transmitted using port number (IP payload) + 2 and row FEC (if used) is transmitted using port number (IP payload) + 4.

Introducing FEC for the IP connection obviously leads to additional data overhead and consequently a higher demand on data capacity. The generated FEC packets need to be "squeezed" in between the payload packets, which will tend to increase the packet jitter experienced by the receiver. Notably, in a rectangular matrix all column-FEC packets are generated and inserted into the stream in succession. This leads to a short burst of packets in quick succession, or a considerable delay before the first packet of the next FEC frame can be transmitted (or indeed, some of each).

Figure C.7 illustrates the relative timing of FEC packets and payload packets. Applying an offset column structure results in a smoother packet stream. The overall packet rate will be the same in both schemes, since the same number of FEC packets are generated, but the packets will be more evenly spread in the IP stream. With larger matrix sizes the smoothing effect of an offset matrix will even more pronounced. The effect of added overhead and jitter should be considered when applying FEC to an IP video stream in a heavily loaded network. High instantaneous packet rates may cause temporary overload resulting in packet loss, defeating the object of introducing FEC in the first place.

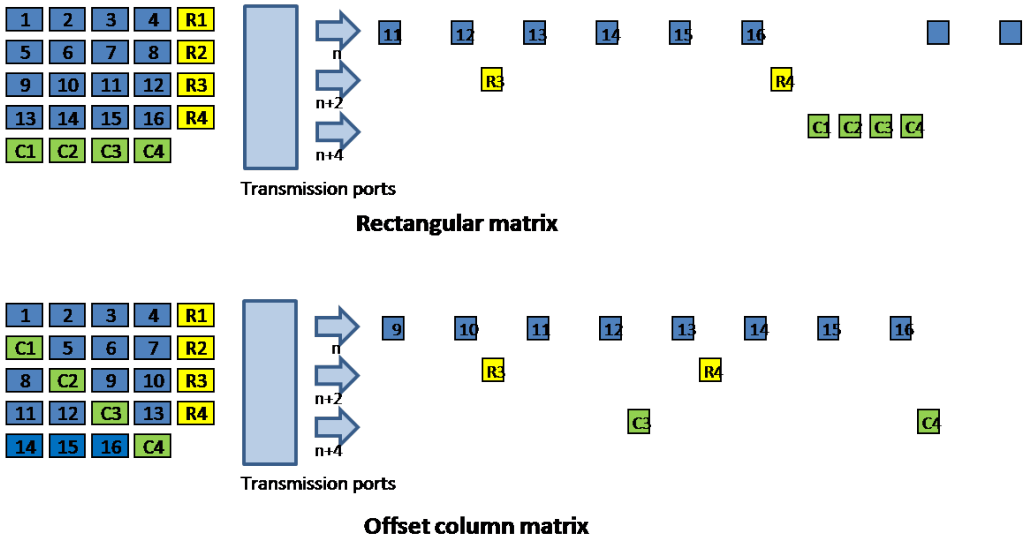


Figure C.7 FEC data transmission

C.5 Quality of service and packet loss in IP networks

One may ask how the FEC strategy relates to an operational IP network. Little information is available on packet loss patterns. Measurements show that up to 1% of the packets are duplicates and generated as a result of a retransmission request. Either because the packet has been lost or it has arrived too late. However, since these results are for TCP connections they merely serve to indicate an upper level for packet loss rate in an IP/MPLS network. Reported jitter measurements indicate that 0.01% of the packets were delayed more than 31ms and a fraction of those packets were delayed more than 100ms. This is also relevant for transmission of video as out-of-order packets arriving too late will be regarded as lost and must, if possible, be regenerated by FEC.

There are three main factors that cause packet loss:

- Occasional bit errors in the Ethernet frame caused by low noise margin or equipment fault
- Buffer overflow or packet delay caused by network congestion
- Packet re-routing, to circumvent a node breakdown or network bottlenecks

Some of the packets will arrive late. IP packet latency will vary as a result of variable traffic load on the network. Packets that do not arrive in time will be handled as lost packets. The FEC process will thus be able to handle occasional delay increase for a few packets and maintain a satisfactory Quality of Service. A video gateway should offer a setting for permissible packet delay, which should be optimised for the operation. If the receiver buffer latency is increased it is possible to reduce the FEC overhead and still get an error-free video link.

The Packet Loss Ratio (PLR) for an IP network is not a given number. Performance figures are normally in the order of 1×10^{-6}, but occasionally a link may become degraded showing PLR figures like 3×10^{-3}. The performance will vary over the day with the lowest performance tending to occur at about the same time every weekday and lasting for one-half to one hour. The FEC setting should be set up to handle this peak hour with low residual loss.

The table of **Figure C.8** shows the IP network performance figures to meet the quality requirements of various grades of television services, as given by ITU recommendation Y.1541 **[10]**. Along these lines the DVB IPTV standard sets the performance requirement for a 4Mbit/s IPTV service at 1 visible error per hour, which means an IP packet loss ratio of $1x10^{-6}$.

Profile (Typical bit rate)	One performance hit per 10 days	One performance hit per day	10 performance hits per day
Contribution (270 Mbit/s)	4×10^{-11}	4×10^{-10}	4×10^{-9}
Primary Distribution (40 Mbit/s)	3×10^{-10}	3×10^{-9}	3×10^{-8}
Access Distribution (3 Mbit/s)	4×10^{-9}	4×10^{-8}	4×10^{-7}

Figure C.8 Recommended error performance (as per ITU)

C.6 Error improvement

So, what does it take to make FEC improve the packet error rate of an IP network link to a level acceptable for the application? Assuming packet loss occurs at random **Figure C.9** shows how the depth of a one-dimensional FEC matrix affects the error correcting capability.

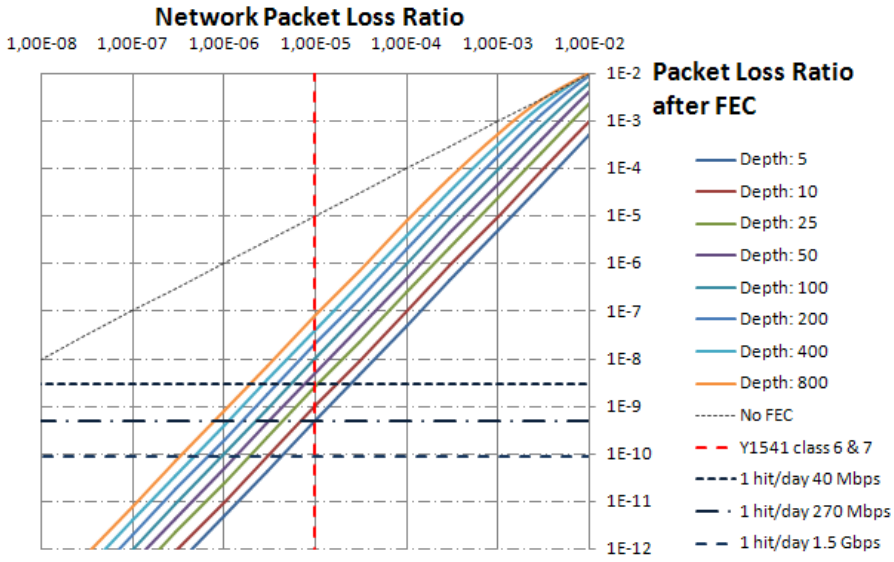


Figure C.9 Error improvement using column FEC only

It is evident that the smaller the column depth the better error correcting capability. At a network packet loss rate of 10^{-5} adding FEC will provide up to 4 magnitudes of improved error performance.

For ease of reference the diagram indicates packet loss rates resulting in one visible impairment (error hit) per day at transport stream bit rates of 40Mb/s, 270Mb/s and 1,5Gb/s, respectively. It can be seen that in a network with worst hour packet loss rate of $3x10^{-3}$ it is not possible to provide distribution of a 3Mb/s transport stream with less than 10 hits per day (i.e. packet loss

rate of $4x10^{-7}$, as recommended in **Figure C.8**) using column-only FEC. In IP networks of ITU class 6 and 7 however, column-only FEC with reasonably small column depths will perform nicely for bit rates up to 270Mb/s.

Distributing video transport streams over high packet loss rate networks demand use of two-dimensional FEC. As explained earlier this increases the added overhead and thus the required network bandwidth.

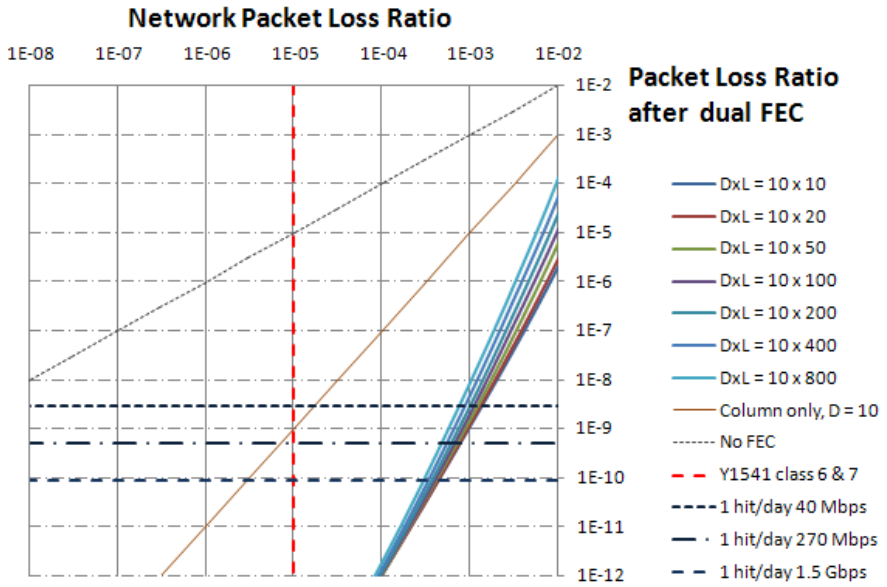


Figure C.10 Error improvement using two-dimensional FEC

Figure C.10 shows how adding row FEC dramatically increases performance in high packet loss networks. Reverting to the previous case, a 3Mbit/s video transport stream in an IP network with worst hour PLR of $3x10^{-3}$, a service with less than 10 error hits per day may be provided using any of the matrix sizes shown. In less error-prone networks however, using two-dimensional FEC schemes may be overkill and generate unnecessary FEC overhead.

C.7 Latency and overhead

Latency is increased when FEC is applied. The latency that can be accepted in a particular application may vary, and should be considered when setting FEC parameters.

FEC packet calculation in the transmitter is done on-the-fly and adds little to the latency. In a rectangular matrix, however, all FEC packets are generated nearly at the same time, as indicated in **Figure C.7**. FEC packets should be spread in transmission to avoid introducing extra jitter. This also contributes to latency in error packet recovery. In the receiver all packets involved in the FEC calculation must be collected before a missing packet can be recovered. **Figure C.11** shows how different matrix sizes result in different latencies and required buffer sizes, using column-only FEC processing.

	Overhead	Latency			Recovery	Buffer size
		3Mbps	30 Mbps	100 Mbps		
XOR (5,10)	10%	175.5 ms	17.5 ms	5.3 ms	5 IP packets	66400 Bytes
XOR (10,10)	10%	350.9 ms	35.1 ms	10.5 ms	10 IP packets	132800 Bytes
XOR (20,5)	20%	350.9 ms	35.1 ms	10.5 ms	20 IP packets	132800 Bytes
XOR (8,8)	12.5%	224.6 ms	22.5 ms	6.7 ms	8 IP packets	84992 Bytes
XOR (10,5)	20%	175.5 ms	17.5 ms	5.3 ms	10 IP packets	66400 Bytes
XOR (8,5)	20%	140.4 ms	14.0 ms	4.2 ms	8 IP packets	53120 Bytes
XOR (5,5)	20%	87.7 ms	8.8 ms	2.7 ms	5 IP packets	33200 Bytes
XOR (4,6)	16.7%	84.2 ms	8.4 ms	2.5 ms	4 IP packets	31872 Bytes
XOR (6,4)	25%	84.2 ms	8.4 ms	2.5 ms	6 IP packets	31872 Bytes

Figure C.11 FEC latency and buffer size

Also shown is the resulting overhead and the number of packets that can be corrected. In column-only FEC there is one FEC packet per column, resulting in a 1/D increase in transmission overhead, D being the matrix column depth. I.e. in a 10 row matrix (D=10) the added overhead is 10%. The minimum allowable column depth of 4 will produce 25% overhead.

In two-dimensional FEC there will be D+L FEC packets in a DxL matrix (L being the row length). Thus the added overhead is D+L/DxL, which for a 10 by 10 matrix amounts to 20%.

Adding row-FEC will increase the error correcting capability without significantly increasing the latency or buffer size requirement. Applying row- and column-FEC also enables use of iterative FEC calculations to recover more missing packets. The equipment manufacturer is at liberty to determine the algorithm used in error recovery as long as the requirements and limitations of the specification are respected.

Appendix D Alarms

The Virtuoso indicates alarm or failure status to the user in four ways:

- WEB interface
- Alarm LED on the front and on the rear
- SNMP trap messages to Network Management System
- Alarm relay

The user can define the severity level of the different alarm events. There are five levels, and each level is also indicated by a colour on the alarm severity indicator:

Table D.1 Alarm severity levels

Severity	Level	Colour
Notification	2	Blue
Warning	3	Yellow
Minor	4	Amber
Major	5	Orange
Critical	6	Red

In addition it is possible to set an alarm to filtered, so that there will be no alarm events generated for this alarm.

The WEB interface gives the most detailed alarm information as all active alarms and warnings are listed with time of occurrence

The unit sends an SNMP trap message to all registered trap receivers when an alarm condition arises. A critical alarm will have severity level 6 and a Notification will have severity level 2. When the alarm is cleared, a new message is sent to indicate that the alarm condition is cleared.

Finally, the red alarm LED will be lit when an unmasked critical alarm condition arises. At the same time the alarm relay will be set to alarm state.

Table D.3 shows the possible alarms that can be signalled by the Virtuoso. For each alarm type, essential information is presented. The different fields are described in **Table D.2**.

Table D.2 Fields in the alarm description table

Field	Description
Alarm ID	Unique identifier (number) for this alarm. There are no duplicates in the table, e.g. a specific alarm number always maps to a specific alarm.
Text	A short text describing the alarm
Description	A longer text describing the cause of the alarm
Def. severity	The default severity of the alarm
Type	Alarms are grouped together into different *types*. This field contains a textual description of the type.
Type ID	Each alarm type has a corresponding number (ID).
Clear event	Set to *Yes* if an "off/cleared" alarm is expected after an "asserted" alarm. In most cases the value is *Yes*. For "stateless" alarms, e.g. the event that a user has logged into the system, no explicit clear events are expected.
Subid2	This field is present if the `Subid2` value of the alarm type is used. The text in the table describes the usage of the `Subid2` value.
Subid3	This field is present if the `Subid3` value of the alarm type is used. The text in the table describes the usage of the `Subid3` value.

Table D.3.a Alarms

Alarm ID	Text	Def. severity	Details	
106	Unable to transmit	Critical	*Description:*	Channel not able to transmit any data, or only part of the data is transmitted.
			Type:	Port
			Clear event:	Yes
			Subid3:	"IP Dest"
130	Ethernet link down	Critical	*Description:*	No link on Ethernet layer.
			Type:	Port
			Clear event:	Yes
133	Generic SFP alarm	Critical	*Description:*	Generic SFP alarm for Mipot and SFF-8472 based modules.
			Type:	Undetermined
			Clear event:	Yes
140	IP address unresolved	Warning	*Description:*	IP address is not resolved into physical MAC address.
			Type:	Port
			Clear event:	Yes
			Subid3:	"IP Dest"
141	Waiting for source	Warning	*Description:*	Source is not available or does not have sync.
			Type:	Port
			Clear event:	Yes
142	Transmitting alternative signal	Warning	*Description:*	An alternative signal is transmitted instead of the source signal.
			Type:	Port
			Clear event:	Yes
143	Source format not supported	Major	*Description:*	The source signal format is not supported with the current mode/configuration/licences.
			Type:	Port
			Clear event:	Yes
144	Source bitrate too high	Major	*Description:*	The source signal bitrate is too high with the current mode/configuration.
			Type:	Port
			Clear event:	Yes
150	RTP sequence error	Warning	*Description:*	Network error. Analysis of the sequence number of the RTP layer indicates that IP frames have been lost or that they have been received out of order. The alarm details field shows the actual jumps in the RTP sequence number field.
			Type:	Port
			Clear event:	Yes
			Subid3:	"IP Flow"
151	No data received	Major	*Description:*	No data received on Ethernet input for stream. See details field on alarm for description.
			Type:	Port
			Clear event:	Yes
			Subid3:	"IP Flow"
154	Data lost	Critical	*Description:*	The data stream received for a channel is incomplete or packets were received out of order and the buffer was not large enough. Also, if running FEC, the FEC engine was not able to recover all the lost frames.
			Type:	Port
			Clear event:	Yes

Table D.3.b Alarms

Alarm ID	Text	Def. severity	Details
155	No lock	Critical	*Description:* The incoming packet stream is absent or incompatible with the expected format. *Type:* Port *Clear event:* Yes
157	Receive buffer too small for FEC	Warning	*Description:* The receive buffer size is set lower than the buffer required to fully utilize the current FEC. Increase Receive buffer size to resolve. *Type:* Port *Clear event:* Yes
161	Too high temperature	Warning	*Description:* Internal temperature of unit is too high. *Type:* System *Clear event:* Yes
162	Defective fan	Warning	*Description:* One or more fans are not spinning. *Type:* System *Clear event:* Yes
163	Time reference unreachable	Warning	*Description:* No selected timesources are OK. *Type:* System *Clear event:* Yes
165	Time source not OK	Note	*Description:* One or more time sources are not OK. *Type:* System *Clear event:* Yes
166	Time source switch	Note	*Description:* Device started using a new time source. *Type:* System *Clear event:* No
167	Time adjusted	Note	*Description:* The real time clock of the device was adjusted significantly. *Type:* System *Clear event:* No
168	Power failed	Warning	*Description:* One or more power supplies have failed, or are out of regulation. *Type:* System *Clear event:* Yes *Subid3:* "Power supply ID"
172	No reference sync	Critical	*Description:* There is no valid signal detected on the reference sync input. *Type:* Undetermined *Clear event:* Yes
173	No SDI sync	Critical	*Description:* No sync is detected on the SDI input. *Type:* Port *Clear event:* Yes
175	SDI resynced to reference	Critical	*Description:* The SDI output from the decoder was resynced due to a change in the ref. sync signal. *Type:* Undetermined *Clear event:* Yes
176	SDI reference format mismatch	Critical	*Description:* Decoder is unable to lock to reference sync due to mismatch between ref. sync format and decoded format *Type:* Undetermined *Clear event:* Yes

Table D.3.c Alarms

Alarm ID	Text	Def. severity	Details	
177	SDI checksum (EDH/CRC) error	Warning	*Description:*	SDI EDH/CRC error is detected on the SDI input, typically due to noisy signal.
			Type:	Port
			Clear event:	Yes
189	High PPM offset	Note	*Description:*	Frequency of SDI input is more than 10ppm different from system clock
			Type:	Port
			Clear event:	Yes
193	SDI input format mismatch	Critical	*Description:*	SDI input port is unable to process input signal due to mismatch between field rate of input format and system field rate mode.
			Type:	Port
			Clear event:	Yes
195	Black frames limit exceeded	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
196	Freeze frames limit exceeded	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
220	Time adjusted for DST	Note	*Description:*	Device local time adjusted due to daylight saving.
			Type:	System
			Clear event:	No
225	Clock ref. not locked	Critical	*Description:*	Unable to lock to external reference signal (1PPS, GPS etc.)
			Type:	System
			Clear event:	Yes
226	Clock ref. resynced	Critical	*Description:*	The clock reference mechanism has been resynchronized due to too large phase error
			Type:	System
			Clear event:	No
230	Template: Video format	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
231	Template: Audio channel missing	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
232	Template: Audio channel present	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
233	Template: Audio silence	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
255	Refsync not locked	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes

Table D.3.d Alarms

Alarm ID	Text	Def. severity	Details
256	Outputting generated signal	Warning	*Description:* The SDI output is outputting a generated signal *Type:* Undetermined *Clear event:* Yes
257	Waiting for input	Warning	*Description:* The SDI output is waiting for an input *Type:* Undetermined *Clear event:* Yes
258	SDI resynced to reference	Critical	*Description:* The SDI output was resynced due to a change in the ref. sync signal. *Type:* Undetermined *Clear event:* Yes
259	SDI reference format error	Critical	*Description:* SDI output is unable to lock to reference sync *Type:* Undetermined *Clear event:* Yes
302	Encoder input format not supported	Major	*Description:* The input format is not supported in the current encoder mode. *Type:* Undetermined *Clear event:* Yes
304	Encoding started	Note	*Description:* The encoder has started encoding. *Type:* Undetermined *Clear event:* No
306	Unexpected encoder error	Warning	*Description:* An unexpected internal error has occurred, causing the encoder to stop temporarily. *Type:* Undetermined *Clear event:* Yes
308	Encoding alternative signal	Warning	*Description:* The encoder is encoding an alternative signal instead of the SDI input signal. *Type:* Undetermined *Clear event:* Yes
309	Ancillary bitrate too low	Warning	*Description:* The current configured ancillary bitrate is too low for the ancillary data contained in the current input signal. *Type:* Undetermined *Clear event:* Yes
310	Waiting for valid input	Warning	*Description:* Encoder is waiting valid input video *Type:* Undetermined *Clear event:* Yes
311	Feature not licensed	Major	*Description:* Unable to encode since a feature or a function is not licensed *Type:* Undetermined *Clear event:* Yes
312	Co-processor error	Critical	*Description:* Unable to encode due to a issue with the co-processor *Type:* Undetermined *Clear event:* Yes
320	Decoder input format not supported	Major	*Description:* The input format is not supported in the current decoder configuration. *Type:* Undetermined *Clear event:* Yes

Table D.3.e Alarms

Alarm ID	Text	Def. severity	Details	
322	Decoding started	Note	*Description:*	The decoder has started decoding.
			Type:	Undetermined
			Clear event:	No
324	Unexpected decoder error	Warning	*Description:*	An unexpected internal error has occurred, causing the decoder to stop temporarily.
			Type:	Undetermined
			Clear event:	Yes
325	Decoder unable to decode	Critical	*Description:*	The decoder is unable to output continuous decoded video due to problems with the input stream.
			Type:	Undetermined
			Clear event:	Yes
327	Outputting generated signal	Warning	*Description:*	The decoder is outputting a generated signal instead of a decoded IP signal.
			Type:	Undetermined
			Clear event:	Yes
328	Waiting for input	Warning	*Description:*	The decoder is waiting for an input stream
			Type:	Undetermined
			Clear event:	Yes
329	Unable to decode audio	Warning	*Description:*	The decoder is unable to decode an audio stream
			Type:	Undetermined
			Clear event:	Yes
330	Feature not licensed	Major	*Description:*	Unable to decode since a feature or a function is not licensed
			Type:	Undetermined
			Clear event:	Yes
331	Freeze frame	Warning	*Description:*	Freeze frame detected
			Type:	Undetermined
			Clear event:	Yes
332	Black frame	Warning	*Description:*	Black frame detected
			Type:	Undetermined
			Clear event:	Yes
333	Template: Audio channel missing	Warning	*Description:*	
			Type:	Undetermined
			Clear event:	Yes
334	Template: Audio channel present	Warning	*Description:*	
			Type:	Undetermined
			Clear event:	Yes
335	Template: Audio silence	Warning	*Description:*	
			Type:	Undetermined
			Clear event:	Yes
350	No lock	Critical	*Description:*	Unable to lock to group
			Type:	Undetermined
			Clear event:	Yes
			Subid3:	"Decoder"

Table D.3.f Alarms

Alarm ID	Text	Def. severity	Details
400	Card mismatch	Critical	*Description:* The accepted card configuration differs from the detected card. *Type:* System *Clear event:* Yes *Subid3:* "Slot"
401	Card missing	Critical	*Description:* Could not find accepted card. *Type:* System *Clear event:* Yes *Subid3:* "Slot"
402	Card driver error	Critical	*Description:* Card driver error *Type:* System *Clear event:* Yes *Subid3:* "Slot"
403	Card version error	Critical	*Description:* Card version not supported *Type:* System *Clear event:* Yes *Subid3:* "Slot"
404	Insufficient power	Critical	*Description:* Insufficient power available to start card *Type:* System *Clear event:* Yes *Subid3:* "Slot"
501	User logged in	Note	*Description:* This event is generated when a user logs on to the system. *Type:* System *Clear event:* No
502	User logged out	Note	*Description:* This event is generated when a user logs out from the system. *Type:* System *Clear event:* No
503	System started	Note	*Description:* The system has booted. *Type:* System *Clear event:* No
504	Switch done	Note	*Description:* The input relay has switched position. *Type:* Undetermined *Clear event:* No
505	Config changed	Note	*Description:* A modification has been made to the configuration of the device. *Type:* System *Clear event:* No
506	Unable to switch	Major	*Description:* The relay controller is unable to switch because the spare input is not sufficiently good. *Type:* Undetermined *Clear event:* Yes
517	Alarm log cleared	Note	*Description:* Alarm log was cleared, user in details *Type:* System *Clear event:* No

Table D.3.g Alarms

Alarm ID	Text	Def. severity	Details
519	Forced reset initiated	Note	*Description:* A reset of the device was forced by the operator. *Type:* System *Clear event:* No
520	SW loading in progress	Note	*Description:* Loading of an embedded SW image is in progress *Type:* System *Clear event:* Yes
521	New SW pending	Note	*Description:* A SW image has been successfully loaded, but manual reboot is needed for SW to be activated. *Type:* System *Clear event:* Yes
524	Simultaneous users	Note	*Description:* Multiple users with administrator or operator access level are logged in. *Type:* System *Clear event:* Yes
535	Alarm log fill	Note	*Description:* Alarm log filling high. Overwrite of older alarms will take place when completely full *Type:* System *Clear event:* Yes
536	Heartbeat trap	Note	*Description:* Heartbeat to signal the system is still functional *Type:* System *Clear event:* No
550	Valid input number below threshold	Warning	*Description:* The number of valid inputs to the switch is below the selected threshold. *Type:* Undetermined *Clear event:* Yes
710	Seamless switch impossible	Major	*Description:* Seamless switch to port not possible. This can be due to delay problems or mismatching streams. *Type:* Undetermined *Clear event:* Yes
711	Switch done	Note	*Description:* Switch has selected another source *Type:* Undetermined *Clear event:* No
712	Delay reset	Note	*Description:* Buffer delays has been reset by user *Type:* Undetermined *Clear event:* No
713	Invalid buffer	Warning	*Description:* Buffer size outside of valid limits *Type:* Undetermined *Clear event:* Yes *Subid3:* "Pri"
1100	Sync unstable	Major	*Description:* Two separate sync-losses in 10s. *Type:* Port *Clear event:* Yes

Table D.3.h Alarms

Alarm ID	Text	Def. severity	Details	
1101	TS unstable	Minor	*Description:*	Lots of PIDs appearing/disappearing or CC errors. Threshold is set in percentage of present PIDs that can have an event (sum of detected and disappeared, or number of C errors) before alarm is set. Other detailed alarms such as CC errors are filtered while TS unstable is active. Alarm is also set if too many PIDs are present.
			Type:	Port
			Clear event:	Yes
1110	No sync	Critical	*Description:*	No valid transport stream detected. See test 1.1 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1120	Sync byte error	Warning	*Description:*	Sync byte not equal to 0x47. See test 1.2 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1131	PAT repetition interval	Warning	*Description:*	Measured interval between each PAT is greater than the configured limit. ETR290 specifies limit to 500 ms. Part of test 1.3 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1132	PAT invalid table ID	Warning	*Description:*	Unable to find section with table_id 0x00 on PID 0. Part of test 1.3 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1133	PAT scrambled	Warning	*Description:*	Scrambling control field set for PID 0. Part of test 1.3 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1134	PAT missing	Warning	*Description:*	PAT not found in transport stream. The PAT is required to do any further PSI decoding.
			Type:	Port
			Clear event:	Yes
1140	CC error	Warning	*Description:*	The Continuity Counter in the TS header was not as expected. Should increase by 1 for each packet with the Payload bit set, and not increase if not. Typically caused by lost TS packets. See test 1.4 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1151	PMT repetition interval	Warning	*Description:*	Measured interval between each PMT on a specific PID referenced in the PAT is greater than the configured limit. ETR290 specifies limit to 500 ms. Part of test 1.5 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1152	PMT scrambled	Warning	*Description:*	Scrambling control field set for any PID carrying table_id 0x02, i.e. a PMT. Part of test 1.5 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes

Table D.3.i Alarms

Alarm ID	Text	Def. severity	Details	
1153	PMT missing	Warning	*Description:*	PMT referenced in the PAT, but not found in transport stream.
			Type:	Port
			Clear event:	Yes
			Subid3:	"Service"
1160	PID error	Warning	*Description:*	PID referred in a PSI table, but not found within the configured period. The period is configured using the PIDs disappeared alarm. See test 1.6 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1161	PIDs disappeared	Ok	*Description:*	This alarm is set when PIDs are timed out. The timeout can be specified per PID. Timeouts specified affect the PID Error alarm also.
			Type:	Port
			Clear event:	No
			Subid3:	"PID"
1162	PIDs detected	Ok	*Description:*	This alarm is used to notify about new PIDs detected.
			Type:	Port
			Clear event:	No
1210	Transport error	Warning	*Description:*	Transport Error Indicator (TEI) set in the TS header. See test 2.1 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1220	CRC error	Warning	*Description:*	CRC on a table section error occurred in CAT, PAT, PMT, NIT, EIT, BAT, SDT or TOT table. See test 2.2 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1230	PCR repetition error	Warning	*Description:*	Time interval between two consecutive PCR values more than the configured value. ETR290 specifies the limit to 40 ms. 40 ms. See test 2.3a in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1231	PCR discontinuity indicator error	Warning	*Description:*	The difference between two consecutive PCR values is outside the configured range without the discontinuity_indicator set. ETR290 specifies range from 0=>100ms. See test 2.3b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1240	PCR overall jitter	Ok	*Description:*	Measures PCR stamp against expected PCR stamp based on local clock. Error if jitter above configured value, ETR290 specifies the limit to 500 ns. Connect external PPS for exact measurements. See Annel.7.4 in ETSI TR 101 290 v1.2.1 for details, part of test 2.4.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"

Table D.3.j Alarms

Alarm ID	Text	Def. severity	Details	
1241	PCR accuracy error	Warning	*Description:*	Measures PCR stamp against expected PCR stamp based on averaged previous PCR stamps. Error if jitter above configured value, ETR290 specifies the limit to 500 ns. See Annel.7.1 in ETSI TR 101 290 v1.2.1 for details, part of test 2.4.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1261	CAT missing	Warning	*Description:*	Found no section with table_id 0x01 or CAT scrambled. Part of test 2.6 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1262	CAT invalid table ID	Warning	*Description:*	Found PID 1, but no section has another table_id than 0x01. Part of test 2.6 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1311	NIT invalid table ID	Warning	*Description:*	Section with table_id other than 0x40 or 0x41 or 0x72 (i. e. not an NIT or ST) found on PID 16. Part of test 3.1 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1312	NITa repetition interval	Warning	*Description:*	Part of test 3.1 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1313	NITo repetition interval	Warning	*Description:*	Part of test 3.1b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1314	NITa section gap too small	Warning	*Description:*	See test 3.1a in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1315	NITo section gap too small	Warning	*Description:*	Part of test 3.1b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1316	NITa missing	Warning	*Description:*	NIT actual is not present.
			Type:	Port
			Clear event:	Yes
1317	NITo missing	Ok	*Description:*	No NIT other sections are present.
			Type:	Port
			Clear event:	Yes
1320	SI repetition error	Warning	*Description:*	Repetition rate of SI tables outside of specified limits. Note that this alarm fires together with the repetition interval and gap alarms for each specific table. See test 3.2 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes

Table D.3.k Alarms

Alarm ID	Text	Def. severity	Details	
1340	Unreferenced PID	Warning	*Description:*	See test 3.4 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1351	SDT invalid table id	Warning	*Description:*	Part of test 3.5 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1352	SDTa repetition interval	Warning	*Description:*	Part of test 3.5 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1353	SDTo repetition interval	Warning	*Description:*	Part of test 3.5b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1354	SDTa section gap too small	Warning	*Description:*	See test 3.5a in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1355	SDTo section gap too small	Warning	*Description:*	Part of test 3.5b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1356	SDTa missing	Warning	*Description:*	SDT actual is not present.
			Type:	Port
			Clear event:	Yes
1357	SDTo missing	Ok	*Description:*	No SDT other sections are present.
			Type:	Port
			Clear event:	Yes
1361	EIT invalid table id	Warning	*Description:*	See test 3.6 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1362	EITpfa repetition interval	Warning	*Description:*	See test 3.6a in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1363	EITpfo repetition interval	Warning	*Description:*	See test 3.6b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
1364	EITpfa section gap too small	Warning	*Description:*	See test 3.6a in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"Service"
1365	EITpfo section gap too small	Warning	*Description:*	See test 3.6b in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"Service"

Table D.3.1 Alarms

Alarm ID	Text	Def. severity	Details
1366	EITpfa section missing	Warning	*Description:* See test 3.6a in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1367	EITpfo section missing	Warning	*Description:* See test 3.6b in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1368	EITpfa missing	Warning	*Description:* See test 3.6a in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes *Subid3:* "Service"
1369	EITpfo missing	Ok	*Description:* See test 3.6b in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1371	RST invalid table id	Warning	*Description:* Part of test 3.7 in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1372	RST section gap too small	Warning	*Description:* Part of test 3.7 in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1381	TDT repetition interval	Warning	*Description:* Part of test 3.8 in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1382	TDT/TOT invalid table id	Warning	*Description:* Part of test 3.8 in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1383	TDT section gap too small	Warning	*Description:* Part of test 3.8 in ETSI TR 101 290 v1.2.1. *Type:* Port *Clear event:* Yes
1384	TDT missing	Warning	*Description:* *Type:* Port *Clear event:* Yes
1385	TOT missing	Warning	*Description:* *Type:* Port *Clear event:* Yes
1386	TOT repetition interval	Warning	*Description:* *Type:* Port *Clear event:* Yes
1602	PDV	Ok	*Description:* Packet Delay Variation over configured threshold *Type:* Port *Clear event:* Yes *Subid3:* "IP Flow"

Table D.3.m Alarms

Alarm ID	Text	Def. severity	Details	
1603	MDI delay factor	Ok	*Description:*	MDI delay factor over configured threshold
			Type:	Port
			Clear event:	Yes
			Subid3:	"IP Flow"
1604	MDI media loss rate	Ok	*Description:*	MDI media loss rate over configured threshold
			Type:	Port
			Clear event:	Yes
			Subid3:	"IP Flow"
1605	Waiting for source	Warning	*Description:*	Source is not available or does not have sync.
			Type:	Port
			Clear event:	Yes
1620	SIPS buffer error	Warning	*Description:*	Differential latency of SIPS input flows is too high
			Type:	Port
			Clear event:	Yes
1621	SIPS flows not identical	Warning	*Description:*	SIPS input flows are not identical
			Type:	Port
			Clear event:	Yes
1622	SIPS unexpected lagging flow	Warning	*Description:*	SIPS lagging input flow is different from configured expected lagging flow
			Type:	Port
			Clear event:	Yes
1801	TS-ID incorrect	Ok	*Description:*	The TS-ID of the incoming stream does not match the TS-ID of the configured CSI section. For modes where the input TS-ID is not known, the TS-ID expected must be configured manually.
			Type:	Port
			Clear event:	Yes
1802	PID rate too high	Ok	*Description:*	PID bitrate is higher than set limit. Only PIDs added to override list are monitored, and the marate must be set per PID.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1803	PID rate too low	Ok	*Description:*	PID bitrate is lower than set limit. Only PIDs added to override list are monitored, and the min rate must be set per PID.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1804	Static scrambling bits	Ok	*Description:*	Scrambling bits are static (not changing between odd and even) within the user defined interval.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"

Table D.3.n Alarms

Alarm ID	Text	Def. severity	Details	
1806	PID scrambled	Ok	*Description:*	Define list of PIDs which should NOT be scrambled. Alarm will be triggered if PID is scrambled
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1807	PID not scrambled	Ok	*Description:*	Define list of PIDs which should be scrambled. Alarm will be triggered if PID is NOT scrambled
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1808	Program severity change	Note	*Description:*	Event set when top level alarm severity level of a program changes. This is a one-shot event which is sent with a severity matching the new severity level of the program. The alarm details has the format: <from_severity>=><to_severity> Alarm(ID:<AlarmID>,<PID|Service>:<Value>,
			Type:	Port
			Clear event:	No
			Subid3:	"Service"
1812	TS rate too high	Ok	*Description:*	TS bitrate is higher than set limit.
			Type:	Port
			Clear event:	Yes
1813	TS rate too low	Ok	*Description:*	TS bitrate is lower than set limit.
			Type:	Port
			Clear event:	Yes
1814	CA system ID missing	Ok	*Description:*	A specified CA system ID is missing in CAT
			Type:	Port
			Clear event:	Yes
			Subid3:	"CAID"
1901	EITpf timing error	Warning	*Description:*	The start/end time of the EITpf present event is not matching current time. The maoffset from current time can be configured with the offset parameter.
			Type:	Port
			Clear event:	Yes
			Subid3:	"TS-ID"
1902	EITpf following error	Warning	*Description:*	The following event is not immediately following the present event
			Type:	Port
			Clear event:	Yes
			Subid3:	"TS-ID"
1903	EITs segmentation error	Warning	*Description:*	Events found in wrong segment based on segmentation rules, or in wrong order
			Type:	Port
			Clear event:	Yes
			Subid3:	"TS-ID"

Table D.3.o Alarms

Alarm ID	Text	Def. severity	Details	
1904	EITs illegal event time	Warning	*Description:*	Event start/end times outside valid range
			Type:	Port
			Clear event:	Yes
			Subid3:	"TS-ID"
1905	EITs gaps found	Warning	*Description:*	Events are not describing all time span of EIT
			Type:	Port
			Clear event:	Yes
			Subid3:	"TS-ID"
2101	MGT repetition interval	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2102	MGT missing	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2103	MGT scrambled	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2104	MGT CRC error	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2106	TVCT repetition interval	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2107	TVCT missing	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2108	TVCT scrambled	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2109	TVCT CRC error	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2111	CVCT repetition interval	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2112	CVCT missing	Ok	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2113	CVCT scrambled	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes

Table D.3.p Alarms

Alarm ID	Text	Def. severity	Details
2114	CVCT CRC error	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2116	RRT repetition interval	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2117	RRT missing	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2118	RRT scrambled	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2119	RRT CRC error	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2121	STT repetition interval	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2122	STT missing	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2123	STT scrambled	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2124	STT CRC error	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2130	EIT-0 repetition interval	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2131	EIT-0 missing	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
			Subid3: "Source-ID"
2132	EIT-1 repetition interval	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
2133	EIT-1 missing	Warning	*Description:* See ATSC Recommended Practice A/78.
			Type: Port
			Clear event: Yes
			Subid3: "Source-ID"

Table D.3.q Alarms

Alarm ID	Text	Def. severity	Details	
2134	EIT-2/3 repetition interval	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2135	EIT-2/3 missing	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
			Subid3:	"Source-ID"
2136	EIT scrambled	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2137	EIT CRC error	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2138	ETT scrambled	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
2139	ETT CRC error	Warning	*Description:*	See ATSC Recommended Practice A/78.
			Type:	Port
			Clear event:	Yes
3055	No license file found!	Critical	*Description:*	No license file found on flash memory. Please load a license key file, and reboot unit.
			Type:	System
			Clear event:	Yes
3100	No lock	Critical	*Description:*	Unable to lock on transport stream
			Type:	Port
			Clear event:	Yes
3101	AGC at maximum	Minor	*Description:*	Automatic gain control is at maximum gain. Loss in signal level can not be compensated.
			Type:	Port
			Clear event:	Yes
3102	C/N low	Warning	*Description:*	Carrier to noise ratio is low. Signal reception may be weak.
			Type:	Port
			Clear event:	Yes
3103	C/N very low	Minor	*Description:*	Carrier to noise ratio is very low. Signal may drop and be difficult to re-tune.
			Type:	Port
			Clear event:	Yes
3104	Signal power low	Warning	*Description:*	The signal power at RF input is low.
			Type:	Port
			Clear event:	Yes
3105	Signal power very low	Minor	*Description:*	The signal power at RF input is very low.
			Type:	Port
			Clear event:	Yes

Table D.3.r Alarms

Alarm ID	Text	Def. severity	Details
3106	High BER/PER	Warning	*Description:* Signal contains a high number of bit/packet errors. *Type:* Port *Clear event:* Yes
3107	LDPC iterations too high	Warning	*Description:* The measured LDPC iterations has exceeded the limit *Type:* Port *Clear event:* Yes
3108	MER is low	Warning	*Description:* Modulation error ratio is below set threshold. *Type:* Port *Clear event:* Yes
3109	Number of uncorrectable blocks is high.	Warning	*Description:* Found a high number of uncorrectable blocks in signal. *Type:* Port *Clear event:* Yes
3112	Configuration error	Major	*Description:* Configuration or licence error *Type:* Port *Clear event:* Yes
3200	No lock	Critical	*Description:* Unable to lock on transport stream *Type:* Port *Clear event:* Yes
3201	No signal	Critical	*Description:* No signal present at RF input *Type:* Port *Clear event:* Yes
3202	Signal power low	Warning	*Description:* The signal power at RF input is low. *Type:* Port *Clear event:* Yes
3203	Signal power very low	Minor	*Description:* The signal power at RF input is very low. *Type:* Port *Clear event:* Yes
3204	Masignal level	Warning	*Description:* The signal at the input port is very high. *Type:* Port *Clear event:* Yes
3205	SNR too low	Major	*Description:* Signal-to-noise ratio (SNR) is too low on RF input. *Type:* Port *Clear event:* Yes
3206	Pre-equalizer MER warning	Warning	*Description:* Pre-equalizer MER (modulation error ratio) is low at RF input. *Type:* Port *Clear event:* Yes
3207	Pre-equalizer MER alarm	Minor	*Description:* Pre-equalizer MER (modulation error ratio) is very low at RF input. *Type:* Port *Clear event:* Yes
3208	PLP not present	Critical	*Description:* The PLP is not present in the T2 stream. *Type:* Port *Clear event:* Yes

Table D.3.s Alarms

Alarm ID	Text	Def. severity	Details	
3209	Echo not present	Warning	*Description:*	The echo was not found in the Channel impulse response
			Type:	Port
			Clear event:	Yes
3210	Shoulder level too high	Warning	*Description:*	The shoulder value of the signal exceeded the limit.
			Type:	Port
			Clear event:	Yes
3211	LDPC iterations too high	Warning	*Description:*	The measured LDPC iterations has exceeded the limit
			Type:	Port
			Clear event:	Yes
3212	Frequency offset high	Warning	*Description:*	The offset from the center frequency is high.
			Type:	Port
			Clear event:	Yes
3213	Frequency offset very high	Major	*Description:*	The offset from the center frequency is high.
			Type:	Port
			Clear event:	Yes
3214	SFN drift alarm	Warning	*Description:*	The SFN has drifted too far in time.
			Type:	Port
			Clear event:	Yes
3215	Post-equalizer MER alarm	Warning	*Description:*	Post-equalizer modulation error ratio (MER) is too low at RF input.
			Type:	Port
			Clear event:	Yes
4700	TS config mismatch	Major	*Description:*	TS is incompatible with the configuration of the input.
			Type:	Port
			Clear event:	Yes
4701	Signal license mismatch	Critical	*Description:*	Incoming signal requires an additional license to receive.
			Type:	Port
			Clear event:	Yes
4800	PTP clock not locked	Warning	*Description:*	Unable to lock to master clock
			Type:	Port
			Clear event:	Yes
13610	EITsa missing	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
			Subid3:	"Service"
13611	EITso missing	Warning	*Description:*	
			Type:	Port
			Clear event:	Yes
			Subid3:	"TS-ID"

Appendix E References

[1]
ISO13818-1, 2 and 3; MPEG-2 Video and Audio and Systems

[2]
ETSI EN 300 468: Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB Systems.

[3]
ETSI TR 101 211: Digital Video Broadcasting (DVB); Guidelines on Implementation and Usage of Service Information.

[4]
ETSI EN 300 744. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television.

[5]
ETSI TS 101 191. Digital Video Broadcasting (DVB); DVB mega-frame for Single Frequency Network (SFN) synchronisation.

[6]
ETR 154 Digital Video Broadcasting (DVB); Implementation Guidelines for the Use of MPEG-2 Systems, Video and Audio in Satellite and Cable Broadcasting Applications. ETSI Technical Report ETR 154, European Telecommunications Standards Institute ETSI.

[7]
IEEE 802.1Q-2005 802.1QTM, Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks

[8]
SMPTE 2022-2-2007: Unidirectional Transport of Constant Bit-Rate MPEG-2 Transport Streams on IP Networks

[9]
SMPTE 2022-1-2007: Forward Error Correction for Real-time Video/Audio Transport over IP Networks

[10]
ITU-T Y.1541 (02/2006) Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Internet protocol aspects; Quality of service and network performance. Network performance objectives for IP-based Services

[11]
Pro-MPEG Forum: Pro-MPEG Code of Practice #3 release 2, July 2004: Transmission of Professional MPEG-2 Transport Streams over IP Networks

[12]
Pro-MPEG Forum: Pro-MPEG Code of Practice #4 release 1, July 2004: Transmission of High Bit Rate Studio Streams over IP Networks

[13]
J. Rosenberg, H. Schulzrinne, IETF RFC2733, December 1999: An RTP Payload Format for Generic Forward Error Correction

[14]
RFC 4445 - A Proposed Media Delivery Index (MDI)

[15]
RFC 3393 - IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)