TNS546 MPEG-2 Transport Stream Monitor User's Manual

Revision: 2.8.0 (4758)

2015-05-06

Valid for SW version 2.8.0 and newer

Contents

1 History

Revision	Date	Comments
2.8.0	2015-05-05	– Added SCTE35 monitor description – Added HbbTv monitor description – Added Service Performance monitor description – Added Charts page descritpion.
2.6.0	2013-09-10	– Changed documentation of input port switches to match new implementation with more than two ports in a switch group. – New Nevion look on screen GUI shots and manual. – Documented support for DHCP (automatic IP address assignment) on Ethernet interfaces. – Traceroute documented. – New option on loading config from another device on Save/Load page. – Comment on hot upgradable features. – Updated alarm table.
2.2.26	2012-09-17	– General clean up and improvements.
2.2	2012-04-25	– Update the T2-MI analysis description – Updated EIT analysis description – Updated available licences.
2.0	2011-08-31	– Added IP input statistics description – Added SLA description – Added T2-MI Analysis description – Added EIT analysis description – Added FEC description on IP inputs – Updated screenshots of the GUI
1.0	2010-10-18	– First version

2 Introduction

2.1 Scope

This manual is written for operators and users of the TNS546 MPEG-2 Transport Stream Monitor and provides necessary information for installation, operation and day-to-day maintenance of the unit. The manual covers the functionality of the software version 2.8.0 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 Nils Hansens vei 2 NO-0667 Oslo Norway

3 Short Product Description

The TNS546 is part of the Nevion nSure product line which safeguards the delivery of high-quality video content, by providing 24/7 monitoring and advanced analysis.

The TNS546 is capable of simultaneously monitoring up to 24 MPEG-2 transport streams, although with an overall limit to the aggregate bit rate of the streams. It bears strong resemblence with the CP545 with respect to monitoring functions, but features up to eight separate ASI inputs. In addition it provides Ethernet inputs which will allow monitoring up to 16 IP encapsulated MPEG transport streams.

Parameters of the monitored transport streams will be compared against specifications and specific requirements, and values of critical components can be displayed graphicallly. Alarms may be programmed to indicate errors in the transport stream, or deviations from operational requirements. A log of the recorded alarms are stored in non-volatile memory. The content of selected packets, or groups of packets, may be recorded for examination and/or documentation.

Salient features of the TNS546 are:

- PSI/SI/PSIP table decoding
  - Repetition rate monitoring
  - Full decoding of all standard PSI/SI/PSIP 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
  - Equipment monitoring from Nevion Connect

- MIP packet inspection
- T2-MI analysis
- Service level agreement monitoring of inputs
- 1 PPS timing reference input
- Reception of transport stream over Gigabit Ethernet

3.1 Software options

The TNS546 functionality depends on the software licences installed. The following table describes the features available as software options. Please refer to **Section 9.4.8.3** for more information how to obtain and enable feature upgrades.

Table 3.1 Functionality enabled through software licences

Functionality	**Code**	**Max value**	**Description**
T2-MI Analysis	T2AN	-	Enables analysis of T2-MI packets in the stream.
SFP module	SFP	-	Enables operation of the Small form-factor pluggable (SFP) transceiver slot.
SFP configuration	SFPC	-	Enables configuration interface and parameter storage for some specifically supported SFP modules.
Number of input ports activated	TSIX	24	Controls the number of simultaneously activated transport stream inputs.
Forward Error Correction	FEC	-	Controls availability of the FEC feature for IP outputs and IP inputs.
Ethernet data interface	IP	-	Controls whether carriage of MPEG transport streams on Ethernet is made available.
Allow ASI inputs	ASIN	-	Enables use of ASI input ports. Without this key the device can be used with IP input only.
Emergency switch support	ESW	-	Enables support for external switch panel to switch between pre-loaded configurations.
Connect control	TCON	-	Enables supervision of the unit through the Connect Software.

4 Getting Started

This section provides a short description of the minimum steps that must be taken in order to start operating the TNS546.

If you are an experienced user of Nevion equipment or similar types of MPEG-2 processing equipment the following description should enable you to quickly install the TNS546 MPEG-2 Transport Stream Monitor and start operation. If this is your first time to install such equipment you are strongly adviced to read the full installation procedure. To gain full benefit of the product functionality and capabilities refer to the user interface description.

The procedures outlined below are based on the assumption that the unit is in the factory default state.

4.1 Management interface

Since the TNS546 is all Web controlled the first step is to set up the IP address for the management interface.

Changing the default IP address using the Web interface requires that your management computer may be configured with a static IP address. If a static IP address cannot be configured on your computer the IP address may be configured via the terminal interface. The procedure is described in the user manual.

Note: Avoid connecting through a network at this stage, as this may give unpredictable results due to possible IP address conflict.

1. Connect an Ethernet cable directly between the PC and the Ethernet "Control" port of the TNS546. The default IP address of the TNS546 is **10.0.0.10/255.255.255.0**. Configure the PC to be on the same subnet as the TNS546.

2. Open your Web browser and type http://10.0.0.10 in the address field of the browser. Log into the GUI with username **admin** and password **salvador**.

3. Browse to *"Device Info -> Network -> Control"* in the GUI, and set the IP address settings required for your network. Click "Apply" to activate the new parameters.

4. The connection with your management PC will now be lost. To re-connect to the TNS546 connect both the "Control" port of the unit and the management PC to the network. The IP settings of the management PC must now be set to agree with the network used.

5. Again, open your Web browser and type http: *(New-IP-Address)* in the address field of the browser. Log into the GUI with username **admin** and password **salvador**.

4.2 Operational mode

The TNS546 can operate in different modes. Thus the appropriate mode for your installation must be enabled.

1. Assign a name for the device in order to more easily identify the unit in the network. Browse to *"Device Info -> Product Info"* and enter a "Name" and "Inventory ID". Click "Apply" to activate.

2. Set date and time of the real time clock to ensure correct time stamping of the alarm log entries. Browse to *"Device Info -> Time Settings"*. The internal clock may be used to time stamp alarm log entries, in which case a manual *"Date"* and *"Time"* adjust is all that is needed. Click "Apply" to activate.

   You may enable an external time source to provide a common reference for alarm logs of all units of a system. Refer to the user manual for details.

3. Configure the operational mode. Browse to *"Device Info -> Maintenence"* and select "DVB" or "DVB/ATSC" mode as required. Click "Apply" to activate. When the operating mode is altered the TNS546 resets, which means you have to refresh the browser and log in as explained above.

4.3 Input configuration

Depending on options licensed the TNS546 will accept ASI transport streams through the BNC input ports and/or IP encapsulated transport streams through the Ethernet/SFP ports.

1. Configure an ASI input port. Browse to *"Inputs"* and click on the input port number you want to activate, designated "ASI #" or "ASI/310M#" according to the chosen operational mode.

2. IN the *"Main"* page tick the "Enable input" check box and type an identifying name, e.g. the service name in the "Input label" box. Click "Apply" to activate. If the operating mode has been set to **DVB** the TNS546 is now ready to accept a DVB transport stream on the configured input port.

3. If the operating mode has been set to **ATSC+DVB** the input format and transport stream mode must be specified. In the *"Input format"* pull-down list select the transport stream input format. In the *"TS mode"* pull-down list select the transport stream mode. Click "Apply" to activate.

The coloured indicator at the top of the page shows the input signal status. Red indicates that the input signal cannot be decoded. Yellow indicates that an error has been detected in a decoded signal. Green indicates a decoded signal with no errors. Gray colour indicates that the input has not been enabled.

1. Configure a data interface. Browse to *"Device Info"* and click on the network interface you intend to use. In the *"Main"* page tick the "Enable input" check box. Enter suitable IP address parameters and speed/duplex mode. Click "Apply" to activate.

2. Enable an IP input. Browse to *"Inputs -> Inputs overview -> IP Inputs"* and click on the *"Add IP Input"* button. Click "Apply" to activate.

3. Configure the IP input. Click on the IP input port icon that has appeared in the *"Inputs Overview"* list. This opens the configuration page.

4. Click the "Enable input" check box, type an identifying label in the "Input label" field and from the *"Source interface"* pull-down list select the appropriate data interface.

5. Enter the IP address and port number of the desired stream to receive. Tick the "Join multicast" check box, if appropriate.

6. Finally, if the operating mode has been set to **ATSC+DVB** select transport stream mode from the *"TS mode"* pull-down list. Click "Apply" to activate.

Again, the coloured indicator at the top of the page shows the input signal status.

5 Installing the Equipment

Caution: The TNS546 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.

5.1 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 TNS546 is mechanically and electrically in order.
- Verify that you received the following items:
  - TNS546 with correct power supply option
  - Power cord(s)
  - CD-ROM containing documentation and Flash Player installation files
  - Any optional accessories you have ordered

Note: 48 VDC versions do not ship with a power cord; instead a Power D-SUB male connector for soldering to the supply leads is supplied.

5.2 Installation Environment

As with any electronic device, the TNS546 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 TNS546.
- 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 TNS546 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.

5.3 Equipment installation

The TNS546 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 TNS546 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 TNS546.

5.4 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 5.1 .
- The TNS546 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 5.1 shows the air path through the unit, where cool air is taken from the left hand side, seen from the front.

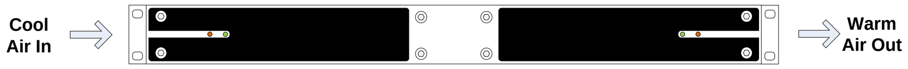


Figure 5.1 Air path through the unit

5.5 Power supply

The TNS546 may be delivered rated for AC or DC operation, respectively.

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.

5.5.1 AC power supply

The TNS546 has a wide-range power supply accepting the voltage range 100-240 VAC, 50/60 Hz. Please refer to **Appendix A** for a detailed specification of the AC power supply.

5.5.1.1 Dual AC power supplies

Alternatively, the TNS546 may be fitted with dual internal wide-range AC power supplies. If so, the size of the cabinet is full-width 19" rack, 1RU. 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 A** for a detailed specification of the AC power supply.

5.5.1.2 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 5.1**.

Table 5.1 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

5.5.1.3 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 A** 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.

5.5.1.4 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 TNS546 mains input connector(s) and then to the local mains supply.

5.5.2 DC power supply

The TNS546 can be delivered with a 48 VDC power supply for use in environments where this is required. The DC power supply accepts an input voltage range of 36-72 VDC. Please refer to **Appendix A** for detailed specification of the power supply.

5.5.2.1 Dual DC power supplies

Alternatively, the TNS546 may be fitted with dual internal wide-range DC power supplies. If so, the size of the cabinet is full-width 19" rack, 1RU. The power supplies cover the voltage range 36-72 VDC.

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 DC mains circuits.

Please refer to **Appendix A** for a detailed specification of the DC power supply.

5.5.2.2 DC power cable

Units delivered with DC power supply have a 3-pin male D-SUB power connector instead of the standard mains power connector. Also a female 3-pin D-SUB connector is supplied. The pin assignment is shown in **Table 5.2**. The power cable itself is not supplied.

Table 5.2 DC power connector pin assignment

Pin	Placement	Specification
1	top	+ (positive terminal)
2	middle	- (negative terminal)
3	bottom	Chassis Ground

To connect the unit to the local DC power supply:

1. Use an electronics soldering iron or a hot air workstation to attach the supplied female D-SUB power connector to suitable power leads.
2. Connect the power leads to your local power supply.
3. Connect the DC power connector, with attached power leads, to the TNS546 power input connector.

5.5.3 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.

6 Functional Description

The TNS546 designed for monitoring of MPEG-2 transport streams. The transport streams to be monitored may be input as DVB ASI signals, or they may be input as IP encapsulated streams. The Ethernet inputs may carry several independent transport streams, using separate IP addresses. An arbitrary set of the incoming transport streams may be selected for monitoring. The number of transport streams that may be monitored simultaneously is however governed by the aggregate bit rate of these transport streams.

The TNS546 provides two ASI transport stream outputs, which may output copies of selected input transport streams.

The product offers an easy-to use WEB based user interface giving access to all configuration settings and monitoring results. The TNS546 may be integrated with network management systems via the SNMP interface.

This chapter gives a brief description of the inner workings of the TNS546,

Figure 6.1 shows a functional block diagram of the main components inside TNS546. The different blocks are described in more detail in the following sections.

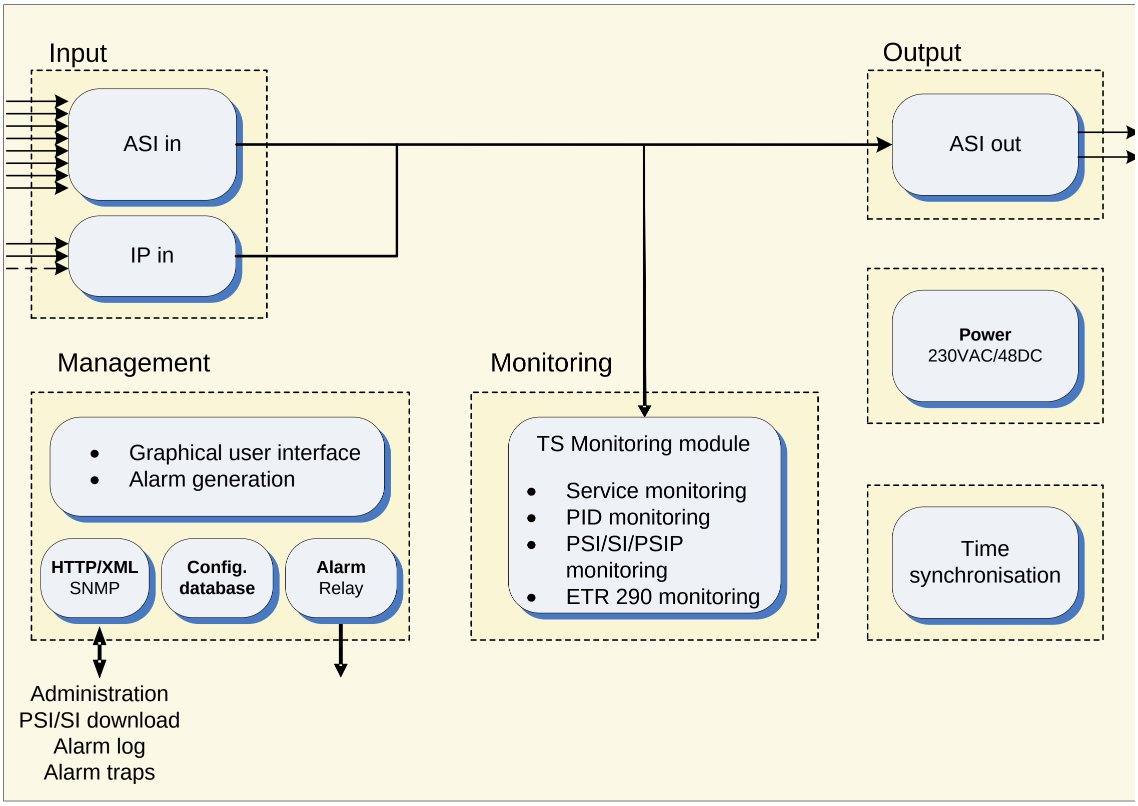


Figure 6.1 TNS546 block diagram

6.1 Input

The input interfaces include eight ASI inputs (BNC connectors) and three IP inputs: two ethernet ports and an SFP socket. However, only two of the three IP inputs may be active at any one time. One of the Ethernet inputs may be substituted for an SFP module giving the option to provide input via e.g. optical fibre. Use of an SFP module is user configurable, provided this software option has been licensed.

6.2 Output

The *Output* section has two BNC connectors that can be freely configured as ASI outputs. This will allow for visual and aural supervision of specific transport streams, if desired.

6.3 Monitoring

The *Monitoring* section provides monitoring of multiple 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 graphicallly. 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.

6.4 Management subsystem

The management subsystem is a set of modules that handles all the interfaces to monitor and control the operation of the TNS546.

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 (T-Vips XML Protocol) to retrieve and set configuration and status
- Alarm relays on alarms
- SNTP client for real time clock synchronisation
- 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.

6.4.1 Graphical user interface

Operators monitor and control the TNS546 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 TNS546 can be controlled from the web GUI.

6.4.2 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
- On-device stored configurations

6.4.3 Alarm manager

The TNS546 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 relay and alarm LED are meant to signal whenever a **critical** alarm is present. In addition the relay can also be programmed to be activated for alarm levels other than level 6.

The alarm manager keeps a log in non-volatile memory of the latest 10000 alarms that have occurred.

As an additional option, the alarm manager in the TNS546 supports so-called *Virtual Alarm Relays*. These are highly programmable items that can be customised to react to virtually any given alarm event or combination of alarm events. The status of each virtual alarm relay can be viewed in the GUI and can also be exported using SNMP. Details on configuring the virtual alarm relays can be found in the WEB interface section.

6.5 Time synchronisation

The TNS546 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 servers using SNTP protocol. Up to four NTP servers can be configured for NTP server redundancy.

More than one clock source may be specified in a prioritised order. If one source fails the next priority source will be used.

7 Physical Description

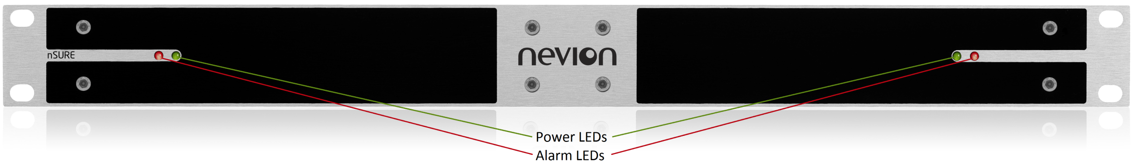


Figure 7.1 Front panel of TNS546

The front panel, figure 7.1, provides two LEDs per TNS546. Two units may share a common front panel. The meaning of the LED indicators is shown in table 7.1.

Table 7.1 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

These LEDs are replicated on the rear panel.

Figure 7.2 shows the rear panel of the TNS546, with indications as to the significance of each connector. A further description follows below.

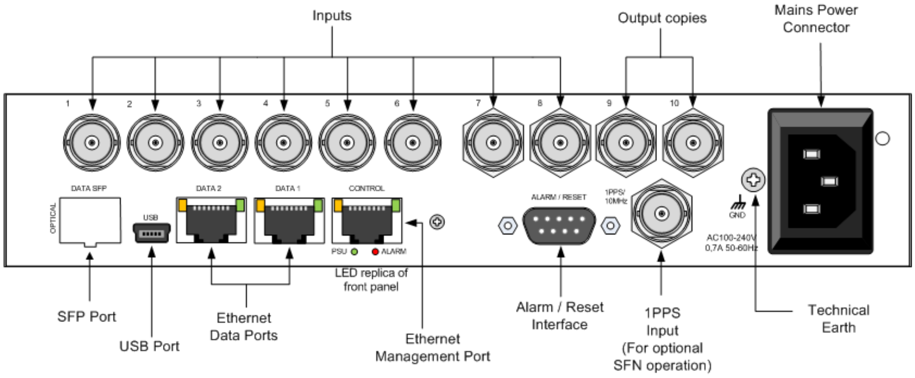


Figure 7.2 Rear panel of TNS546

7.1 MUX inputs

BNC connectors 1 through 8 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 number of input ports that can actually be used depends on the product licence key. If not all ports are visible in the user interface they may be opened by purchasing an additional licence from Nevion.

7.2 Output copies

BNC connectors 9 and 10 are output ports. These may be used to forward any of the input transport streams to supplementary equipment for analysis purposes. Each of the two ports provide independent output signals selected from the transport stream inputs. Note that the output stream will be ASI even if the input signal copied is SMPTE 310M.

Depending on the licence key installed transport streams present on Ethernet inputs may be extracted and output on the ASI monitor outputs.

7.3 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.

7.4 Alarm/Reset interface

The unit is equipped with a 9-pin male DSub 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. Please refer to section 9.4.2.3 for a description how to program the relays.

The pin-out of the connector is shown in table 7.2.

Table 7.2 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

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 **Section 9.4.2.3**. 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 **A** (Technical Specifications).

7.5 Ethernet data port

The TNS546 is equipped with two Ethernet data ports, “Data1” and “Data2”. These allow monitoring of up to 16 IP encapsulated MPEG transport streams in addition to those present on the MUX input ports. There is, however, an upper limit to the overall bit rate of the transport streams (MUX and IP encapsulated) that can be monitored simultaneously.

Note that if both Ethernet data ports are enabled the SFP module may not be enabled simultaneously.

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.

7.6 Ethernet management port

The TNS546 provides one Ethernet port, “Control”, dedicated to control and management. Connect the management port to the management network. The management port LEDs give the following information:

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

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

Beneath the management port are two LEDs that replicate the front panel LEDs.

7.6.1 SFP port

The TNS546 provides a slot to accommodate an SFP module. This will provide an additional Ethernet port supporting fibre optical transmission.

Enabling of the SFP slot is done from the ’Device Info->Maintainance’ page. Note that when using the SFP slot, the DATA-2 Electrical Ethernet port is automatically turned off.

To use the SFP slot, the licence key SFP module must be installed.

7.6.2 USB port

The mini USB connector provides an IP network-independent means to configure and monitor the TNS546. This is useful especially when the unit shall be introduced into a network already in operation.

USB 1.1 standard is supported.

7.6.3 Technical Earth

Connect the Technical earth to a suitable system earth point.

7.6.4 Mains power connector

Figure 7.2 shows the unit with an AC mains power connector. In the case of a DC operated unit this connector is replaced by a 3-pin male D-SUB power connector.

Section 5.5 provides details of the power supply, protective earth and security. Read these instructions carefully prior to connecting the unit to mains power.

8 Operating the Equipment

The TNS546 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 9.0 or newer is required to use the Web interface of the TNS546. As a general rule it is recommended to always use the latest official release of Flash Player (version 10 or newer). 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.

Note: When using Microsoft Internet Explorer, version 6.0 or higher is required. It is however recommended to upgrade to version 8.0 or newer for best performance.

8.1 Accessing the graphical user interface

The default IP address of the TNS546 will most probably not be suitable for the network where the unit will operate. Initially therefore, the user should change the IP address of the management interface so that access may be gained from the network.

The TNS546 offers two options to alter the user interface IP address; through an Ethernet connection or using a USB terminal interface. If your management computer allows setting a fixed IP address, change the IP address using the Ethernet option described in **Section 8.3.1**.

If a static address cannot be configured on your management computer, **Section 8.3.2** 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 9**.

8.2 Password protection

Remote access to the device is controlled by password protection. If you access the TNS546 using the USB terminal interface a password is not required.

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

The passwords can later be changed, either from the Web GUI or via the terminal.

8.2.1 Resetting the password list

If a password is lost, the password list can be reset to factory defaults via the local USB terminal interface. To reset the password list, type the following command in the terminal interface:

```
userdb factory_defaults
```

> **Note:** The `factory_defaults` option on the `userdb` command is available without administrator previledges only when accessing the terminal via the local USB interface. In remote terminal sessions with a Telnet client, administrator privileges are required to run the same command.

8.3 Changing the IP address of the unit

The TNS546 is supplied with a dedicated management Ethernet port, labeled Control. The default IP configuration (IP address and netmask) of the port is **10.0.0.10/255.255.255.0**.

8.3.1 Changing IP address via the Web GUI

Changing the default IP address using the Web interface requires that your management computer may be configured with a static IP address.

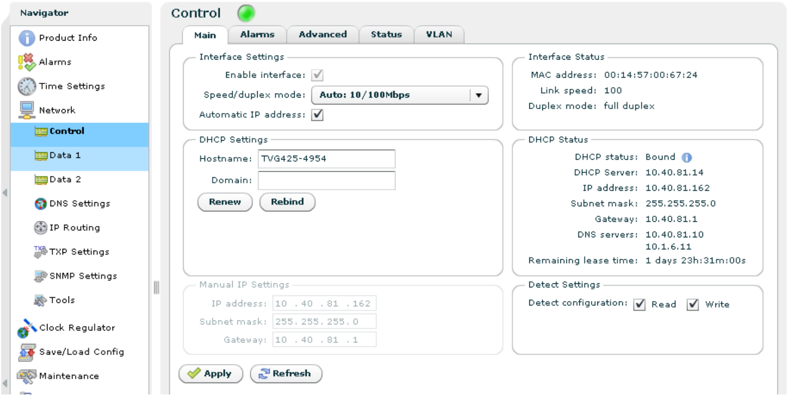
> **Note:** Avoid connecting through a network at this stage, as this may give unpredictable results due to possible IP address conflicts.

1. Connect an Ethernet cable directly between the PC and the Ethernet control port of the TNS546. Configure the PC to be on the same sub net as the TNS546. See Figure 8.2.
2. Open your web browser and type http://10.0.0.10 in the address field of the browser. Log into the GUI with username **admin** and password **salvador**.
3. Browse to Device Info -> Network -> Control in the GUI, and set the correct IP address settings. Click apply to activate the new parameters. Figure 8.1 shows this GUI screen.

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

Windows XP example

The screen-shot in Figure 8.2 shows how to configure the network interface in Windows XP to communicate with the TNS546 with factory default settings. The IP address/netmask is set



Interface Settings

Enable interface: ☑

Speed/duplex mode: Auto: 10/100Mbps

Automatic IP address: ☑

Interface Status

MAC address: 00:14:57:00:67:24

Link speed: 100

Duplex mode: full duplex

DHCP Settings

Hostname: TVG425-4954

Domain:

DHCP Status

DHCP status: Bound

DHCP Server: 10.40.81.14

IP address: 10.40.81.162

Subnet mask: 255.255.255.0

Gateway: 10.40.81.1

DNS servers: 10.40.81.10
10.1.6.11

Remaining lease time: 1 days 23h:31m:00s

Manual IP Settings

IP address: 10 .40 .81 .162

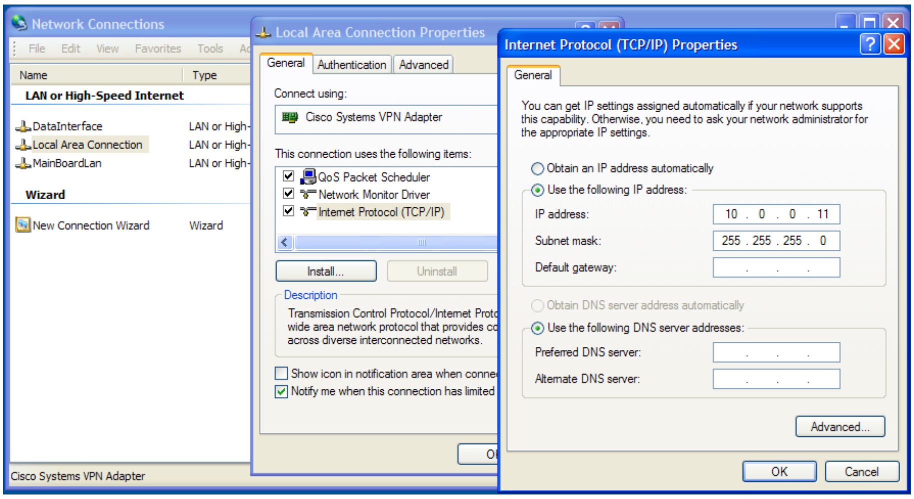
Subnet mask: 255. 255. 255. 0

Gateway: 10 .40 .81 .1

Detect Settings

Detect configuration: ☑ Read ☑ Write

Figure 8.1 Configuring network settings via the Web GUI



Connect using:

Cisco Systems VPN Adapter

This connection uses the following items:

☑ QoS Packet Scheduler

☑ Network Monitor Driver

☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Proto
wide area network protocol that provides co
across diverse interconnected networks.

☐ Show icon in notification area when conne

☑ Notify me when this connection has limited

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 8.2 Setting static IP address 10.0.0.11 in Windows XP

to 10.0.0.11/255.255.255.0 which is on the same sub net as the TNS546, and does not conflict with the IP address of the device.

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

8.3.2 Changing the management port IP address via 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 (*setup_ftdi_usb_drivers.exe*). (This step may be omitted if the driver has already been installed.)

2. Connect your computer USB port to the TNS546 USB port using a suitable cable.
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. Test that the connection is successful by hitting the <Enter> key. If successfull an >app prompt should be shown.
5. In the terminal, type the following command and press <Enter>:

   ```
   net ipconfig --ip <ip address> --mask <subnet mask> --gw <default gateway>.
   ```

Example:

```
app>net ipconfig --ip 10.40.80.100 --mask 255.255.255.0 --gw 10.40.80.1
```

This will result in the IP address 10.40.80.100 being set. The subnet mask is set to 255.255.255.0 and the default gateway to 10.40.80.1.

> **Note:** The product CD shipped with the TNS546 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. Drivers retrieved from http://www.ftdichip.com will also work, but these may not have the same COM port number mapping.

8.3.3 Configuring automatic IP address assignment

The TNS546 can be configured to obtain an IP address automatically from a DHCP server on the network. See section 8.3.1 for how to connect, and section 9.4.4.1.1.1 for how to configure this from the GUI. Alternatively, configure it in the terminal by connecting as in 8.3.2 and issuing the following command:

```
ipconfig --dhcp 1 --hostname <your_device_name>
```

Example:

```
ipconfig --dhcp 1 --hostname bonemachine-100
```

Replace <your_device_name> with the name to register in the DNS system for your device. After this, it should be possible to contact the unit in a browser using the URL:

```
http://<your_device_name>
```

To disable automatic IP assignment, use the command

```
ipconfig --dhcp 0
```

Note: Hostname registration is only done via the DHCP server, so if DHCP is not enabled the hostname is not registered. The default hostname used is on the format TNS546-`<serial-no>`-`<interface-no>`

Note: If automatic IP address assignment is configured and the interface is connected to a network that does not support DHCP, the interface will not receive an address and will fall back to a link local address after about 1 minute, using the first available address in the range 169.254.1.0 - 169.254.254.255. If you have a unit that has been configured with DHCP, but current network does not support it, you should be able to connect to the device for reconfiguration on a local network connection using the address 169.254.1.0. If more devices are using link local addresses, try 169.254.1.1, 169.254.1.2, etc.

8.3.4 Detecting the management port IP address

If you have a unit and do not know the IP address of the Control Interface there are a few options available. The simplest solution is connecting through the USB interface.

8.3.4.1 USB Interface

See 8.3.2 on how to connect to the unit using the USB Interface.

Type the following command to list the currently assigned IP addresses:

```
app>net ipconfig
```

8.3.4.2 Nevion Detect

If you are not able to connect through the USB Interface, you may use the Nevion Detect software. This software may be found on the Nevion Product CD (version 2.20 and newer), or by contacting Nevion Support (see **Section 2.4**). An User's Manual is also included.

The Nevion Detect software detects devices by sending broadcast messages that the TNS546 and other Nevion devices will recognize and reply to with some essential information. The PC running Nevion Detect may be on a totally different subnet than the TNS546, such that the device will be discovered regardless of IP addresses and IP submasks.

Warning: Some Ethernet equipment might block broadcast traffic. Connect your PC directly to the TNS546 to avoid this.

Note: It is possible to avoid that the TNS546 is detected by the Nevion Detect software. See **Section 9.4.4.1.1** for details on how to do this.

9 WEB Interface

The TNS546 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 TNS546 and get status information.

9.1 Login

Access the TNS546 by entering its IP address in the address field of your favourite browser. When accessing the TNS546 the first time, the progress bar (**Figure 9.1**) should appear while the Flash application is loading from the device.

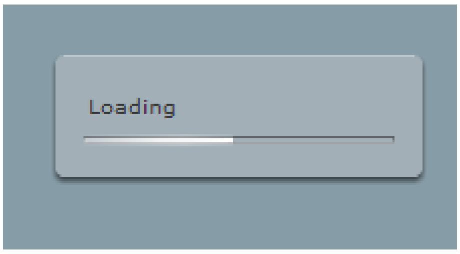
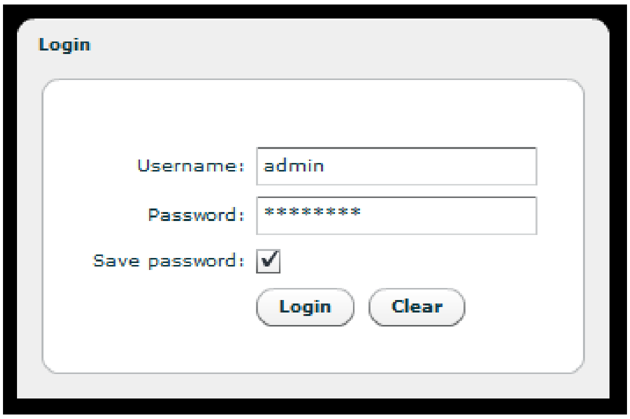


Figure 9.1 Flash application loading

When the loading of the Flash application is finished, the login window (see **Figure 9.2**) is displayed. Type the username and password to enter the GUI application. The default passwords are listed in **Section 8.2**.


Login

Username: admin

Password: ********

Save password: ☑

Figure 9.2 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.

9.2 Status header

After successful login the start page is shown. The top part of the page (shown in **Figure 9.3**) is called the status header, while the bottom part of the page (shown in **Figure 9.4**) is called the status footer.

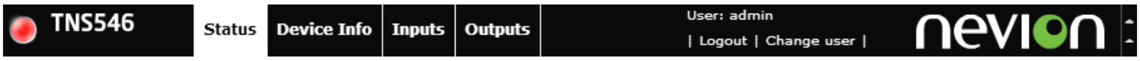


Figure 9.3 The status header

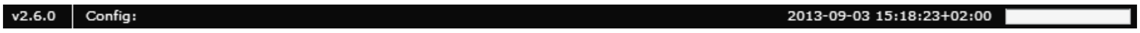


Figure 9.4 The status footer

In the status header the product name is shown on the left hand side, along with the configurable product label, see **Section 9.4.1**.

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 C**.

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

- A text showing the current user name.
- 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 current software version
- The name of the current configuration, if any. See **Section 9.4.1** for details on how to configure this.
- The local device time.
- 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 9.5. This pane is used to navigate between sub-pages of the tab.

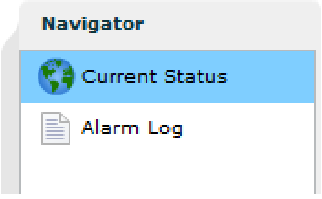


Figure 9.5 Status navigator

> **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.

9.3 Status

The status page presents an overview of the device operational status as well as a log of alarm events.

There are two sub-pages within the status page.

Current Status
: Indicates the running status of 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).

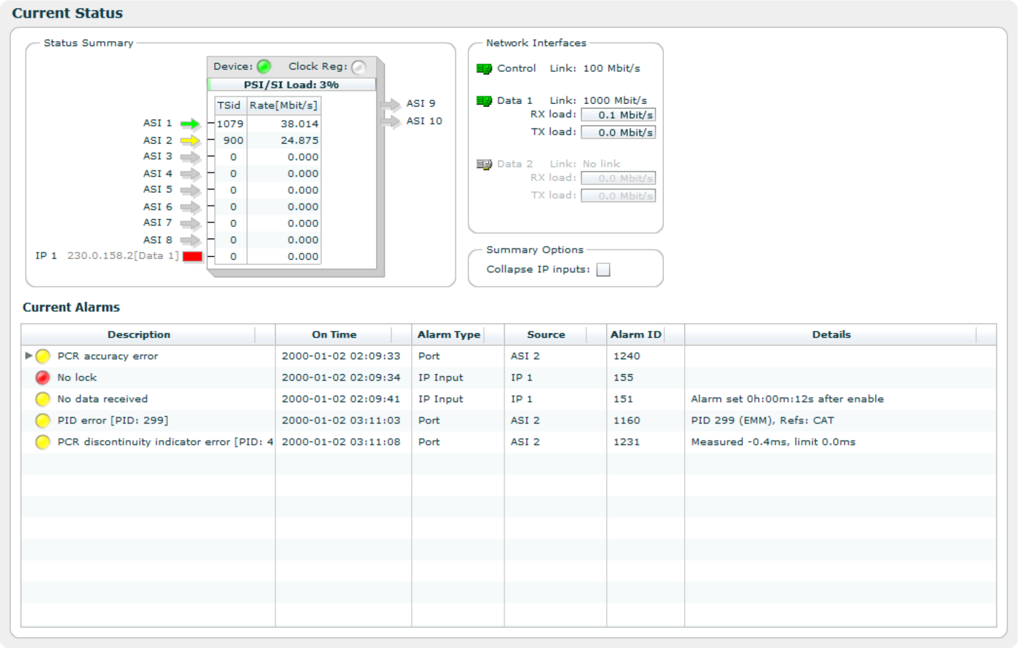
9.3.1 Current Status

This page displays the current status of the device. It consists of a block diagram illustrating the device with its input and output ports, an overview of the currently active network interfaces and a list of currently active alarms.

Block Diagram
: The block diagram provides a compact view of the unit status. It shows:

  - The name of the functional units of the device.
  - The name and alarm status of each input/output port.
  - The status of non-I/O port related alarms.

  The alarm status is shown with colours indicating the severity of the alarm. The various severities and colours used are described in Appendix C.



Current Status

Status Summary

Device: ● Clock Reg: ○

PSI/SI Load: 3%

	TSid	Rate[Mbit/s]
ASI 1	1079	38.014
ASI 2	900	24.875
ASI 3	0	0.000
ASI 4	0	0.000
ASI 5	0	0.000
ASI 6	0	0.000
ASI 7	0	0.000
ASI 8	0	0.000
IP 1 230.0.158.2[Data 1]	0	0.000

ASI 9
ASI 10

Network Interfaces

Control Link: 100 Mbit/s

Data 1 Link: 1000 Mbit/s
RX load: 0.1 Mbit/s
TX load: 0.0 Mbit/s

Data 2 Link: No link
RX load: 0.0 Mbit/s
TX load: 0.0 Mbit/s

Summary Options

Collapse IP inputs: □

Current Alarms

Description	On Time	Alarm Type	Source	Alarm ID	Details
PCR accuracy error	2000-01-02 02:09:33	Port	ASI 2	1240	
No lock	2000-01-02 02:09:34	IP Input	IP 1	155	
No data received	2000-01-02 02:09:41	IP Input	IP 1	151	Alarm set 0h:00m:12s after enable
PID error [PID: 299]	2000-01-02 03:11:03	Port	ASI 2	1160	PID 299 (EMM), Refs: CAT
PCR discontinuity indicator error [PID: 4	2000-01-02 03:11:08	Port	ASI 2	1231	Measured -0.4ms, limit 0.0ms

Figure 9.6 Current status

Access to additional information pertaining to the various ports of the block diagram is provided by hovering the mouse pointer over the port within the diagram. The port representations in the diagram also act as shortcuts to the corresponding configuration page for the port. The shortcut is activated by clicking on the port in the diagram.

Right-clicking the status block diagram top bar offers a shortcut to clear device statistics parameters. Selecting *Reset device statistics* brings up a dialogue where you can select which information to clear.

The precise lay-out of the block diagram depends on the device configuration; partly as a function of the installed options and partly depending on the user's selections.

The main functional block of the TNS546 is shown on the right hand side displaying all input and output ASI ports. Active ports are coloured green. The transport stream ID and the current transport stream bit rate for each input port are displayed. If an output port is enabled a connecting line shows which input stream is being passed to the output.

At the top of the block is an indicator showing the overall operational status. Below the indicator a status bar shows the total PSI/SI/PSIP handling load on the device, contributed by all incoming transport streams.

To the left of the ASI ports there is one large box per IP interface that can carry data traffic. Above the box is the name of the interface. Below this is a bar showing the current IP RX load. Below the bar is a box that shows the overall status of the interface. If the box is grey the interface is disabled or data traffic is not allowed on the interface. If the box is coloured, the colour shows the current alarm status of the interface.

Inside the IP interface boxes one or more horizontal or vertical frames are displayed. The top horizontal frame represents the IP input port using the physical interface. The vertical frames represent virtual interfaces (VLANs) configured on the physical interface. Small boxes inside a frame represent IP input ports. There is one vertical frame for each configured VLAN, each containing IP input ports using that VLAN.

Each of the small boxes represents an IP input port. It is coloured depending on its status, similar to an ASI port. It is possible to move an IP input port from one interface to another by dragging the box and dropping it on a different interface. By clicking an IP input port the configuration page for that port will displayed.

Current Alarms

The bottom part of the page shows the currently active alarms. Some alarms may contain several sub-entries that are displayed by clicking on the arrow in front of the entry's description. The severity of each alarm is represented by an error indicator (visually similar to a LED). The colour of the indicator represents the severity level configured for the specified alarm. The various severities and colours used are described in **Appendix C**.

The Current Alarms table contains six columns:

Description

Description of the alarm condition.

For sub-entries, the extended index is shown in brackets. To the left is an indicator visualising the severity of the alarm. The indicator has a tool-tip providing a textual description of the alarm severity.

On Time

The time when the alarm was raised.

Alarm type

Category of the alarm, i.e. Port, System, Switch etc.

Source

This identifies the source of the alarm. For port alarms, this is a reference to the specific port raising the alarm. This field has a tool-tip showing the subid1 and subid2 values for the alarm.

Subid1

Reserved for future use in multi-slot chassis and is always set to 1 in the TNS546.

Subid2

The device or port to which the alarm relates. The value is zero for alarms that are related to the device rather than to a specific port. Values of 1 and up reference specific ports.

Alarm ID

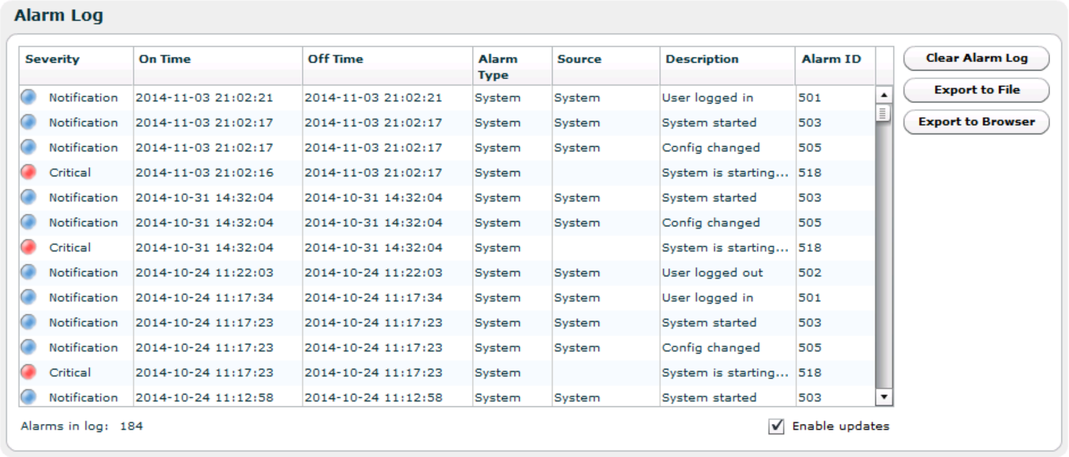
Each alarm condition has an associated numerical alarm ID.

Details

An optional string to provide more alarm information in human readable form. The format of this string depends on the alarm type. Hovering the mouse over this field produces a tool-tip displaying the full text.

A detailed overview of alarm conditions is given in **Appendix C**.

9.3.2 Alarm log



Alarm Log

Severity	On Time	Off Time	Alarm Type	Source	Description	Alarm ID
● Notification	2014-11-03 21:02:21	2014-11-03 21:02:21	System	System	User logged in	501
● Notification	2014-11-03 21:02:17	2014-11-03 21:02:17	System	System	System started	503
● Notification	2014-11-03 21:02:17	2014-11-03 21:02:17	System	System	Config changed	505
● Critical	2014-11-03 21:02:16	2014-11-03 21:02:17	System		System is starting...	518
● Notification	2014-10-31 14:32:04	2014-10-31 14:32:04	System	System	System started	503
● Notification	2014-10-31 14:32:04	2014-10-31 14:32:04	System	System	Config changed	505
● Critical	2014-10-31 14:32:04	2014-10-31 14:32:04	System		System is starting...	518
● Notification	2014-10-24 11:22:03	2014-10-24 11:22:03	System	System	User logged out	502
● Notification	2014-10-24 11:17:34	2014-10-24 11:17:34	System	System	User logged in	501
● Notification	2014-10-24 11:17:23	2014-10-24 11:17:23	System	System	System started	503
● Notification	2014-10-24 11:17:23	2014-10-24 11:17:23	System	System	Config changed	505
● Critical	2014-10-24 11:17:23	2014-10-24 11:17:23	System		System is starting...	518
● Notification	2014-10-24 11:12:58	2014-10-24 11:12:58	System	System	System started	503

Alarms in log: 184

☑ Enable updates

Figure 9.7 Alarm log

The alarm log shows every alarm that has been triggered since the last time the alarm log was cleared.

The table consists of the same columns as the Current Alarms table, but does not show details by default. You can change which columns to show, including the details column, in **Section 9.4.2.4**. 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 TNS546.

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.

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 three 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 dialogue 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).

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

The alarm log is stored in non-volatile memory, so the content is kept even if the unit is rebooted.

The log is circular. Events occurring after the maximum number of entries has been reached overwrite the oldest entries in the log. The maximum number of stored entries is 10000.

9.4 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 9.8**.

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

9.4.1 Product info

The product info page contains general device information.

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 9.4.7**. The device name is shown in the web GUI status header (see **Section 9.3.1**), 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.

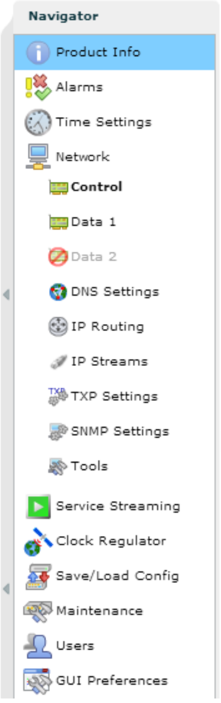
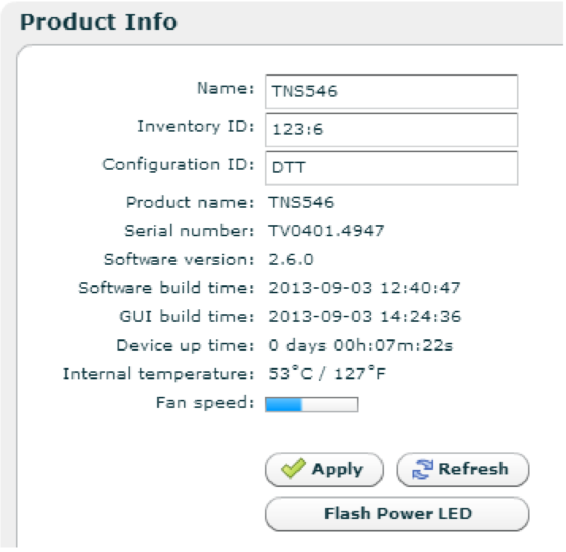


Figure 9.8 Device Info navigator



Product Info

Name: TNS546

Inventory ID: 123:6

Configuration ID: DTT

Product name: TNS546

Serial number: TV0401.4947

Software version: 2.6.0

Software build time: 2013-09-03 12:40:47

GUI build time: 2013-09-03 14:24:36

Device up time: 0 days 00h:07m:22s

Internal temperature: 53°C / 127°F

Fan speed:

Figure 9.9 Product Information

Configuration ID

Configure a user defined name for the current configuration of the unit. This name will, if given, be displayed in brackets after the unit name in the status header as shown in Figure 9.3. 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 9.4.7 on how to load a new configuration.

Product name

Displays the name of the product as designated by Nevion.

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.

Device up time

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

Internal temperature

This shows the current internal temperature of the unit in degrees Celsius and Fahrenheit.

Fan speed

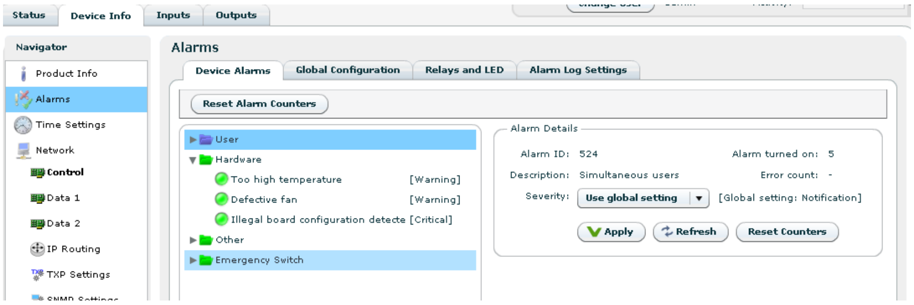
This bar chart shows the current speed of the device fans relative to full speed.

Flash Power LED button

The Flash Power LED button activates flashing the green power LED on the device in question. This is useful for identifying which device is currently being configured. Each click of the button extends the blinking period by five seconds up to a maximum of about 30 seconds of blinking.

9.4.2 Alarms

The Alarms page is shown in Figure 9.10:



User
Hardware
Too high temperature [Warning]
Defective fan [Warning]
Illegal board configuration detecte [Critical]
Other
Emergency Switch

Alarm Details

Alarm ID: 524 Alarm turned on: 5

Description: Simultaneous users Error count: -

Severity: Use global setting [Global setting: Notification]

Figure 9.10 Alarm configuration

This page displays the status of all system alarms and allows the user to program the severity of these alarms. Global alarm configuration is performed on this page, as well as alarm relay configuration and alarm log configuration.

It gives access to the following sub pages:

- Device Alarms
- Global configuration
- Relay and LED configuration
- Alarm Log Settings

9.4.2.1 Device alarms

The page shown in Figure 9.10 provides the administrator with an interface to view the status and configure the behaviour of all alarms related to the system. At the top the Reset Alarm Counters button allows resetting all alarm counters simultaneously.

The page is divided into two parts. On the left is a tree that shows all the alarms. The colour of the folder icon and the specific indicator represents the current status of the alarm. The text to the right of the tree shows the currently configured severity of the alarm.

The right hand side of the page displays the Alarm Details field when an alarm is selected:

Alarm ID
: The internal numerical ID of the selected alarm.

Alarm
: Title of the alarm.

Description
: Brief description of the condition of the alarm.

Severity
: A configurable option defining the severity of the alarm. Options in the pull-down box range

between Filtered (meaning ignored) to Critical. The text in brackets represents the default setting.

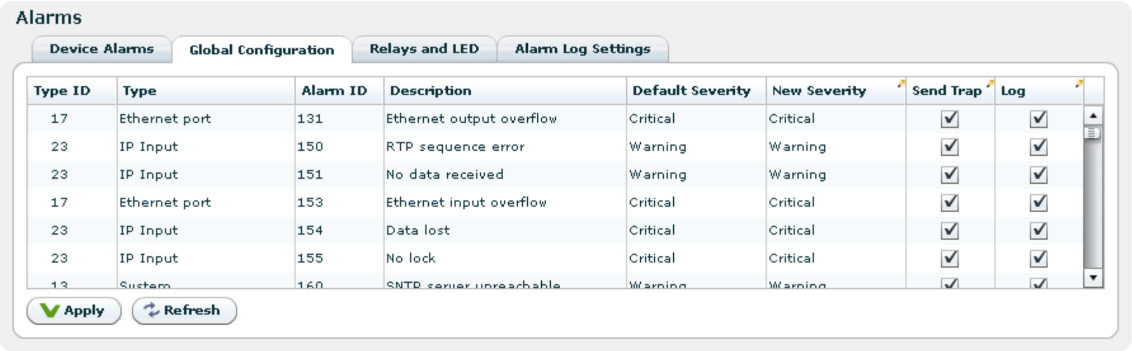
Alarm turned on
: The number of times the alarm has transitioned from off to on since last reset of the alarm counter.

Error count
: Not used.

'Reset Counters' button
: When clicked, clears the alarm counters for the current alarm.

The right-click context menu of the device alarm page provides an option to reset the counters of all the alarms in the Device Info tree.

9.4.2.2 Global configuration



Type ID	Type	Alarm ID	Description	Default Severity	New Severity	Send Trap	Log
17	Ethernet port	131	Ethernet output overflow	Critical	Critical	☑	☑
23	IP Input	150	RTP sequence error	Warning	Warning	☑	☑
23	IP Input	151	No data received	Warning	Warning	☑	☑
17	Ethernet port	153	Ethernet input overflow	Critical	Critical	☑	☑
23	IP Input	154	Data lost	Critical	Critical	☑	☑
23	IP Input	155	No lock	Critical	Critical	☑	☑
13	System	160	SNTP server unreachable	Warning	Warning	☑	☑

Figure 9.11 Global alarm configuration

This page provides an interface to configure globally the behaviour of all alarms. By default ports use the global configuration settings but each port alarm can be configured individually to override these settings.

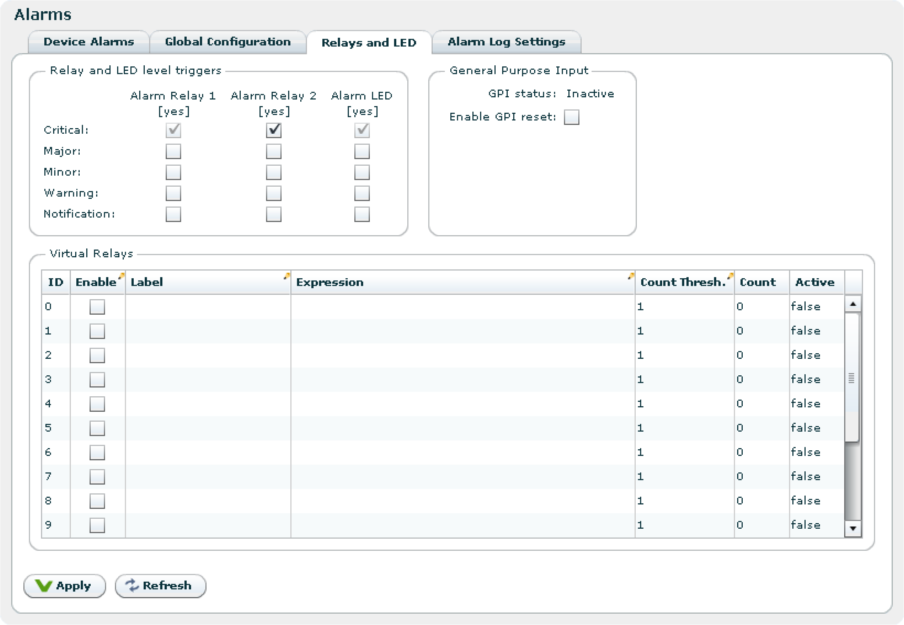
For each alarm a custom severity level can be configured. In addition the alarms can be omitted from the alarm log and trap transmission.

Edited rows are highlighted until changes have been applied.

> **Tip:** For the Log and Send Trap columns, you can quickly select/deselect all items by right-clicking on the header fields in the columns.

9.4.2.3 Relays and LED

This page lets the user configure the alarm severity level that shall turn the relay and alarm LED on. Note that the Alarm relay and the Alarm LED will always be enabled for alarm severity level Critical, as indicated by the disabled check boxes in the Relay and LED level triggers field. The current state of the relay and LED is indicated inside the associated brackets.



Alarms

Relay and LED level triggers

	Alarm Relay 1 [yes]	Alarm Relay 2 [yes]	Alarm LED [yes]
Critical:	☑	☑	☑
Major:	□	□	□
Minor:	□	□	□
Warning:	□	□	□
Notification:	□	□	□

General Purpose Input

GPI status: Inactive

Enable GPI reset: □

Virtual Relays

ID	Enable	Label	Expression	Count Thresh.	Count	Active
0	□			1	0	false
1	□			1	0	false
2	□			1	0	false
3	□			1	0	false
4	□			1	0	false
5	□			1	0	false
6	□			1	0	false
7	□			1	0	false
8	□			1	0	false
9	□			1	0	false

Figure 9.12 Relays and LED configuration

The General purpose input field allows the user to enable pin 9 of the alarm D-SUB connector as a remote reset input. See **Section 7.4**. GPI status indicates if the input signal is active.

For further details on the physical relays refer to **Section A.5.1**.

The Virtual Relays field shown in **Figure 9.12** also includes settings for the so-called *virtual relays*. These are programmable status indicators that can be set to react to any specific alarm condition. In the simplest case you may want to enable a relay in case a specific alarm ID turns up. In another case you may want to enable a relay if a specific alarm turns up on a given port.

Each relay status are exported on SNMP. Activation of a virtual relay also generates a specific alarm, named "Virtual alarm relay activated" (ID=169).

The key element in the settings of the virtual relays is the Expression value. The expression is very close to SQL in syntax and specifies when the relay should be activated. The behaviour is as follows for each virtual relay:

1. Each active alarm event is evaluated against the Expression for the virtual relay (if enabled).

2. If the expression evaluates to `true`, the Count value is increased by 1. You can at any time see the current count value. The Count value simply tells you how many of the current (active) alarm events in the unit that matches the expression.

3. If the count value is larger than or equal (>=) to the Count Thresh. value the relay is activated.

The expressions are validated before they are accepted by the unit. Table 9.1 shows the field values you may enter in an expression.

Table 9.1 Legal field values to use in expressions

Field name	Extracts from event:	Type	Sample expression
id	Alarm ID	Number	`id = 169`
text	Alarm text	Text	`text = 'Defective fan'`
type_num	Type number	Number	`type_num = 13`
type_text	Type text	Text	`type_text = 'port'`
sev	Severity (number 2-6)	Number	`sev = 6`
details	Alarm details (text)	Text	`details = 'PID 113'`
subid1	Alarm *subid1* value	Number	`subid1 = 1`
subid2	Alarm *subid2* value	Number	`subid2 = 2`
subid3	Alarm *subid3* value	Number	`subid3 = 1190`
port	Synonym for *subid2*	Number	`port = 2`
service	Synonym for *subid3*	Number	`service = 102`
pid	Synonym for *subid3*	Number	`pid = 2000`

In the expressions you may enter parentheses to group sub-expressions together. Together with the supported list of operators this gives great flexibility in constructing advanced “match” patterns.

Table 9.2 summarises the operator types you are allowed to use. Please note that the examples below are used for illustration purposes only. For example, the plus and minus operators may not be very useful in practise, but they are included in this table for completeness.

Table 9.2.a Legal operators to use in expressions

Operator	Description	Sample
=	Equal	`id = 169`
!=	Not equal	`id != 169`
AND	Logical AND	`id = 169` AND `port = 2`
OR	Logical OR	`id = 169` OR `id = 200`
IN	Set operator. Returns true if left-hand part is included in set to the right.	`id IN (169,200,201)`
+	Addition	`id + 9 = 169`
-	Subtraction	`id - 8 = 160`
*	Multiply	`id * 10 = 100`
/	Divide	`id / 20 = 8`
>	Greater than	`id > 100`

Table 9.2.b Legal operators to use in expressions

Operator	Description	Sample
<	Less than	`id < 90`
>=	Greater than or equal	`id >= 100`
<=	Less than or equal	`id <= 100`

Some examples are given in **Table 9.3**.

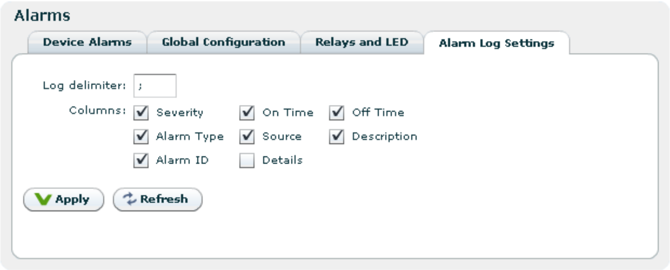
Table 9.3 Expression examples

Task	Expression	Count threshold value
To generate an alarm when any alarm with ID = 200 turns up (independent on source)	`id = 200`	1
To generate an alarm when alarm with ID = 200 turns up on port with ID = 1 (subid2 = 1)	`(id = 200) AND (port = 1)`	1
To generate an alarm when alarm with ID = 200 turns up on both port 1 AND port 2	`(id = 200) AND ((port = 1) OR (port = 2))`	2

Note the last example in the table: Here the count threshold value must be set to 2 to get the expected behaviour. This is because the expression entered matches two different alarm events (port=1 or port=2), and in order to match them both two matches are required in the global alarm list.

9.4.2.4 Alarm log settings

This page is used to set alarm log properties.



Log delimiter: ;

Columns: ☑ Severity ☑ On Time ☑ Off Time
☑ Alarm Type ☑ Source ☑ Description
☑ Alarm ID □ Details

Figure 9.13 Configuring the alarm log

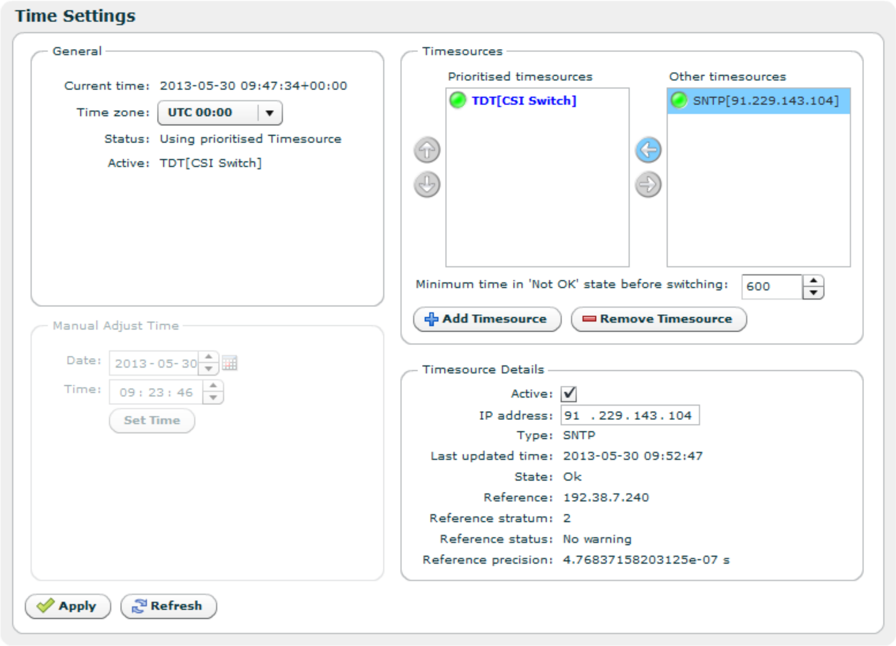
Log delimiter

This parameter is used when exporting the alarm log. It specifies the column separator character. The default value for the delimiter is `;`. The character used may affect auto-importing of the exported file into your favourite tool used to inspect the file content.

Columns

Each of the columns in the alarm log table has a checkbox. Columns that are selected are shown on the alarm log page.

9.4.3 Time Settings



Current time: 2013-05-30 09:47:34+00:00
Time zone: UTC 00:00
Status: Using prioritised Timesource
Active: TDT[CSI Switch]

Date: 2013 - 05 - 30
Time: 09 : 23 : 46

Prioritised timesources: TDT[CSI Switch]
Other timesources: SNTP[91.229.143.104]

Minimum time in 'Not OK' state before switching: 600

Active: ☑
IP address: 91 . 229 . 143 . 104
Type: SNTP
Last updated time: 2013-05-30 09:52:47
State: Ok
Reference: 192.38.7.240
Reference stratum: 2
Reference status: No warning
Reference precision: 4.76837158203125e-07 s

Figure 9.14 Time Settings

The time settings 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 time

The current time as reported by the device.

Time zone

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

Status

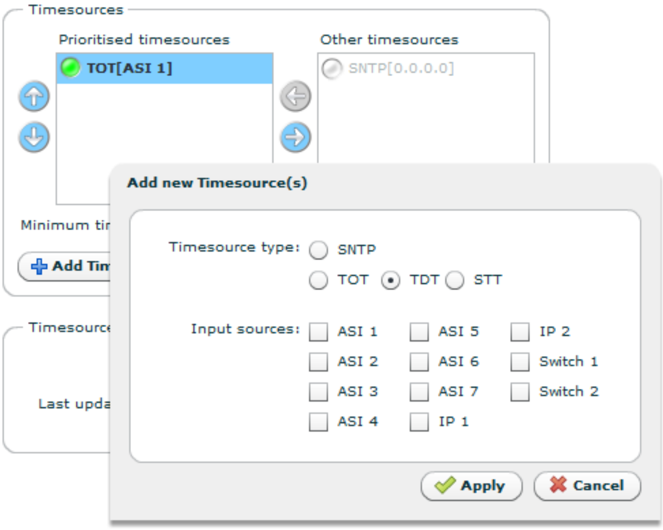
The status of the time synchroniser.

Active

The time source currently in use by the time synchroniser.

The Manual Adjust Time field allows the operator to set the time. The manually configured time will only be used when no other time sources are configured in the Prioritised time sources list.

The Timesource prioritisation field contains two lists showing configured time sources. Disabled time sources are greyed out. Enabled time sources are shown with an indication of the time source status. The list to the right shows time sources that are defined but not used by the time synchroniser. Enabled time sources may be moved to the leftmost list by using the arrow-left button, and back again by using the arrow-right button. Time sources in the left hand list are used by the time synchroniser to set the time. They are listed in prioritised order; the source with the highest priority at the top. The order of priority can be altered by clicking an item in the list and using the up or down arrows to the left of the list to increase or decrease, respectively, the item priority. The time synchroniser will use the time source with the highest priority whose status is "OK" (represented by a green indicator).



Prioritised timesources: ● TOT[ASI 1]

Other timesources: ○ SNTP[0.0.0.0]

Timesource type: ○ SNTP ○ TOT ● TDT ○ STT

Input sources: □ ASI 1 □ ASI 5 □ IP 2 □ ASI 2 □ ASI 6 □ Switch 1 □ ASI 3 □ ASI 7 □ Switch 2 □ ASI 4 □ IP 1

Figure 9.15 Time Settings - Add time source

To add a time source to the system, click the "Add Timesource" button, which brings up the dialog shown in **Figure 9.15** with the following fields:

Timesource type

SNTP

Time source retrieving time from an SNTP server.

Server address

Specify the server IP address here.

TDT TOT or STT

Time source retrieving time from DVB TDT, DVT TOT or ATSC STT time tables on a port.

Input source

Lists ports that can be used as time sources with the selected time source type (**Figure 9.15**. Multiple entries can be selected to add more than one time source. For switched inputs, you may select the time source to get time from the input switch group, which will make the time source retrieve the time from the currently active input in the switch.

To remove time sources, Select them in the list and click the "Remove Timesource" button. Time sources for dynamic ports such as IP inputs and Switch inputs, are automatically removed if the dynamic port is removed.

Located below the lists is also a field to define the maximum allowed time interval between updates from the currently used time source. Exeeding this interval the source is considered "Not OK" and the synchroniser selects the next source in the prioritised list.

Upon selecting a time source, the Timesource Details box at the bottom right of the page provides additional details relating to the selected time source. Depending on the type of time source selected the box may contain some or all of the following parameters:

Active
: A checkbox to enable or disable the time source. Disabled time sources are never updated. Time sources configured and present in the prioritised list must be removed before they can be disabled.

IP address
: Specifies the IP address of an SNTP time server source to poll for updates.

Type
: Type of time source selected. The sources are product dependent, but SNTP is always available.

Last updated time
: The most recent time value received from the time source.

State
: The current state of the time source.

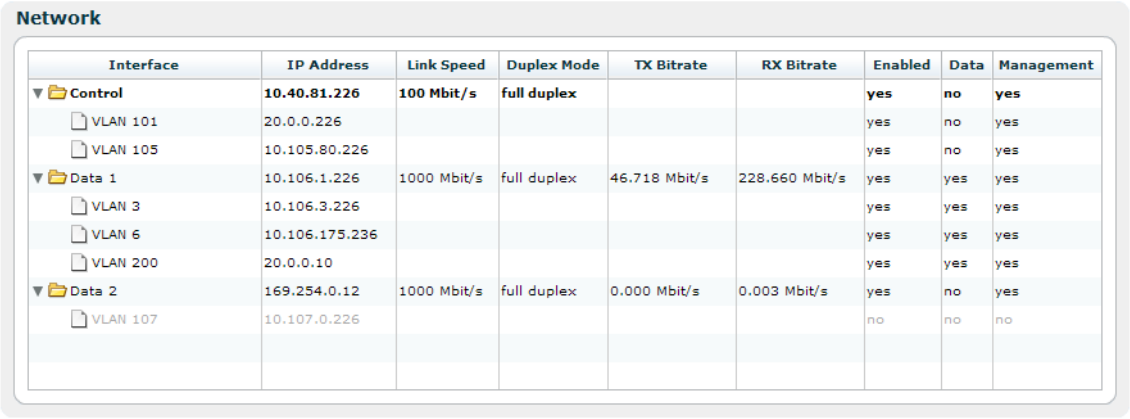
Reference
: Provides the time reference source address of accessed time source.

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

Reference status
: Indicates if the time source is currently governed by a time source at a higher stratum.

Reference precision
: The expected timing accuracy of the current time source.

9.4.4 Network



Network

Interface	IP Address	Link Speed	Duplex Mode	TX Bitrate	RX Bitrate	Enabled	Data	Management
▼ **Control**	**10.40.81.226**	**100 Mbit/s**	**full duplex**			**yes**	**no**	**yes**
VLAN 101	20.0.0.226					yes	no	yes
VLAN 105	10.105.80.226					yes	no	yes
▼ Data 1	10.106.1.226	1000 Mbit/s	full duplex	46.718 Mbit/s	228.660 Mbit/s	yes	yes	yes
VLAN 3	10.106.3.226					yes	yes	yes
VLAN 6	10.106.175.236					yes	yes	yes
VLAN 200	20.0.0.10					yes	yes	yes
▼ Data 2	169.254.0.12	1000 Mbit/s	full duplex	0.000 Mbit/s	0.003 Mbit/s	yes	no	yes
VLAN 107	10.107.0.226					no	no	no

Figure 9.16 Network status

This page presents status information about network interfaces, including virtual (VLAN) interfaces, present on the device. The management interface is always present, and bold characters indicate the web management interface connection. An interface shown in grey colour means that the interface is disabled. There may be physical interfaces on the unit that are not shown in this table as the availability of each interface may vary with the installed software licences and operational mode.

Interface
: A label identifying the interface. If it is a physical interface with virtual interfaces attached to it an arrow is shown. Clicking this arrow will expand/collapse the list of virtual interfaces.

IP Address
: The IP address configured for this interface.

Link Speed
: The current link speed detected for this interface. Applicable to physical interfaces only.

Duplex Mode
: The duplex mode detected for this interface, half or full duplex. Applicable to physical interfaces only.

TX Bitrate
: The bitrate currently transmitted through this interface. Applicable to physical interfaces only.

RX Bitrate
: The bitrate currently received through this interface. Applicable to physical interfaces only.

Enabled
: Shows whether the interface is currently enabled.

Data
: Shows whether data traffic is currently enabled for this interface.

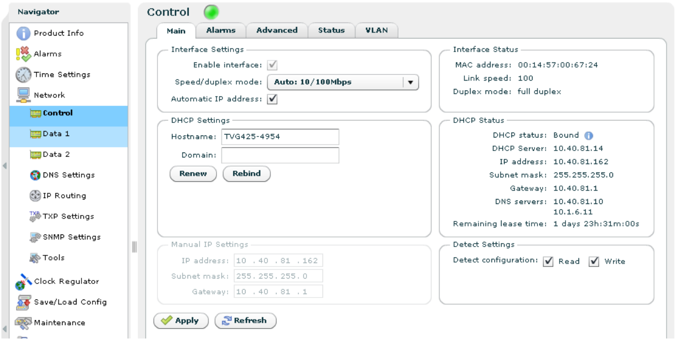
Management

Shows whether management traffic is currently enabled for this interface.

9.4.4.1 Interfaces

Each available network interface has an entry in the Navigator list. Selecting an interface brings up pages where it is possible to configure the interface and view its status. Accessible parameters vary with the interface selected since the functionality of the available interfaces are not necessarily identical.

9.4.4.1.1 Main



Interface Settings
Enable interface: ☑
Speed/duplex mode: Auto: 10/100Mbps
Automatic IP address: ☑

Interface Status
MAC address: 00:14:57:00:67:24
Link speed: 100
Duplex mode: full duplex

DHCP Settings
Hostname: TVG425-4954
Domain:

DHCP Status
DHCP status: Bound
DHCP Server: 10.40.81.14
IP address: 10.40.81.162
Subnet mask: 255.255.255.0
Gateway: 10.40.81.1
DNS servers: 10.40.81.10
10.1.6.11
Remaining lease time: 1 days 23h:31m:00s

Manual IP Settings
IP address: 10 . 40 . 81 . 162
Subnet mask: 255. 255. 255. 0
Gateway: 10 . 40 . 81 . 1

Detect Settings
Detect configuration: ☑ Read ☑ Write

Figure 9.17 Main IP settings

This page provides the main configuration settings for the physical interface.

Caution: Modifying the settings of the interface you are currently using for the GUI application may cause loss of contact with the unit. Make sure you will still be able to contact the unit before applying changed settings.

9.4.4.1.2 Interface Settings

Enable interface

Enables/disables the interface. It is not possible to disable the currently used management interface.

Media Select

Provides a choice between network port Data 2 and the SFP module for the second data interface. Select RJ-45 to use the data port marked Data for data traffic. Select SFP to use the SFP module for data traffic.

Speed/duplex mode

The speed and duplex mode of the interface. The Auto setting enables automatic speed and mode negotiation for the Ethernet link. This option is not available for SFP interfaces.

Note: Modifying the default settings of interface duplex to anything other than auto can cause unpredictable results unless all peer systems accessing the port use similar settings. For more technical information regarding auto negotiation and duplex mismatch, refer to the **Wikipedia duplex mismatch article** (http://en.wikipedia.org/wiki/Duplex_mismatch).

Automatic IP address

Enables automatic IP address assignment using DHCP. This option requires that a DHCP server is present on the network on which the device is connected.

9.4.4.1.3 DHCP Settings

Hostname

The DNS hostname of the interface. This name is sent to the DHCP server with a request to register it at the DNS server. If the name registers correctly, the fully qualified domain name of the interface will be the hostname pluss the domain name assigned by the server.

Domain

Optional field where wanted domain name can be specified. Normally the DHCP decides the domain name for a client, the DHCP server must be set up specifially to allow a client to select a domain name.

Renew button

Press button to renew address now. Renew is done by sending a request for renewal of lease of existing parameters, using uni-cast to DHCP server.

Rebind button

Press to rebind address. Rebind is done by broadcasting a request for the same IP address as previously used.

9.4.4.1.4 DHCP Status

DHCP status

Shows the current state of the DHCP client (RFC2131, Figure 5).

Possible values are:

Disabled

DHCP is not turned on.

Selecting

Client is broadcasting Discover messages and checking for offers from answering DHCP servers. Normally the client should immediately receive and answer and switch to bound state.

Bound

Client has received IP settings and is ready for use.

Renewing
Client is uni-casting request to leasing server to renew previous lease.

Rebinding
Client is broadcasting requests to re-bind to previously assigned address.

Checking
Client is evaluating wether offered IP address is already in use on network.

Backing off
Client received a nack from the server.

DHCP server
The IP of the selected server.

IP address
The IP address assigned to this interface by the server.

Subnet mask
The subnet mask assigned to this interface by the server.

Gateway
The IP address of the gateway to use, assigned by the DHCP server.

DNS servers
Prioritized list of DNS servers to use assigned by the DHCP server. See **Section 9.4.4.2** for manual configuration of DNS server addresses.

Note: If the DNS server is not located on a sub-net local to the unit, it may be required to configure the routing table to route DNS requests to the correct network interface.

Remaining lease time
Time till the IP address must be renewed.

DHCP status info icon

More details on the DHCP client is available on a tool-tip if you hoover over the info icon next to the “DHCP status” parameter. The fields here are:

Domain
The domain name assigned by the DHCP server. The fully qualified domain name of the interface is <hostname>.<domain>

Lease time
The duration of the address lease, specified by the DHCP server.

Renew time/Time to renewal
The renew time specified by the server. Normally the client should transmit a renew request after this time.

Rebind time/Time to rebind
: Time specified by server for re-bind.

Messages transmitted/received
: Number of messages sent and received by the DHCP client.

Last transmission ID
: ID used on last DHCP message transmitted.

9.4.4.1.5 Manual IP Settings

IP address
: IP address of the interface.

Subnet mask
: The subnet mask of the interface.

Gateway
: The default gateway address for the interface.

9.4.4.1.6 Interface Status

MAC address
: The Ethernet Media Access Control (MAC) address of the interface.

Link speed
: Speed of current connection.

Duplex mode
: Shows duplex of current connection.

9.4.4.1.7 Detect Settings

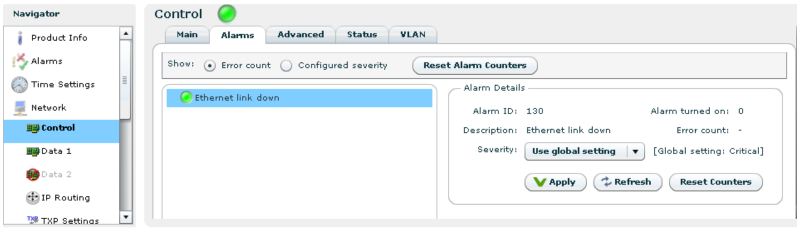
Detect configuration
: Applies to the Control interface, only.

These two boxes enable read and write attributes of the Nevion Detect IP assignment server module. This server is a stand-alone PC application that can be used to discover Nevion devices on a local network and assign IP addresses to them.

Enabling the Read option makes the TNS546 visible for the Nevion Detect on the LAN. If the Write option is enabled the IP address of the TNS546 may be configured using the Nevion Detect. These options do not affect the operation of the device from the management application Nevion Connect.

9.4.4.1.8 Alarms

Alarms related to the interface are listed on the Alarms page. Clicking an alarm opens the field to configure the alarm. Please see Section 9.4.2 for alarm configuration details.



Show: ● Error count ○ Configured severity

Ethernet link down

Alarm Details

Alarm ID: 130 Alarm turned on: 0

Description: Ethernet link down Error count: -

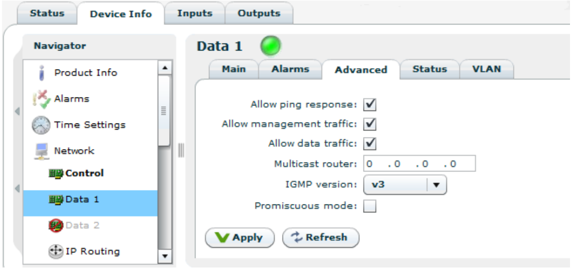
Severity: Use global setting [Global setting: Critical]

Figure 9.18 Network interface alarms

At the top of the page two radio buttons are provided to select between displaying error count or error severity. In addition all alarm counters related to this interface may be reset.

9.4.4.1.9 Advanced

This sub-tab allows configuring advanced IP settings of the interface.



Allow ping response: ☑

Allow management traffic: ☑

Allow data traffic: ☑

Multicast router: 0 .0 .0 .0

IGMP version: v3

Promiscuous mode: □

Figure 9.19 Advanced IP settings

Allow ping response

Check this box to filter incoming ICMP messages. If this option is not enabled the device will not answer ping requests to this port.

Allow management traffic

Tick this box to allow management traffic on this interface. *It is not possible to disable this on the dedicated management interface or on the interface you are currently using for management.*

Allow data traffic

Tick this box to allow data traffic on this interface. *It is not possible to enable data traffic on the management interface.*

Promiscuous mode

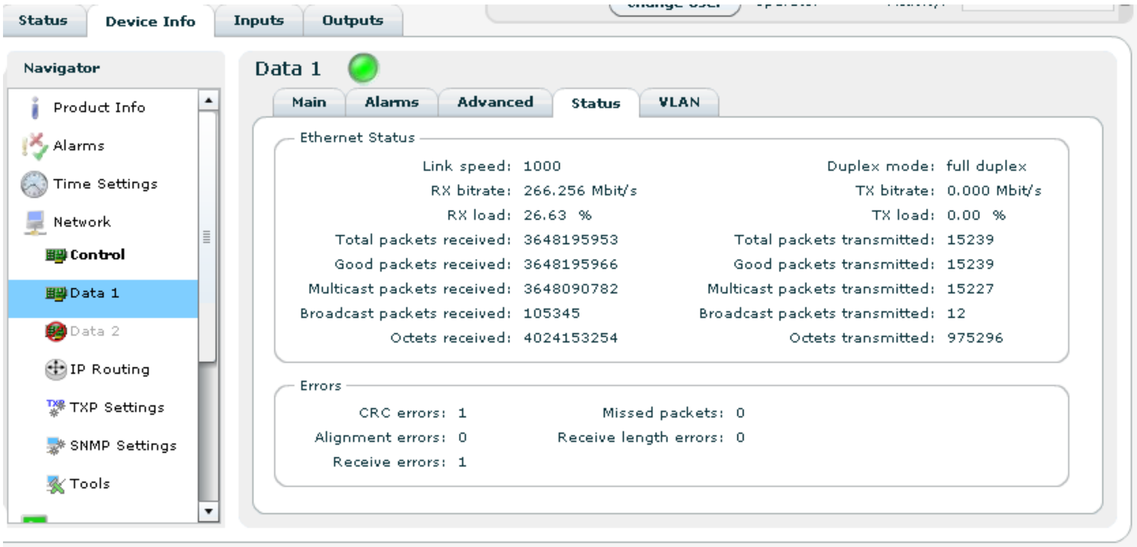
This parameter controls if the data interface is in promiscuous mode. Promiscuous mode is required for IP snooping. *It is not possible to enable promiscuous mode on the management interface.*

IGMP version

This parameter is not shown in the management interface page.

The preferred IGMP version to use. If fixed is selected the unit will keep trying to use the selected version even if it is not supported by the network.

9.4.4.1.10 Status



Data 1

Ethernet Status

Link speed: 1000
Duplex mode: full duplex
RX bitrate: 266.256 Mbit/s
TX bitrate: 0.000 Mbit/s
RX load: 26.63 %
TX load: 0.00 %
Total packets received: 3648195953
Total packets transmitted: 15239
Good packets received: 3648195966
Good packets transmitted: 15239
Multicast packets received: 3648090782
Multicast packets transmitted: 15227
Broadcast packets received: 105345
Broadcast packets transmitted: 12
Octets received: 4024153254
Octets transmitted: 975296

Errors

CRC errors: 1
Missed packets: 0
Alignment errors: 0
Receive length errors: 0
Receive errors: 1

Figure 9.20 Interface Status

This page shows detailed status and error information on the selected physical interface. Different types of interfaces support different status and error parameters; not all parameters listed will be shown for all interface types.

The Ethernet Status field:

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).

The following parameters are available for both received and transmitted packets:

bitrate
: The total bitrate received/transmitted.

load
: Interface load, measured relative to max speed.

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

Good packets
: The number of IP packets received/transmitted containing valid CRCs.

Multicast packets
The number of IP multicast packets received/transmitted by the interface.

Broadcast packets
The number of broadcast packets received/transmitted.

Octets
The number of octets received/transmitted

The Errors field:

CRC errors
Number of packets received with CRC errors.

Alignment errors
Number of packets detected with alignment errors (non-integer number of bytes).

Receive errors
Number of erroneous packets received.

Missed packets
Number of packets missed.

Link symbol errors
Number of link symbol errors detected.

Carrier extension errors
Number of carrier extension errors detected.

Receive length errors
Number of packets with invalid size.

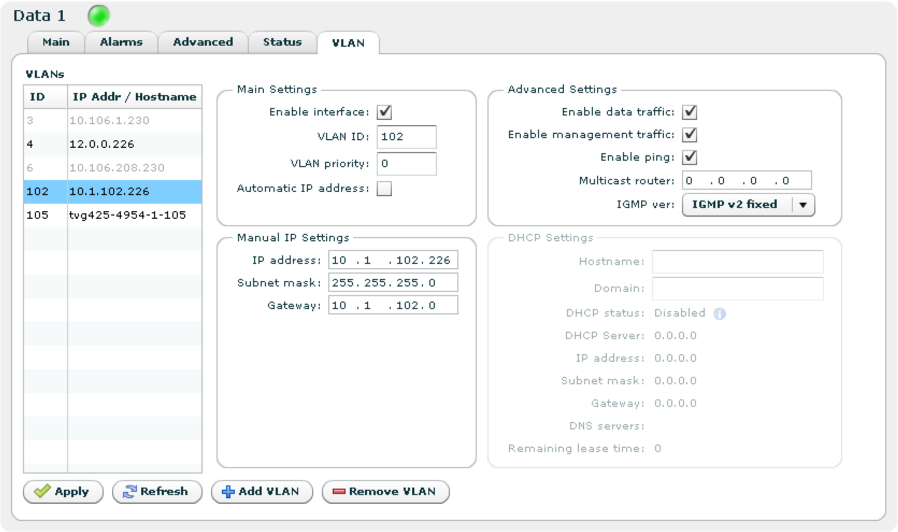
The SFP Info field is only shown if the SFP interface is active. It displays information provided by the SFP module installed.

9.4.4.1.11 VLAN

This page is only shown on interfaces with VLAN (virtual interface) support. The page allows adding, removing and editing virtual interfaces (VLAN) using the selected physical interface. Current VLANs interfaces are shown in the grid on the left, and parameters for each interface are edited by selecting the interface in the grid first.

Once editing is finished, clicking the Apply button will commit all the changes. Hitting Refresh will cancel all changes.

In addition to the Apply and Refresh buttons there are buttons to enable adding and removing VLANs.



Data 1

VLANs

ID	IP Addr / Hostname
3	10.106.1.230
4	12.0.0.226
6	10.106.208.230
102	10.1.102.226
105	tvg425-4954-1-105

Main Settings

Enable interface: ☑
VLAN ID: 102
VLAN priority: 0
Automatic IP address: □

Advanced Settings

Enable data traffic: ☑
Enable management traffic: ☑
Enable ping: ☑
Multicast router: 0 . 0 . 0 . 0
IGMP ver: IGMP v2 fixed ▾

Manual IP Settings

IP address: 10 . 1 . 102 . 226
Subnet mask: 255 . 255 . 255 . 0
Gateway: 10 . 1 . 102 . 0

DHCP Settings

Hostname:
Domain:
DHCP status: Disabled
DHCP Server: 0.0.0.0
IP address: 0.0.0.0
Subnet mask: 0.0.0.0
Gateway: 0.0.0.0
DNS servers:
Remaining lease time: 0

Figure 9.21 VLAN configuration

9.4.4.1.12 Main Settings

Enable interface

Enable/disable the virtual interface.

VLAN ID

The VLAN id of this virtual interface. Must be in the range 1-4094. All virtual interfaces on one physical interface must have a unique id.

VLAN priority

The VLAN priority of this virtual interface. Numers 0 to 7 are valid. For further information on VLAN priority usage, see reference [7].

Automatic IP address

Enables automatic IP address assignment using DHCP. This option requires that a DHCP server is present on the network on which the device is connected.

9.4.4.1.13 Manual IP Settings

IP address

The IP address of the virtual interface.

Subnet mask

The subnet mask of the virtual interface.

Gateway

The gateway address to use for the virtual interface.

9.4.4.1.14 Advanced Settings

Enable data traffic
: Checked box enables the virtual interface to allow video data traffic. Not shown for dedicated management interface.

Enable management traffic
: Checked box enables the virtual interface to allow management traffic.

Enable ping
: Checked box enables the virtual interface to respond to ping messages.

Multicast router
: The multicast router for this virtual interface. Only visible if multicast is allowed.

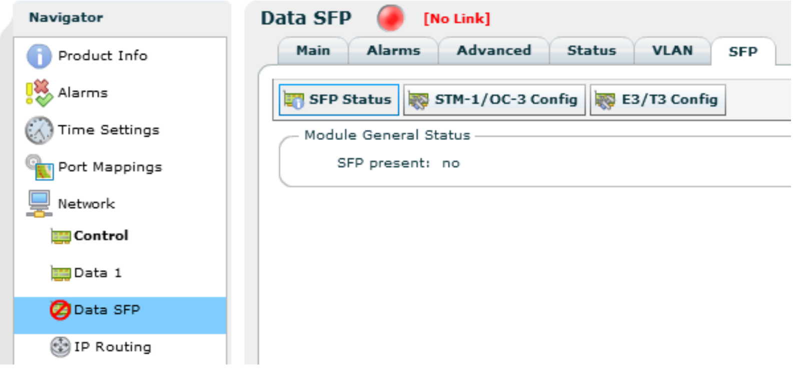
IGMP ver
: Provides selection of the IGMP version to use. *Not applicable to the "Control" interface*.

9.4.4.1.15 DHCP settings and status

Please refer to **Section 9.4.4.1.1.2** and **Section 9.4.4.1.1.3** for a description of the parameters related to DHCP, which are identical to the ones on the main tab.

9.4.4.1.16 SFP

The SFP tab is visible for the second network interface if this interface is set to use SFP. How to enable the SFP is described in section 9.4.8.1 , provided the appropriate licence has been installed .



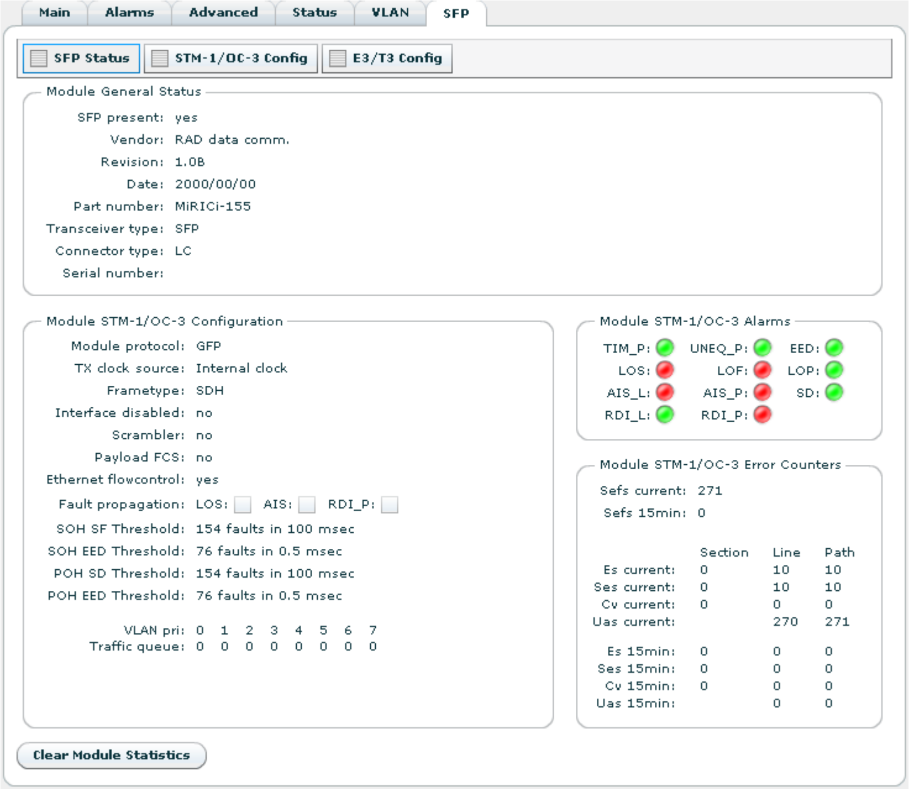
Module General Status

SFP present: no

Figure 9.22 The Device Info > Network > SFP tab

The SFP tab gives access to three sub-pages: SFP Status, STM-1/OC-3 Config and E3/T3 Config. The two configuration sub-pages reflect that separate configuration files are used to configure the different SFP module types. For each module type the TNS546 stores a configuration file that can be edited "off-line". These pages are visible only if SFP configuration has been licensed. The settings will not be committed to the module until writing of the file is expressly initiated.

The **SFP Status** page, shown in figure **Figure 9.23**, provides an overview of the module status. The appearance of the status page and the range of parameters shown depend on the type of module attached.



Module General Status

```
      SFP present: yes
           Vendor: RAD data comm.
         Revision: 1.0B
             Date: 2000/00/00
      Part number: MiRICi-155
 Transceiver type: SFP
   Connector type: LC
    Serial number:
```

Module STM-1/OC-3 Configuration

```
     Module protocol: GFP
     TX clock source: Internal clock
           Frametype: SDH
  Interface disabled: no
           Scrambler: no
         Payload FCS: no
 Ethernet flowcontrol: yes
   Fault propagation: LOS: □  AIS: □  RDI_P: □
    SOH SF Threshold: 154 faults in 100 msec
   SOH EED Threshold: 76 faults in 0.5 msec
    POH SD Threshold: 154 faults in 100 msec
   POH EED Threshold: 76 faults in 0.5 msec

           VLAN pri: 0  1  2  3  4  5  6  7
       Traffic queue: 0  0  0  0  0  0  0  0
```

Module STM-1/OC-3 Alarms

TIM_P:	🟢	UNEQ_P:	🟢	EED:	🟢
LOS:	🔴	LOF:	🔴	LOP:	🟢
AIS_L:	🔴	AIS_P:	🔴	SD:	🟢
RDI_L:	🟢	RDI_P:	🔴		

Module STM-1/OC-3 Error Counters

Sefs current: 271

Sefs 15min: 0

	Section	Line	Path
Es current:	0	10	10
Ses current:	0	10	10
Cv current:	0	0	0
Uas current:		270	271
Es 15min:	0	0	0
Ses 15min:	0	0	0
Cv 15min:	0	0	0
Uas 15min:		0	0

Figure 9.23 The SFP status page

The Module General Status field displays the status of the module as seen by the TNS546.

SFP Present
: Indicates that the module has been detected by the TNS546.

Vendor
: Shows the vendor name.

Revision
: Indicates the module revision.

Date
: Indicates the revison date.

Part number
: The module part number.

Transceiver type
: The type of transceiver inside the SFP module. Only a limited range of transceivers is compatible with the TNS546.

Connector type
: Indicates the network connector type.

Serial number
: The serial number of the SFP module.

The Module <type> Configuration field shows the internal functional status as read back from the module. The field heading will reflect whether a STM-1/OC-3 or an E3/T3 module is installed. A discussion of the parameters shown is included in the Config pages description.

The Module (type) Alarms field is shown if the STM-1/OC-3 module is present and shows all link related alarms settings of the module. Red indicates that the alarm has been raised.

TIM-P
: Trace ID Mismatch (Path)

LOS
: Loss of Signal

AIS_L
: Alarm Indication Signal (Line)

RDI_L
: Remote Defect Indication (Line)

UNEQ_P
: Payload Label Mismatch (Path)

LOF
: Loss of Frame

AIS_P
: Alarm Indication (Path)

RDI_P
: Remote Defect Indication (Path)

EED
: Excessive Error Defect

LOP
: Loss of Point

SD
: Signal Degrade

Refer to product specific documentation for further discussion of these parameters.

The Module (type) Link Status field is shown if the E3/T3 module is present and shows the status of all link related alarm settings of the module. Red indicates that the alarm has been raised.

BV
: Bipolar Violation

LCV
: Line Coding Violation

LOS
: Loss of Signal

RDI
: Remote Detection Indication

WLD
: WAN Loop Detected

EZ
: Excessive Zeroes

PCV
: P-bit Coding Violation

OOF
: Out of Frame

LLD
: Lan Loop Detected

LOL
: LIU Out of Lock

CCV
: C-bit Coding Violation

AIS
: Alarm Indication Signal

SS
: System Status.

Refer to product specific documentation for further discussion of these parameters.

The Module (type) Error Counters field displays errors as they occur, counted during a 15 minute period. Es = Errored seconds, Ses = Severely errored seconds, Cv = Coding violations, Uas = Line unavailable seconds

Current
: The counter increments every time an error is detected, resetting every second.

15mins
: Displays the result of the previous 15 minutes counting interval.

  Section
  : "Section" related error counts

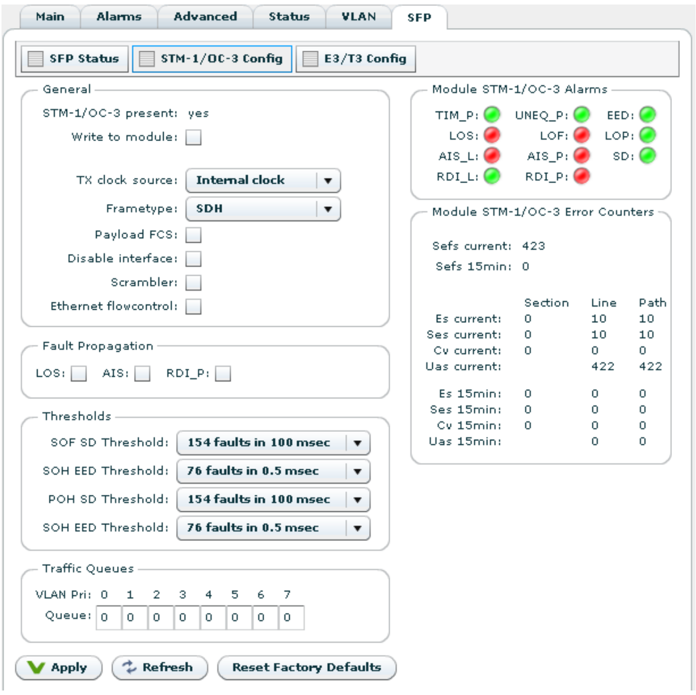
  Line
  : "Line" related error counts

  Path
  : "Path" related error counts

At the page bottom is the Clear Module Statistics button. Clicking this will flush all error counters.

The **STM-1/OC-3 Config** page.

The STM-1/OC-3 module provides an optical interface for high speed data communications in SDH or SONET networks. This page provides access to change the configuration settings of the module. As shown in figure Figure 9.24 the page contains four fields to set operational parameters. The Alarms and Error counters fields are identical to those described for the SFP Status sub-page. Editing the configuration settings will alter the SFP configuration file stored in the TNS546, only.



General

STM-1/OC-3 present: yes
Write to module: □

TX clock source: Internal clock
Frametype: SDH
Payload FCS: □
Disable interface: □
Scrambler: □
Ethernet flowcontrol: □

Fault Propagation

LOS: □ AIS: □ RDI_P: □

Thresholds

SOF SD Threshold: 154 faults in 100 msec
SOH EED Threshold: 76 faults in 0.5 msec
POH SD Threshold: 154 faults in 100 msec
SOH EED Threshold: 76 faults in 0.5 msec

Traffic Queues

VLAN Pri:	0	1	2	3	4	5	6	7
Queue:	0	0	0	0	0	0	0	0

Module STM-1/OC-3 Alarms

TIM_P:	🟢	UNEQ_P:	🟢	EED:	🟢
LOS:	🔴	LOF:	🔴	LOP:	🟢
AIS_L:	🔴	AIS_P:	🔴	SD:	🟢
RDI_L:	🟢	RDI_P:	🔴		

Module STM-1/OC-3 Error Counters

Sefs current: 423
Sefs 15min: 0

	Section	Line	Path
Es current:	0	10	10
Ses current:	0	10	10
Cv current:	0	0	0
Uas current:		422	422
Es 15min:	0	0	0
Ses 15min:	0	0	0
Cv 15min:	0	0	0
Uas 15min:		0	0

Figure 9.24 The configuration page for the STM-1/OC-3 SFP module

In the General field the main operational parameters are set.

STM-1/OC-3 present
: Indicates if the module has been detected by the TNS546.

Write to module
: This box must be checked to allow the configuration file be written to the SFP module. If the box is not checked the configuration file may still be edited without affecting the module. If the box is checked the configuration file is written to the module every time the Apply button is clicked.

Tx clock source
: The transmitter clock may be internally generated, or derived from the received data stream.

Frame type
: Select SDH or SONET, respectively, according to the accessed network.

Payload FCS (Frame check sequence)
: Check this box to enable FCS error detection.

Disable interface
: Not available.

Scrambler
: Tick this box to enable the module internal scrambler. Must be ticked to successfully receive scrambled network data.

Ethernet flow control
: A tick enables flow control of Ethernet data from the TNS546 to the SFP module. Flow control prevents data overflow in the SFP module buffer. Buffer overflow leads to data loss that would go unnoticed until attempting to decode the data at the receiving end.

In the Fault Propagation field check boxes allow to select which network fault(s) shall cause shutdown of the Ethernet data flow:

LOS
: Loss of signal

AIS
: Alarm indication signal

RDI_P
: Remote defect indication

In the Thresholds field bit error rate measurements indicate an estimate of the network link quality. The check boxes allow selection of pre-defined threshold BER values to raise alarms. For further details refer to the vendor SFP user manual.

SOH SD
: Section Overhead, degraded Signal Defect

SOH EED
: Section Overhead, Excessive Error Defect

POH SD
: Path Overhead, degraded Signal Defect

POH EED
: Path Overhead, Excessive Error Defect

The Taffic Queues field allows mapping of network traffic queues to VLAN priorities. For information on VLAN priority usage refer to [7].

To aid troubleshooting while changing configuration the Module Alarm and Module Error Counters fields of the status page are replicated here.

At the bottom of the page are three buttons:

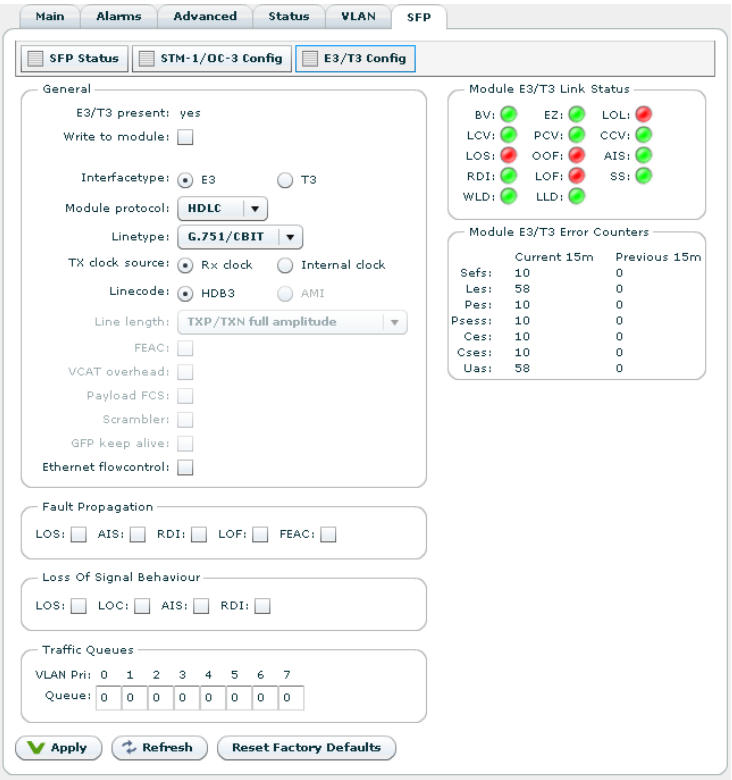
Apply
: Writes changes to the SFP configuration file. Also initiates writing the configuration file to the module if the Write to module box has been ticked.

Refresh
: Cancels changes that have been entered.

Reset Factory Defaults
: Only active if the Write to module box has not been ticked. Clicking this button returns the module to factory default settings but will not affect the settings of the configuration page. The status of the SFP module is at all times displayed in the SFP Status sub-page.

The **E3/T3 Config** page.

The E3T3 module provides an electrical interface for high speed data communications in E3 or T3 networks. This page provides access to change the configuration settings of the module. As shown in figure **Figure 9.25** the page contains four fields to set operational parameters. Editing the configuration settings will alter the SFP configuration file stored in the TNS546, only.



General

E3/T3 present: yes
Write to module: □
Interfacetype: ● E3 ○ T3
Module protocol: HDLC
Linetype: G.751/CBIT
TX clock source: ● Rx clock ○ Internal clock
Linecode: ● HDB3 ○ AMI
Line length: TXP/TXN full amplitude
FEAC: □
VCAT overhead: □
Payload FCS: □
Scrambler: □
GFP keep alive: □
Ethernet flowcontrol: □

Fault Propagation

LOS: □ AIS: □ RDI: □ LOF: □ FEAC: □

Loss Of Signal Behaviour

LOS: □ LOC: □ AIS: □ RDI: □

Traffic Queues

VLAN Pri:	0	1	2	3	4	5	6	7
Queue:	0	0	0	0	0	0	0	0

Module E3/T3 Link Status

BV: 🟢 EZ: 🟢 LOL: 🔴
LCV: 🟢 PCV: 🟢 CCV: 🟢
LOS: 🔴 OOF: 🔴 AIS: 🟢
RDI: 🟢 LOF: 🔴 SS: 🟢
WLD: 🟢 LLD: 🟢

Module E3/T3 Error Counters

	Current 15m	Previous 15m
Sefs:	10	0
Les:	58	0
Pes:	10	0
Psess:	10	0
Ces:	10	0
Cses:	10	0
Uas:	58	0

Figure 9.25 The configuration page for the E3/T3 SFP module

E3/T3 present
: Indicates if the module has been detected by the TNS546.

Write to module
: This box must be checked to allow the configuration file be written to the SFP module. If the box is not checked the configuration file may still be edited without affecting the module. If the box is checked the configuration file is written to the module every time the Apply button is clicked.

Interface type
: Click the appropriate button for the network used.

Module protocol
: Allows selecting the desired data link protocol for the network; HDLC (High Level Data Link Control), GFP (Generic Frame Protocol) or cHDLC (Cisco extension to HDLC).

Line type
: Line protocol selection. Choices vary according to the interface type and data link protocol selected.

Tx clock source
: The transmitter clock may be internally generated, or derived from the received data stream.

Line code
: Must be HDB3 for an E3 interface. Select between B3ZS and AMI for a T3 interface.

Line length
: Only applicable for a T3 interface. Allows the output signal to be adjusted according to the line length to reach the termination point.

FEAC
: Far end alarm and control indication. Only applicable for a T3 interface using G.751 line protocol.

VCAT overhead
: Only applicable when using the GFP data link protocol. VCAT allows arbitrary grouping of VCAT members (STS1 or STS3c timeslots) to accommodate any bandwidth.

Payload FCS (Frame check sequence)
: For error detection. Only applicable when using the GFP data link protocol.

Scrambler
: Only applicable when using the GFP data link protocol. Tick this box to enable the module internal scrambler. Must be ticked to successfully receive scrambled network data.

GFP keep alive
: If enabled, sends 2-3 keep alive messages per second. Enable this parameter if Loss of Frame (LOF) indication is frequently encountered. Generally relevant to older equipment types. Only applicable when using the GFP data link protocol in a T3 interface.

Ethernet flow control
: A tick enables flow control of Ethernet data from the TNS546 to the SFP module. Flow control prevents data overflow in the SFP module buffer. Buffer overflow leads to data loss that would go unnoticed until attempting to decode the data at the receiving end.

In the Fault Propagation field check boxes allow to select which TDM network fault(s) shall cause shut-down of the ethernet data flow:

LOS
: Loss of signal

AIS
: Alarm indication signal

RDI
: Remote defect indication

LOF
: Loss of frame

FEAC
: Far end alarm and control

Whether or not RDI, LOF and FEAC are applicable depends on Interface type, Module protocol and Line type settings.

In the Loss of Signal Behaviour field check boxes allow selecting which TDM condition shall send an LOS indication to the Ethernet interface:

LOS
: Loss of signal

LOC
: Receive loss of lock

AIS
: Alarm indication signal

RDI
: Remote defect indication

The Taffic Queues field allows mapping of network traffic queues to VLAN priorities. For information on VLAN priority usage refer [7].

To aid troubleshooting while changing the configuration the Module Alarm and Module Error Counters fields of the status page are replicated here.

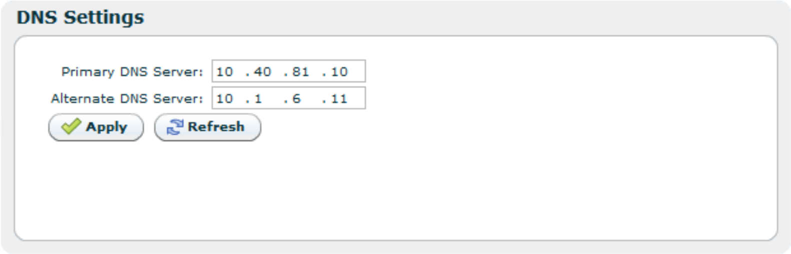
At the bottom of the page are three buttons:

Apply
: Writes changes to the SFP configuration file. Also initiates writing the configuration file to the module if the Write to module box has been ticked.

Refresh
: Cancels changes that have been entered.

Reset Factory Defaults
: Only active if the Write to module box has not been ticked. Clicking this button returns the module to factory default settings. This will not affect the settings of the configuration page. The status of the SFP module is at all times displayed in the SFP Status sub-page.

9.4.4.2 DNS Settings



DNS Settings

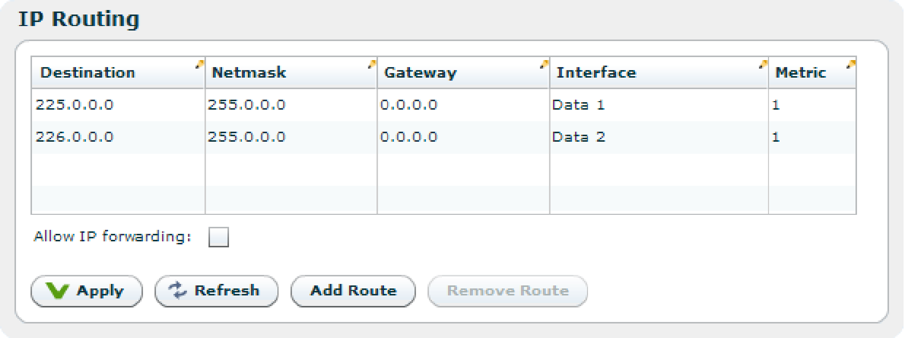
Primary DNS Server: 10 .40 .81 .10

Alternate DNS Server: 10 .1 .6 .11

Figure 9.26 DNS settings

The DNS settings page lets you configure a main and secondary DNS server IP address. The DNS server is used to map names to IP addresses.

9.4.4.3 IP Routing



IP Routing

Destination	Netmask	Gateway	Interface	Metric
225.0.0.0	255.0.0.0	0.0.0.0	Data 1	1
226.0.0.0	255.0.0.0	0.0.0.0	Data 2	1

Allow IP forwarding: ☐

Figure 9.27 IP Routing

The IP Routing table lets the user configure IP routing rules for the unit. These rules tell the unit which interface to send IP traffic to, based on the destination IP address of the traffic.

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

Netmask
: The subnet mask to use for matching against this routing rule.

Gateway
: The IP destination to send a packet to if the destination address of the packet is on a different subnet than the destination interface.

Interface
: IP packets matching this rule will be sent through this interface.

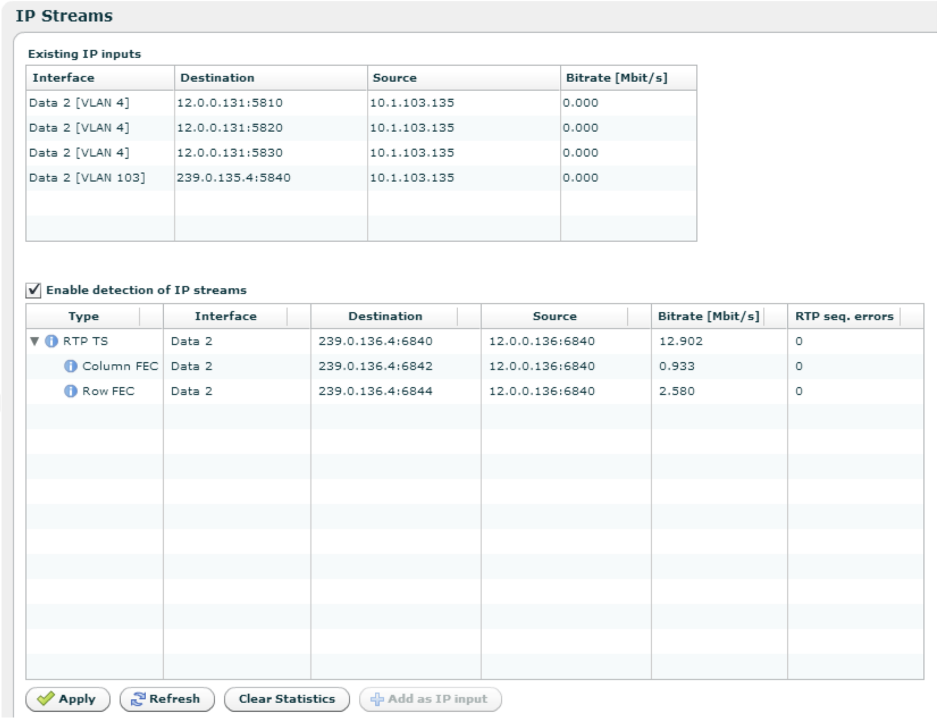
Metric
: The metric of the routing rule. If more than one rule matches a destination address the rule with the lowest metric will be used.

When an IP packet is sent from the unit the destination address of the packet is matched against the configured routing rules. If the destination address matches one or more rules the rule with the lowest metric will be used. The packet will then be forwarded to the interface determined by this rule. If the destination address is on a different subnet than the configured interface the packet will be sent to the gateway determined by the rule.

Below the table is a checkbox where the user can Allow IP forwarding. If enabled incoming TCP packets that are not addressed to the unit will be forwarded to an interface according to the routing rules. The receiving interface must have management traffic enabled to forward TCP traffic to a different interface.

> **Note:** Modifying the IP routing rules may cause loss of contact with the unit. Make sure you will still be able to contact the unit with the new settings before applying the changes.

9.4.4.4 IP Streams



IP Streams

Existing IP inputs

Interface	Destination	Source	Bitrate [Mbit/s]
Data 2 [VLAN 4]	12.0.0.131:5810	10.1.103.135	0.000
Data 2 [VLAN 4]	12.0.0.131:5820	10.1.103.135	0.000
Data 2 [VLAN 4]	12.0.0.131:5830	10.1.103.135	0.000
Data 2 [VLAN 103]	239.0.135.4:5840	10.1.103.135	0.000

☑ Enable detection of IP streams

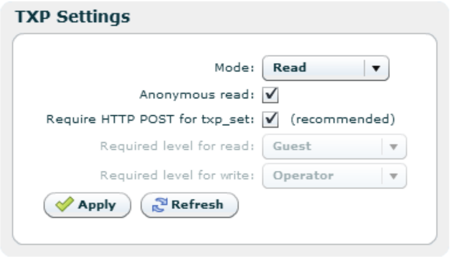
Type	Interface	Destination	Source	Bitrate [Mbit/s]	RTP seq. errors
▼ ⓘ RTP TS	Data 2	239.0.136.4:6840	12.0.0.136:6840	12.902	0
ⓘ Column FEC	Data 2	239.0.136.4:6842	12.0.0.136:6840	0.933	0
ⓘ Row FEC	Data 2	239.0.136.4:6844	12.0.0.136:6840	2.580	0

Figure 9.28 IP Streams

The IP streams page is divided into two parts. The top part shows the existing configured IP inputs, while the bottom part shows detected IP streams if this feature is enabled. The IP streams detection lists all the TsOIp streams visible on the physical data interfaces and on all VLAN interfaces. Typically this list will contain Multicast streams, and Unicast streams transmitted to this unit. If there are FEC streams, they will be detected and linked to the corresponding data streams.

By selecting one or more streams, one may create TS channels by clicking “Add as IP input”. When adding an IP stream as an input, the stream will be moved up to the “Existing IP inputs” view.

9.4.4.5 TXP Settings



TXP Settings

Mode: Read

Anonymous read: ☑

Require HTTP POST for txp_set: ☑ (recommended)

Required level for read: Guest

Required level for write: Operator

Figure 9.29 TXP Settings

TXP is a Nevion proprietary HTTP/XML based protocol designed to retrieve configuration and status information using WEB/HTTP requests. TXP exists side by side with an SNMP agent and provides an alternative way to access data in a product. TXP and SNMP therefore complement each other.

This page contains settings to determine how the unit should respond to TXP queries.

Mode
: Controls the mode of the TXP server. If set to Disabled, all TXP accesses are disabled.

Anonymous read
: Selects whether read accesses should be allowed without entering user credentials. This may only be edited if Mode is different from Disabled.

Require HTTP POST for txp_set
: Recommended to reduce risk of unwanted configuration changes.

Required level for read
: The required user level for TXP read accesses. This may only be edited if Mode is different from Disabled and Anonymous read is not selected.

Required level for write
: The required user level for TXP write accesses. This may only be edited if Mode is set to Write.

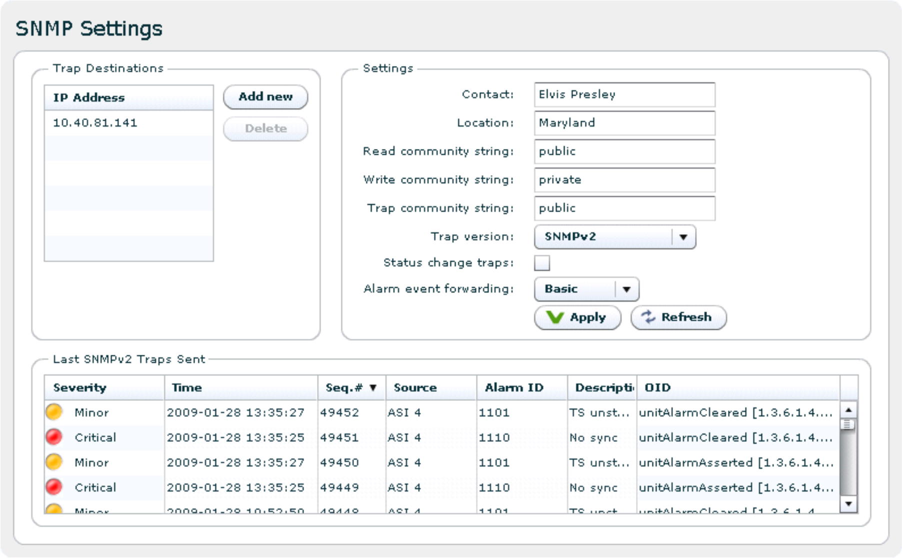
Below follows a simple example of how to get the units uptime.

```
http://10.0.0.10/txp_get?path=/dev/time|_select:uptimetxt

<response request_id="0" method="txp_get" time_stamp="2012-08-17 11:14:20" version="1.0">
  <status status="0" status_text="OK"/>
  <data>
    <dev>
      <time uptimetxt="49 days 21h:56m:09s"/>
    </dev>
  </data>
</response>
```

9.4.4.6 SNMP Settings

The Simple Network Management Protocol (SNMP) is used to monitor network-attached devices for conditions that warrant administrative attention. This page gives access to SNMP settings such as destination IP addresses of trap receivers and community string. It Also displays a log of the latest traps sent by the unit.



SNMP Settings

Trap Destinations

IP Address
10.40.81.141

Settings

Contact: Elvis Presley
Location: Maryland
Read community string: public
Write community string: private
Trap community string: public
Trap version: SNMPv2
Status change traps: □
Alarm event forwarding: Basic

Last SNMPv2 Traps Sent

Severity	Time	Seq.# ▼	Source	Alarm ID	Descripti	OID
● Minor	2009-01-28 13:35:27	49452	ASI 4	1101	TS unst...	unitAlarmCleared [1.3.6.1.4....
● Critical	2009-01-28 13:35:25	49451	ASI 4	1110	No sync	unitAlarmCleared [1.3.6.1.4....
● Minor	2009-01-28 13:35:27	49450	ASI 4	1101	TS unst...	unitAlarmAsserted [1.3.6.1.4...
● Critical	2009-01-28 13:35:25	49449	ASI 4	1110	No sync	unitAlarmAsserted [1.3.6.1.4...
● Minor	2009-01-28 10:52:50	49448	ASI 4	1101	TS unst	unitAlarmCleared [1.3.6.1.4

Figure 9.30 SNMP Settings

The Trap Destination table lets the user configure the trap servers that should receive SNMP traps from the unit. To add a server click the Add new button, enter an IP address, then click the Apply button. To delete an entry select a server entry from the list and click the Delete button.

The Settings group of parameters configures MIB-2 parameters and SNMP password protection. The SNMP version to use for traps, version 1 or version 2, may be selected. When selecting to transmit SNMPv2 traps, two additional options are applicable.

Status change traps
: Selecting this causes a trap to be transmitted each time the overall device status changes.

Alarm event forwarding
: Configures which alarms to forward as SNMP traps. The drop-down list has the following options:

  Disabled
  : No traps are transmitted when alarms appear or disappear. If the Status change traps check box is checked, device status traps are still transmitted.

  Basic
  : The device forwards alarm events as SNMP traps. If there are several sub-entries only a single trap is transmitted.

Detailed
: The device forwards alarm events as SNMP traps. If there are several sub-entries, an SNMP trap is transmitted for each sub-entry.

The table at the bottom of the page shows the most recent SNMP traps sent by the device.

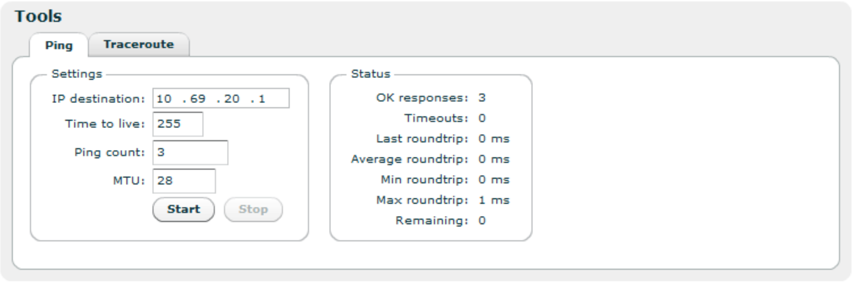
For more information about the configuration settings for SNMP, please refer to **Section 10.4** in **Chapter 10: SNMP**.

9.4.4.7 Tools

The tools menu contains helpfull tools for network debugging.

9.4.4.7.1 Ping

The ping tool can be used to check for connectivity between devices. It is especially useful to ping the receiving data port from the IP transmitter to see if the receiver can be reached.



Settings
IP destination: 10 .69 .20 .1
Time to live: 255
Ping count: 3
MTU: 28

Status
OK responses: 3
Timeouts: 0
Last roundtrip: 0 ms
Average roundtrip: 0 ms
Min roundtrip: 0 ms
Max roundtrip: 1 ms
Remaining: 0

Figure 9.31 The Ping tool

IP destination
: The IP address of the receiving data port. The ping messages will be routed to the matching Ethernet port, either data or management, or to the port configured as default management interface if the specified IP address does not match either of the two sub-nets. Note that if you are pinging between data interfaces, the Allow ping response option on the network page Advanced tab (see **Section 9.4.4.1.3**) must be enabled both in the transmitter and the receiver.

> **Note:** When the IP destination is a multicast address one cannot expect to receive a response to a ping request. It is recommended to test connectivity using the device's actual IP address.

TTL (Time To Live)
: Enter the time to live value for the ping messages here. The time to live value is a field in the IP protocol header that is decremented once for each router that the datagram passes. When the count reaches 0, the datagram is discarded. You can use this to check the number of routers between the transmitter and the receiver by starting with a low value and increment it until ping responses are received. TTL is also specified for each data channel on the IP transmitter, and must be high enough to reach the receiver. Values range from 1 to 255.

Ping count
: The number of ping messages to send. The messages are transmitted with an interval of about 1 second.

MTU
: Maximum Transfer Unit. Specify a length for the ICMP frames to check that frames with given length pass through the network. The ICMP data payload size is adjusted to yield Ethernet frames with the specified length. The ping messages are transmitted with the "don't fragment" bit set.

Start
: Press this button to start the pinging sequence configured above. The status of the ping sequence is displayed in the status frame. Status values are reset on pressing the start button. After pressing the start button the label switches to Stop, and the button can be pressed again to cancel the pinging sequence.

OK responses
: The number of ping responses received.

Timeouts
: The number of ping requests that were not answered. If the timeout counter is incrementing while the OK responses counter is zero, there is no contact with the specified IP address.

Last roundtrip
: The round trip time measured for the last ping request in units of milliseconds.

Average roundtrip
: The average round trip time measured for the ping requests in this session. The value is reset every time the start button is pressed.

Min roundtrip
: The shortest round trip time registered for the ping requests in this session.

Max roundtrip
: The longest round trip time measured for the ping requests in this session.

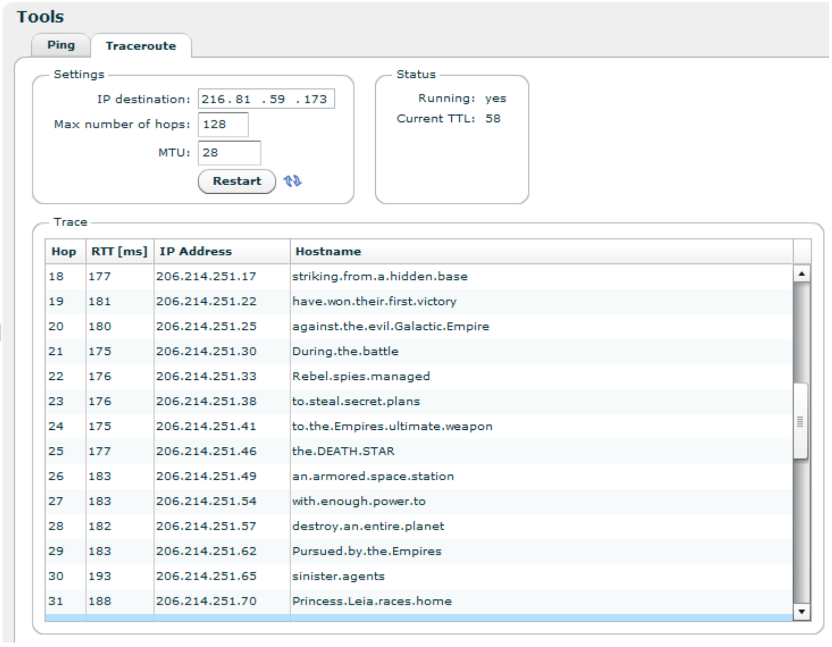
Remaining
: The number of remaining ping requests in this session.

9.4.4.7.2 Traceroute

The traceroute tool can be used to debug the network connectivity with a given host by tracking the router hops between the TNS546 and the host. Traceroute uses ICMP ping messages with increasing TTL to track the router hops.

Settings

IP Destination
: The IP address of the host to check. IP routing decides which interface the ICMP messages are sent on.



IP destination: 216.81 .59 .173

Max number of hops: 128

MTU: 28

Running: yes

Current TTL: 58

Hop	RTT [ms]	IP Address	Hostname
18	177	206.214.251.17	striking.from.a.hidden.base
19	181	206.214.251.22	have.won.their.first.victory
20	180	206.214.251.25	against.the.evil.Galactic.Empire
21	175	206.214.251.30	During.the.battle
22	176	206.214.251.33	Rebel.spies.managed
23	176	206.214.251.38	to.steal.secret.plans
24	175	206.214.251.41	to.the.Empires.ultimate.weapon
25	177	206.214.251.46	the.DEATH.STAR
26	183	206.214.251.49	an.armored.space.station
27	183	206.214.251.54	with.enough.power.to
28	182	206.214.251.57	destroy.an.entire.planet
29	183	206.214.251.62	Pursued.by.the.Empires
30	193	206.214.251.65	sinister.agents
31	188	206.214.251.70	Princess.Leia.races.home

Figure 9.32 The Traceroute tool

Number of hops

This parameter sets a roof to the number of hops that are tracked. Normally this parameter can be set fairly low.

MTU

Maximum Transfer Unit. This parameter can be used to transmit messages with a given length. ICMP messages are transmitted with the don't fragment bit set to yield errors when MTU of a link is too small for the frame.

Status

Running

State of tracer.

Current TTL

Increasing for each new hop traced.

Trace

Grid showing routers encountered.

Hop

Hop number.

RTT[ms]

Round trip time measured in milliseconds for message returned from router at this point in chain.

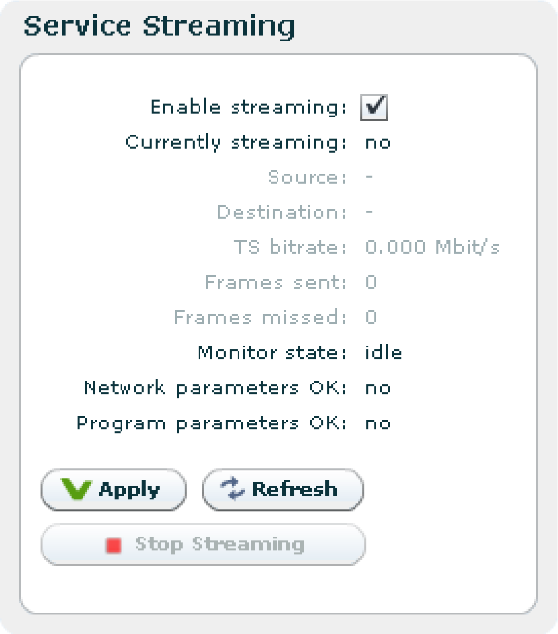
IP Address

IP address of router at this point.

Hostname
DNS resolved host name for IP Address. For this column to be filled in, DNS must be supported and a DNS server must have been defined either manually or by DHCP client.

9.4.5 Service streaming

The streaming feature allows any transport stream to be redirected to the management computer console, enabling an instant check of the service. Successful streaming can only be accomplished if suitable player software is installed on the computer. The player must support the open XSPF file format[1], which e.g. is supported by the commonly available VLC media player[2]. Service streaming is enabled from the *Inputs* tab, see section 9.5.2.1


Service Streaming

Enable streaming: ☑
Currently streaming: no
Source: -
Destination: -
TS bitrate: 0.000 Mbit/s
Frames sent: 0
Frames missed: 0
Monitor state: idle
Network parameters OK: no
Program parameters OK: no

Figure 9.33 Streaming status

This page displays the streaming status of the device and allows any streaming in progress to be terminated. It provides an instant check of the service being streamed. The parameters listed have the following significance:

Enable streaming
This box must be ticked to allow streaming to be performed. Click “Activate” to make the change.

Currently streaming
Indicates if RTP frames are being transmitted

[1] http://xspf.org
[2] http://videolan.org

Source
: Identifies the input port of the service and the service ID

Destination
: Shows the IP address and port number of the computer requesting the stream, which will indicates if the streaming has been initiated from a different computer

TS bitrate
: Indicates the bitrate of the service transport stream

Frames sent
: The accumulated number of RTP frames since the streaming session started

Frames missed
: Number of missed RTP frames

Monitor state
: Indicates "idle" if no active streaming session; "active" when a streaming session is on-going

Network parameters OK
: Indicates "yes" if the network specific parameters signalled in the stream are in order

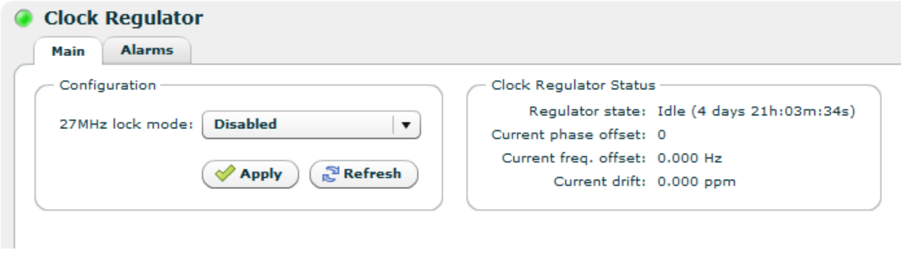
Program parameters OK
: Indicates if the program specific parameters signalled in the stream are in order

The *Stop Streaming* button at the bottom of the page is enabled only if a streaming session is in progress and hence can be stopped.

9.4.6 Clock Regulator

This page lets the user configure synchronisation of the internal 27 MHz clock from an external source.

9.4.6.1 Main


Clock Regulator

Configuration
27MHz lock mode: Disabled

Clock Regulator Status
Regulator state: Idle (4 days 21h:03m:34s)
Current phase offset: 0
Current freq. offset: 0.000 Hz
Current drift: 0.000 ppm

Figure 9.34 Clock regulator

The reference signal is supplied on a separate connector. This page gives access to selecting how the reference is used.

The Configuration field:

27 MHz lock mode

Disabled
: The internal clock will not make use of an external reference signal.

Lock to external 1 PPS
: Configures the internal clock to use the external 1 PPS input connector as reference.

The Clock Regulator Status field:

Regulator state

Idle
: External reference signal is disabled.

Waiting
: External Reference signal is enabled, but the internal clock has not obtained lock to the reference

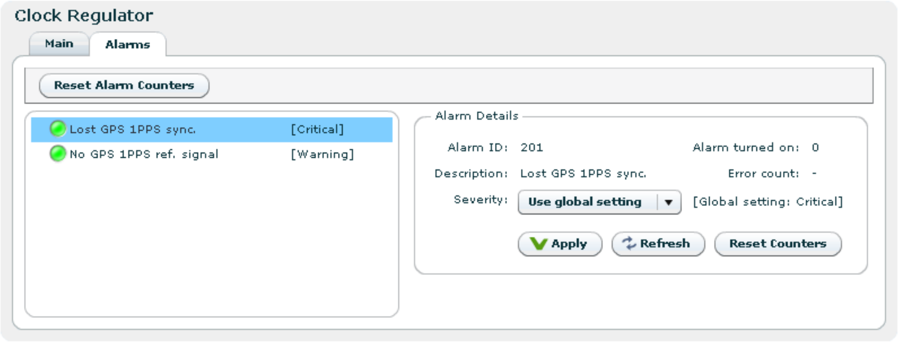
Fine tune
: External Reference signal is enabled, and the internal clock has obtained lock to the reference.

Current phase offset
: Phase offset between the internal clock and 1 PPS clock reference given as a multiple of 3.704 ns (one period of 270 MHz)

Current freq. offset
: Frequency offset between the internal clock and 1 PPS clock reference.

Current drift
: Compensated frequency offset between external and internal reference.

9.4.6.2 Alarms



● Lost GPS 1PPS sync. [Critical]
● No GPS 1PPS ref. signal [Warning]

Alarm ID: 201
Alarm turned on: 0
Description: Lost GPS 1PPS sync.
Error count: -
Severity: Use global setting ▾ [Global setting: Critical]

Figure 9.35 Clock regulator Alarms

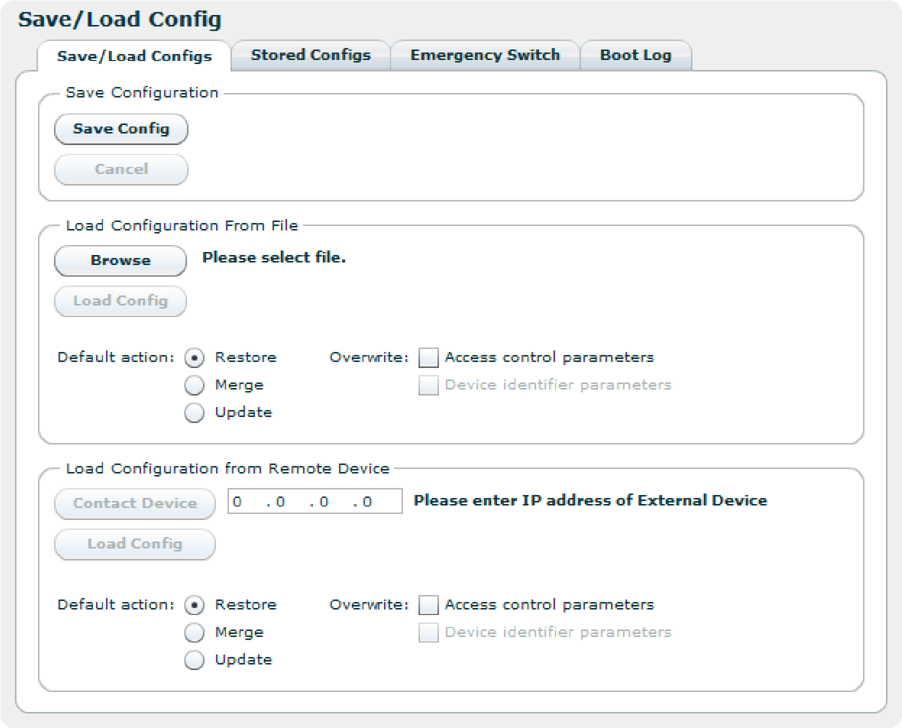
These are the Clock regulator specific alarms. Clicking an alarm opens the field to configure the alarm. Please see **Section 9.4.2** for alarm configuration details.

9.4.7 Save/Load Config

This page provides an interface for managing the device configuration as “snapshots”. From here, snapshots of the device configuration settings can be taken and stored locally, or exported from the device as XML files. Also, previously stored snapshots may be imported and applied.

The device allows for up to 8 configuration snapshots to be stored and managed locally, not including the current running configuration.

9.4.7.1 Save/Load Configs



Please select file.

Default action: ● Restore ○ Merge ○ Update

Overwrite: □ Access control parameters □ Device identifier parameters

0 . 0 . 0 . 0 Please enter IP address of External Device

Default action: ● Restore ○ Merge ○ Update

Overwrite: □ Access control parameters □ Device identifier parameters

Figure 9.36 Saving and loading of configuration files

9.4.7.1.1 Save Configuration

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 cancelling.

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.

9.4.7.1.2 Load Configuration From file

The Load Configuration field of the page provides a means 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 minimising 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 colour 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 behaviour can be changed with the load options, please see **Section 9.4.7.1.4** for a desciption 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.

9.4.7.1.3 Load Configuration from Remote Device

The Load Configuration from Remote Device makes it easy to copy the configuration of another device to this device. This device will therefore be a clone of the remote device, except for device specific parameters such as IP addresses and product name. Loading a configuration from Remote Device is essentially equal to saving the configuration file of another device, and uploading it to this device.

The configuration field includes the IP address of the remote device. Entering an IP address and pressing the Contact Device button will check if the connection is valid and display some information about the device if successful. If the connection is valid, the Load Config button will become clickable.

> **Note:** It is possible, but not advisable, to load configuration from other model types. Even if loading from the same model type, loading a configuration might also fail, especially if the two devices have different feature sets. See **Section 9.4.8.1** for a list of features.

Please see next chapter (**Section 9.4.7.1.4**) for a description of the load options.

9.4.7.1.4 Load options

These options are used to modify the behaviour on configuration loading. The options are available when loading from a file (**Section 9.4.7.1.2**) and when loading from a remove device (**Section 9.4.7.1.3**) .

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 configuation 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

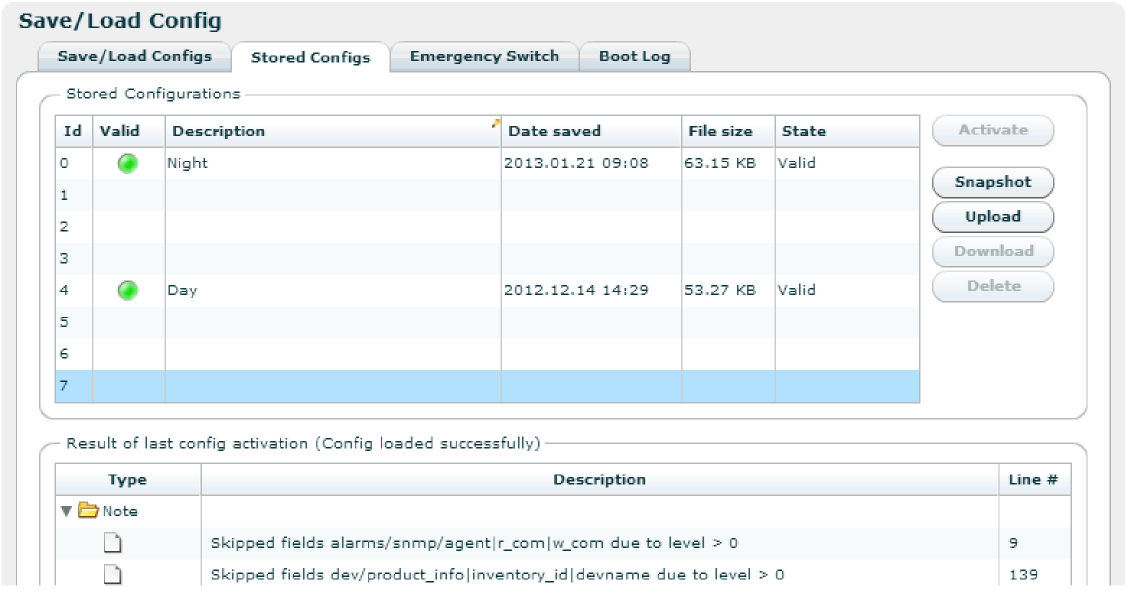
Tick off his check box to overwrite the device identifiers device name and inventory ID. Ethernet Interface IP addresses are not overwritten using this option.

9.4.7.2 Boot Log

This page shows the configuration database status log from the configuration loading at last reboot. If the configuration is rejected at boot the previous configuration will not be replaced. This page may then be inspected to find the reason for rejection.

9.4.7.3 Stored Configs

This page provides an interface to management on-device stored configuration snapshots. Up to 8 full system configuration snapshots can be stored.



Stored Configurations

Id	Valid	Description	Date saved	File size	State
0	●	Night	2013.01.21 09:08	63.15 KB	Valid
1					
2					
3					
4	●	Day	2012.12.14 14:29	53.27 KB	Valid
5					
6					
7					

Result of last config activation (Config loaded successfully)

Type	Description	Line #
Note		
	Skipped fields alarms/snmp/agent|r_com|w_com due to level > 0	9
	Skipped fields dev/product_info|inventory_id|devname due to level > 0	139

Figure 9.37 Locally stored configuration files

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

Id

Each entry in the table has an id in the range from 0 to 7.

Valid

Indicates if the uploaded configuration is valid. Configuration that are valid may be activated without errors. A valid configuration is indicated by a green indicator and a invalid configuration is indicated by a red indicator. A silver indicator in this column signifies that the slot is empty and available.

Description

An snapshot descriptive text can be entered in this field by clicking on the field itself and typing text. The length of this field is limited to a maximum of 64 characters.

Date saved

Time stamp when the configuration was uploaded to the unit.

File size

Size of the configuration file.

State

Extra information regarding the configuration.

To the right of the tables several buttons are provided to perform actions on the snapshots:

Activate
: Loads the selected snapshot as the active configuration of the device. The administrator will be prompted to verify the decision as this action will overwrite any unsaved changes on the device.

Snapshot
: Stores the current running configuration as a snapshot in the slot selected in the snapshot table. This operation will overwrite the snapshot currently stored in that position without prior notification.

Upload
: Import a locally stored configuration file.

Download
: Download selected configuration file to disk.

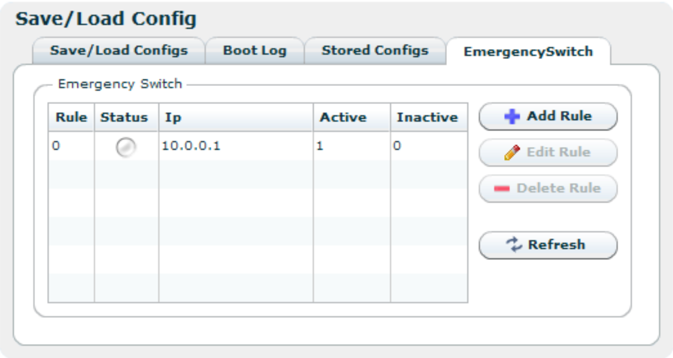
Delete
: Delete the entry selected in the snapshot list.

At the bottom of the page is the Results of last config action field, which will show the result of the last action performed.

9.4.7.4 Emergency Switch

This feature allows the TNS546 to communicate with a central emergency switch unit. The emergency switch unit is designed to facilitate simultaneous configuration switching of all units under its supervision. In this way the operational mode of a comprehensive system may be changed at the press of a single button. Contact Nevion for further information on the emergency switch unit.

Communication with the emergency switch is IP based using the UDP protocol. Each unit enabled for emergency switch control polls the emergency switch repetitively to determine the switch position. The Emergency Switch tab provides the means to configure the behaviour of the TNS546 under emergency switch control.



Rule	Status	Ip	Active	Inactive
0	○	10.0.0.1	1	0

Figure 9.38 Emergency switch

The table lists the rules that have been set up for the emergency switch. Several rules may be configured, albeit only one should be enabled at any one time.

Rule
The list position.

Status

- Green if the rule is enabled and connection to the switch unit is ok.
- Red if the rule is enabled and the connection to the switch is down.
- Grey if the rule is not enabled.

Ip
The IP address of the Emergency Switch unit.

Active
The ID of the configuration that shall be applied when the switch is in the active state.

Inactive
The ID of the configuration that shall be applied when the switch is in the inactive state.

To the right of the table, buttons are provided to set up the switching rule(s):

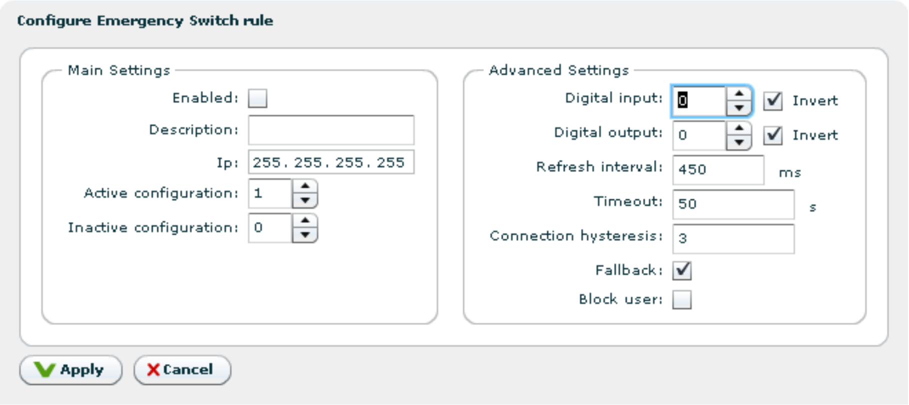
Add Rule
Opens the configuration pane to configure a new switching rule, see **Figure 9.39**.

Edit Rule
Opens the configuration pane for the selected switching rule. See **Figure 9.39**.

Delete Rule
Deletes the selected switching rule.

Refresh
Refreshes the list display.

Configure Emergency Switch rule



Configure Emergency Switch rule

Main Settings

Enabled: □
Description:
Ip: 255.255.255.255
Active configuration: 1
Inactive configuration: 0

Advanced Settings

Digital input: 0 ☑ Invert
Digital output: 0 ☑ Invert
Refresh interval: 450 ms
Timeout: 50 s
Connection hysteresis: 3
Fallback: ☑
Block user: □

Figure 9.39 Configuring the emergency switch

The Main settings field has the following parameters:

Enabled
: A tick in the box enables this rule.

Description
: User defined description of the rule.

Ip
: The IP address of the emergency switch unit.

Active configuration
: The ID of the configuration that shall be applied when the emergency switch is active. This ID must be the ID of a valid configuration from the Stored Configurations list.

Inactive configuration
: The ID of the configuration that shall be applied when the emergency switch is inactive. This ID must be the ID of a valid configuration from the Stored Configurations list.

The Advanced settings field has the following parameters

Digital input
: For future use.

Digital output
: For future use.

Refresh interval
: The time between each poll of the emergency switch state.

Timeout
: Maximum time to wait for a return message from the emergency switch unit.

Connection hysteresis
: Number of timouts allowed before the connection to the emergency switch unit is considered broken.

Fallback
: If this box is ticked the Inactive configuration is applied if the connection with the emergency switch is broken. Othewise the currently applied configuration will remain when the connection is broken.

Block user
: If this box is ticked no user may change the configuration of this unit if the emergency switch is in the active state.

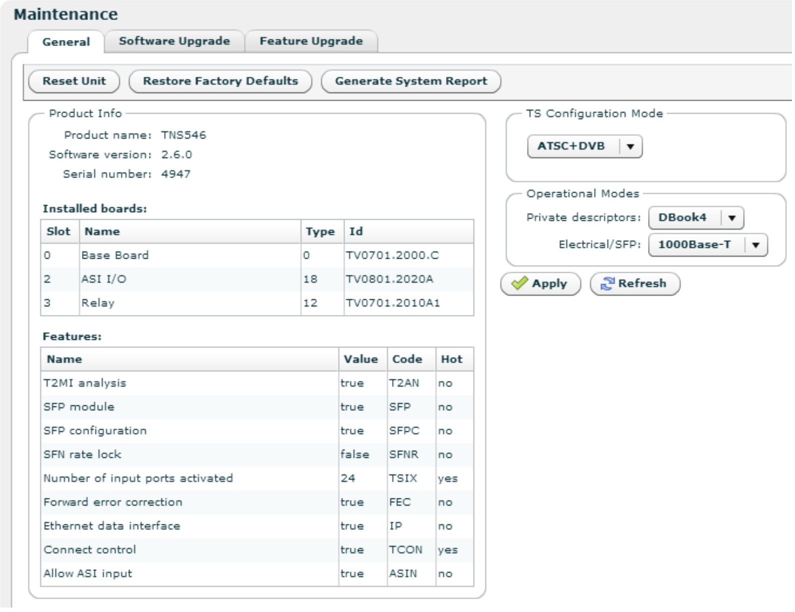
At the bottom of the pane the Apply button is used to confirm and apply changes made; the Cancel button is used to discard changes and close the pane.

9.4.8 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.

9.4.8.1 General



Product Info

Product name: TNS546
Software version: 2.6.0
Serial number: 4947

Installed boards:

Slot	Name	Type	Id
0	Base Board	0	TV0701.2000.C
2	ASI I/O	18	TV0801.2020A
3	Relay	12	TV0701.2010A1

Features:

Name	Value	Code	Hot
T2MI analysis	true	T2AN	no
SFP module	true	SFP	no
SFP configuration	true	SFPC	no
SFN rate lock	false	SFNR	no
Number of input ports activated	24	TSIX	yes
Forward error correction	true	FEC	no
Ethernet data interface	true	IP	no
Connect control	true	TCON	yes
Allow ASI input	true	ASIN	no

TS Configuration Mode

ATSC+DVB ▾

Operational Modes

Private descriptors: DBook4 ▾
Electrical/SFP: 1000Base-T ▾

Figure 9.40 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.

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.

Serial number

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

Installed boards

The name and serial numbers of the circuit boards installed in each of the internal interface slots of the unit.

Features

A list of features relevant to the device and their state (e.g. true, false or the number of ports supported).

Name

Name of the feature

Value

State of the feature or number of licenced items

Code

The factory order code used to identify this feature

Hot

Whether the licence can be upgraded without rebooting the device or not. If the field reads 'yes', no reboot will be required after loading a licence upgrade file.

The TS Configuration Mode field allows the user to select DVB or ATSC operational mode.

The choices are:

DVB

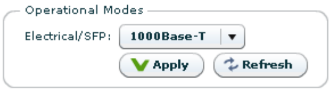
DVB transport streams only are accepted.

ATSC+DVB

Both ATSC and DVB streams are accepted.

> **Caution:** When switching mode from DVB to ATSC+DVB (or vice versa), the unit configuration is set back to factory defaults and it is then rebooted.

if the SFP Module SW licence key is installed, the Operational Modes frame is visible and provides the option Electrical/SFP as shown in figure 9.41. This option is used to allocate the Data-2 IP input to operate through the Electrical Ethernet data interface, or through the SFP slot.



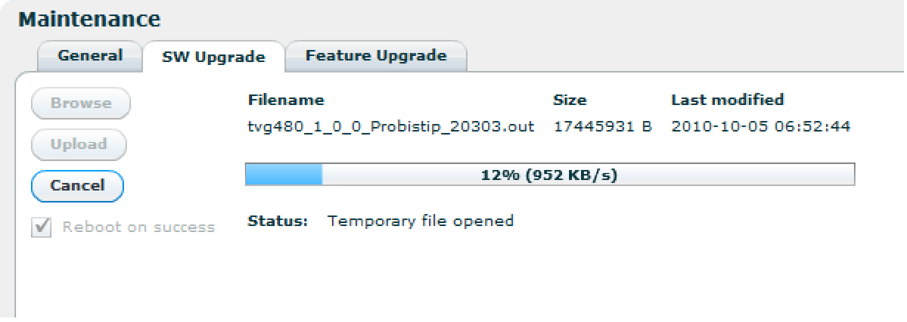
Operational Modes

Electrical/SFP: 1000Base-T

Figure 9.41 SFP and Electrical Ethernet select

When switching mode the unit will automatically reboot. The device configuration is kept but references to Data-2 will be invalid.

9.4.8.2 Software Upgrade



Filename	Size	Last modified
tvg480_1_0_0_Probistip_20303.out	17445931 B	2010-10-05 06:52:44

12% (952 KB/s)

Status: Temporary file opened

Figure 9.42 Software Upgrade

The Software Upgrade sub-page lets the user upgrade the software of the device. The page contains three buttons and a checkbox:

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

Upload
: Once an image file is specified by using the Browse button, the Upload button is used to transmit the file from the administrator PC to the device. 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 on success option has been unchecked.

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

Cancel
: The Cancel button is enabled during the upload process and can be clicked to cancel the operation. It is not possible to continue a cancelled upload.

Reboot on success
: This checkbox is checked by default but can be unchecked to disable automatic reboot upon SW loading completion. If this option is not checked the SW will load but will not be activated before the user performs a manual reboot. Note that this option is not stored on the device, and Reboot on success will be enabled next time you enter the SW upgrade page.

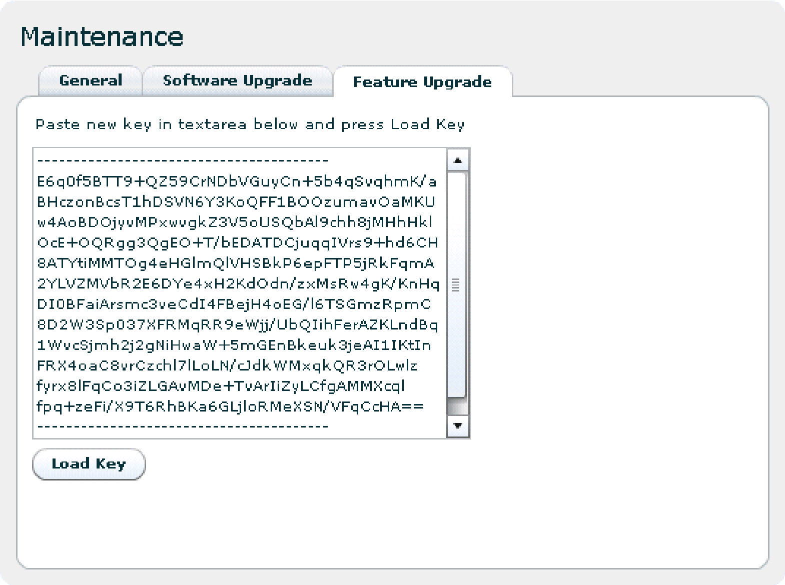
During SW loading, an alarm SW loading in progress is set with the Details field displaying the IP address of the machine from which the loading was initiated. The alarm is turned off when the loading is completed or terminated.

If the Reboot on success option is active the unit will automatically reboot when loading is complete, otherwise an alarm New SW pending is set to indicate that a new SW will be used on next manual reboot.

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 9.4.1**) to verify that the update was successful and the latest software revision is active.

9.4.8.3 Feature Upgrade



Paste new key in textarea below and press Load Key

```
----------------------------------------
E6q0f5BTT9+QZ59CrNDbVGuyCn+5b4qSvqhmK/a
BHczonBcsT1hDSVN6Y3KoQFF1BOOzumavOaMKU
w4AoBDOjyvMPxwvgkZ3V5oUSQbAl9chh8jMHhHkl
OcE+OQRgg3QgEO+T/bEDATDCjuqqIVrs9+hd6CH
8ATYtiMMTOg4eHGlmQlVHSBkP6epFTP5jRkFqmA
2YLVZMVbR2E6DYe4xH2KdOdn/zxMsRw4gK/KnHq
DI0BFaiArsmc3veCdI4FBejH4oEG/l6TSGmzRpmC
8D2W3Sp037XFRMqRR9eWjj/UbQIihFerAZKLndBq
1WvcSjmh2j2gNiHwaW+5mGEnBkeuk3jeAI1IKtIn
FRX4oaC8vrCzchl7lLoLN/cJdkWMxqkQR3rOLwlz
fyrx8lFqCo3iZLGAvMDe+TvArIiZyLCfgAMMXcql
fpq+zeFi/X9T6RhBKa6GLjloRMeXSN/VFqCcHA==
----------------------------------------
```

Figure 9.43 Feature Upgrade page

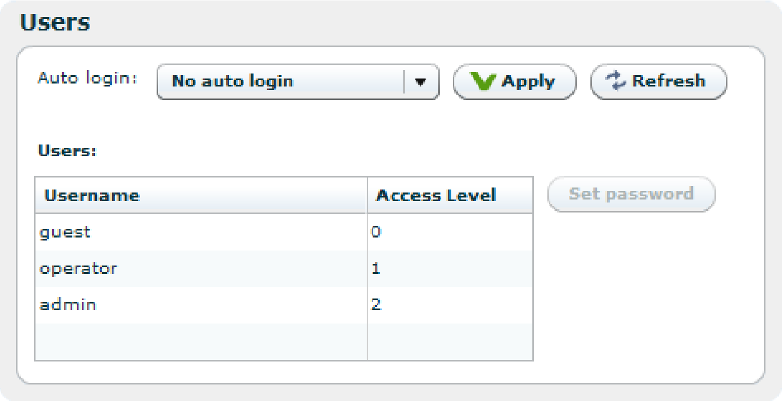
The Feature Upgrade sub-page provides an interface to upload new software licences to upgrade the feature set of the device. The licence key is provided as a text file. Paste the content of file into the text area and click the Load Key button.

Some features do not require a restart of the device when upgraded, they are marked as "hot" in the feature list. If you load a licence changing only hot-upgradable keys, you will get a message back in the load text box telling you that no reboot is required. If any non-hot licence has changed, the device needs to be restarted to activate the new feature(s).

Reset can be performed from the GUI as explained on the Maintenance > General tab in **Section 9.4.8.1**.

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

9.4.9 Users



Users

Auto login: No auto login

Users:

Username	Access Level
guest	0
operator	1
admin	2

Figure 9.44 Users page

The Users page provides a configuration interface for user management. Settings are provided for configuring a password for each privilege level and for configuring automatic login settings. You must have administrator previledges to alter the settings.

Auto login

Specifies the user privilege level to use for automatic login to the device. Changing this feature from the default ("No auto login") to another setting bypasses the initial login screen (**Figure 9.2**) encountered by default.

Users

Each user privilege level has an account name and password. The account name is fixed for each level and therefore cannot be changed. Each privilege level, however, has an administrator definable password.

To modify the password for a given privilege level select the user name from the list and click the Set password button. The administrator is then prompted with a dialogue requesting a new password.

Three user privilege levels are available.

guest

Can view configuration information and alarm logs

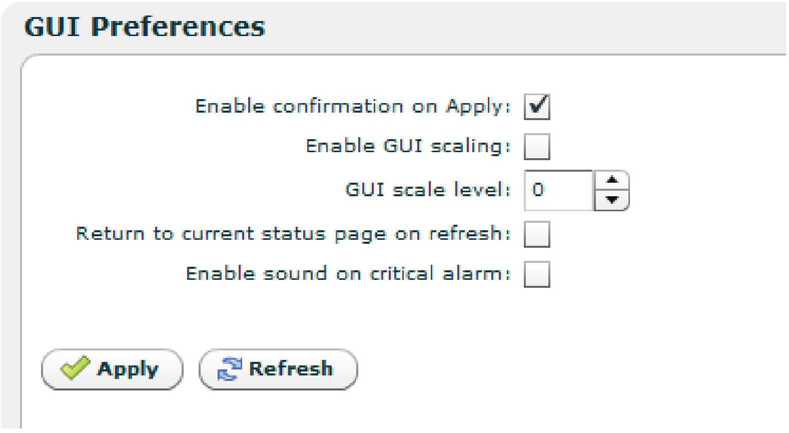
operator

Can configure the settings on the device, but can not alter passwords

admin

Device administrator, full access to the device.

9.4.10 GUI Preferences



GUI Preferences

Enable confirmation on Apply: ☑

Enable GUI scaling: □

GUI scale level: 0

Return to current status page on refresh: □

Enable sound on critical alarm: □

Figure 9.45 GUI Preferences page

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 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.

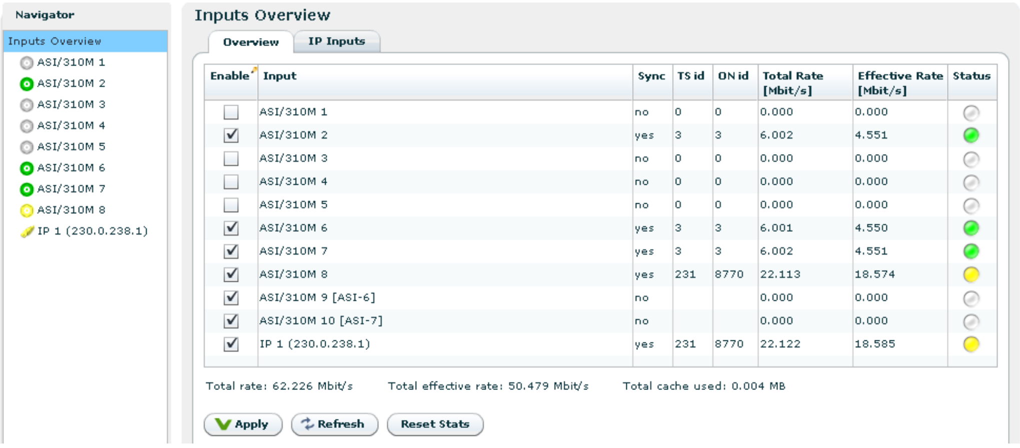
Note: 'Enable confirmation on Apply' is stored on the device, while the other options are stored as browser cookies and thereby only affect the local browser and PC.

9.5 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 labelling of the inputs is a combination of the user defined name of the input and the physical number of the input port.

9.5.1 Inputs Overview



Enable	Input	Sync	TS id	ON id	Total Rate [Mbit/s]	Effective Rate [Mbit/s]	Status
□	ASI/310M 1	no	0	0	0.000	0.000	○
☑	ASI/310M 2	yes	3	3	6.002	4.551	🟢
□	ASI/310M 3	no	0	0	0.000	0.000	○
□	ASI/310M 4	no	0	0	0.000	0.000	○
□	ASI/310M 5	no	0	0	0.000	0.000	○
☑	ASI/310M 6	yes	3	3	6.001	4.550	🟢
☑	ASI/310M 7	yes	3	3	6.002	4.551	🟢
☑	ASI/310M 8	yes	231	8770	22.113	18.574	🟡
☑	ASI/310M 9 [ASI-6]	no			0.000	0.000	○
☑	ASI/310M 10 [ASI-7]	no			0.000	0.000	○
☑	IP 1 (230.0.238.1)	yes	231	8770	22.122	18.585	🟡

Total rate: 62.226 Mbit/s   Total effective rate: 50.479 Mbit/s   Total cache used: 0.004 MB

Figure 9.46 Inputs Overview

The Inputs Overview page shows a short table summary of all the inputs of the device. The table has the following columns:

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

Input
: The name of the input, consisting of the factory defined label with the physical port number and the user defined name.

Sync
: Displays "yes" if the unit has synchronised to this transport stream input.

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

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

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

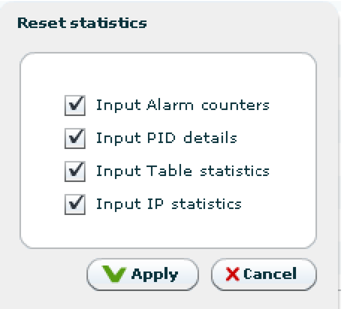
Below the table three values as shown. They are:

Total input rate
: The combined total bitrates of all the transport streams of all the input ports.

Total effective input rate
: The combined effective bitrates (total, minus null packets) of all the transport streams of all the input ports.

Total cache used
: Number of bytes stored in PSI/SI/PSIP database for all input ports. The sections are stored in the database in binary format.

The Reset Stats button at the bottom of the page gives access to a dialog box that allows reset of channel statistics. Figure 9.47 shows the dialog box. Select the statistics items you want to reset and then press Apply.



Reset statistics

☑ Input Alarm counters
☑ Input PID details
☑ Input Table statistics
☑ Input IP statistics

Figure 9.47 Reset statistics dialog box

9.5.1.1 IP Inputs

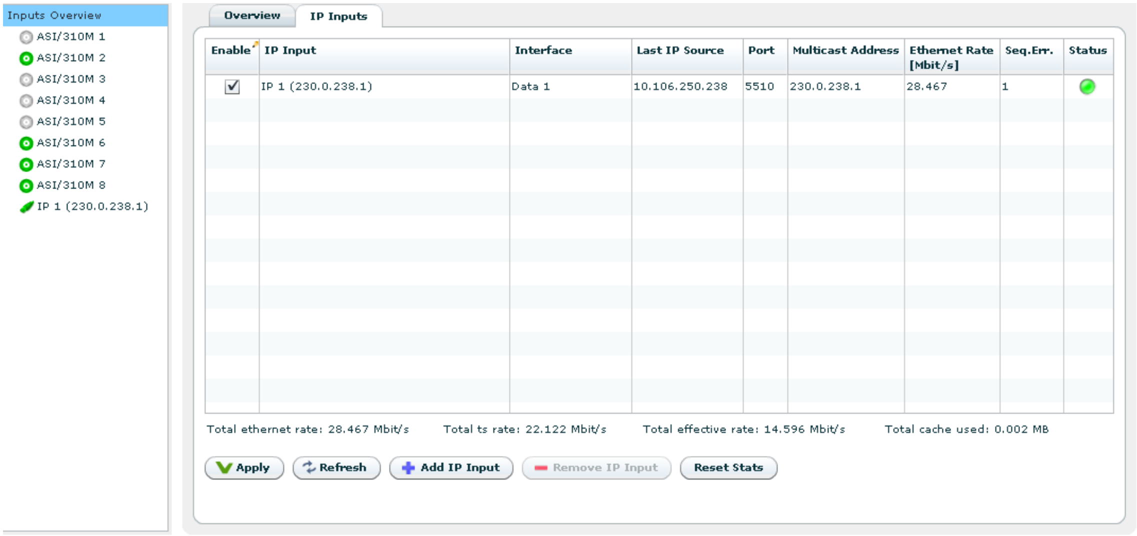
If the unit has the "Ethernet data interface" feature enabled the IP Inputs tab is shown on the Inputs Overview page.

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 with the physical port number and the user defined name. If no user defined label is defined for multicast streams, the multicast address is displayed.

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



Enable	IP Input	Interface	Last IP Source	Port	Multicast Address	Ethernet Rate [Mbit/s]	Seq.Err.	Status
☑	IP 1 (230.0.238.1)	Data 1	10.106.250.238	5510	230.0.238.1	28.467	1	●

Total ethernet rate: 28.467 Mbit/s   Total ts rate: 22.122 Mbit/s   Total effective rate: 14.596 Mbit/s   Total cache used: 0.002 MB

Figure 9.48 Inputs Overview - IP Inputs

Last IP Source
: The IP address that this IP input last received data from. If the input has never received any data the IP address is shown as 0.0.0.0.

Port
: The UDP port this IP input is configured to receive data on.

Multicast Address
: If the IP input is configured to receive data through a multicast the multicast address is shown here.

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

Seq.Err.
: The number of RTP sequence errors reported by the input since the last reset of statistics. RTP sequence error measurements requires the RTP protocol is present in the received stream.

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

Below the table four values are shown. The first one is the total Ethernet bitrate received. The last three are identical to the three values for ASI inputs described in the previous section.

The Add IP and Remove IP 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).

9.5.2 Input

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 dependant on what sort of input is selcted (ASI, IP,...) and what options are selected.

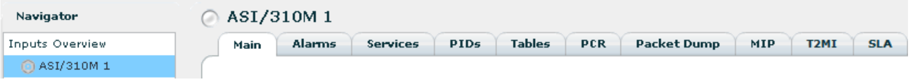


Figure 9.49 Input header

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.

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

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

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

: This page let the user define and manage service templates.

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.

MIP Details
: This page lets you see whether the transport stream contains MIP packets and if so gives detailed information about those packets.

T2MI Analysis

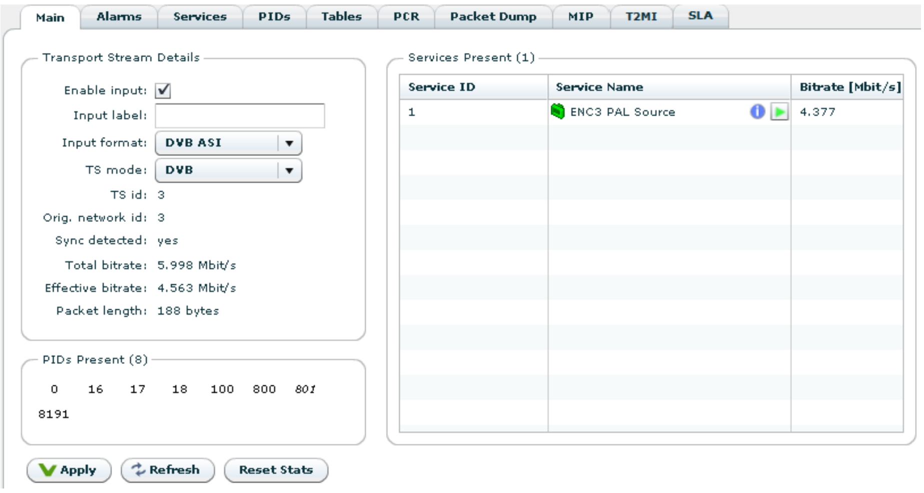
This page lets you see whether the transport stream contains T2-MI packets and if so gives detailed information about those packets.

SLA Monitor

This page provides information of the Service Level Agreement of the input and gives detailed information about alarm severity changes and duration.

In all sub-pages for a selected input 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 9.3.1**.

9.5.2.1 Main



Transport Stream Details

Enable input: ☑
Input label:
Input format: DVB ASI
TS mode: DVB
TS id: 3
Orig. network id: 3
Sync detected: yes
Total bitrate: 5.998 Mbit/s
Effective bitrate: 4.563 Mbit/s
Packet length: 188 bytes

PIDs Present (8)

0 16 17 18 100 800 801
8191

Services Present (1)

Service ID	Service Name	Bitrate [Mbit/s]
1	ENC3 PAL Source	4.377

Figure 9.50 Main

The Main page is divided into three sections for ASI/SMPT310 inputs (figure **Figure 9.50**) and five sections for IP inputs. For IP inputs the two extra sections are the IP RX configuration section (top left) and the IP RX status section (top right), see figure **Figure 9.51**.

In the IP RX configuration section the Enable and Input label fields are identical to those described for the ASI inputs below. The rest of the IP configuration and status parameters are described in **Section 9.5.2.3**.

At the bottom of the page the Reset Stats button is located. Clicking this will set all statistics counters relating to the selected input to zero.

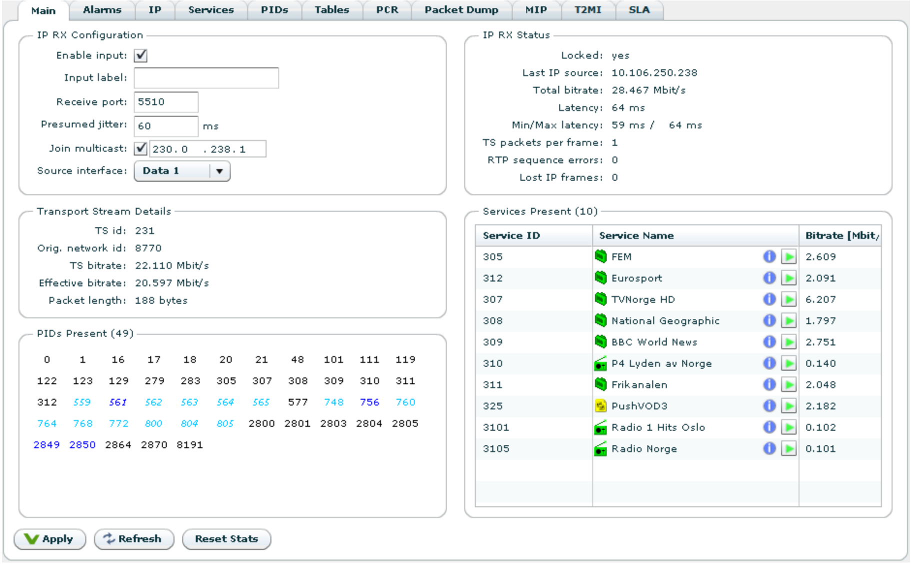
The Transport Stream Details field contains information and some configuration settings for the incoming transport stream:

Enable input

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

Input 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.



IP RX Configuration

Enable input: ☑
Input label:
Receive port: 5510
Presumed jitter: 60 ms
Join multicast: ☑ 230.0 .238.1
Source interface: Data 1 ▼

IP RX Status

Locked: yes
Last IP source: 10.106.250.238
Total bitrate: 28.467 Mbit/s
Latency: 64 ms
Min/Max latency: 59 ms / 64 ms
TS packets per frame: 1
RTP sequence errors: 0
Lost IP frames: 0

Transport Stream Details

TS id: 231
Orig. network id: 8770
TS bitrate: 22.110 Mbit/s
Effective bitrate: 20.597 Mbit/s
Packet length: 188 bytes

PIDs Present (49)

0	1	16	17	18	20	21	48	101	111	119
122	123	129	279	283	305	307	308	309	310	311
312	559	561	562	563	564	565	577	748	756	760
764	768	772	800	804	805	2800	2801	2803	2804	2805
2849	2850	2864	2870	8191						

Services Present (10)

Service ID	Service Name	Bitrate [Mbit/
305	FEM	2.609
312	Eurosport	2.091
307	TVNorge HD	6.207
308	National Geographic	1.797
309	BBC World News	2.751
310	P4 Lyden av Norge	0.140
311	Frikanalen	2.048
325	PushVOD3	2.182
3101	Radio 1 Hits Oslo	0.102
3105	Radio Norge	0.101

Figure 9.51 IP Input Sections

Input format
: The format of the input signal, either DVB ASI or SMPTE 310M (only available in ATSC+DVB configuration mode).

TS mode
: Transport stream mode, either DVB or ATSC (only available in ATSC+DVB configuration mode).

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.

Orig. 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.

Sync detected
: Shows whether the input transport stream has been synchronised.

Bitrate limit
: The maximum bitrate to accept on this input. If the ASI input stream exceeds this bitrate, data will be discarded from this port and an input overflow alarm will be raised.

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

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

Maximum burst rate

The maximum burst bitrate measured by the bitrate limiter. This value is based on 188 byte TS packet length.

Packet length

The length of the transport stream packets in bytes.

Beneath the Transport Stream Details section is the PIDs present section. This 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 coloured 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>.

For ATSC services, the service name displayed is a concatenation of the short channel name, and the major/minor channel number.

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.

To the very right in the Service Name column is an icon displaying the service streaming status. A green arrow indicates that no streaming session is currently running and may be started by clicking on the icon. Starting a streaming session redirects the current service to the management console, which will play the program if suitable player software has been installed.

If the icon shows a green arrow over a red square this indicates that streaming is already in progress from a different input.

See also **Section 9.4.5**

Service Bitrate

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.

9.5.2.2 Alarms

The Alarms page lets the user configure and view the status of all alarms belonging to the selected input. The page has two tabs at the top giving access to the Alarm Config and Alarm Log sub pages.

In figure 9.52 the Alarm Config page is shown. Note that the alarms are organised hierarchically and that only the branches in focus need to be expanded.

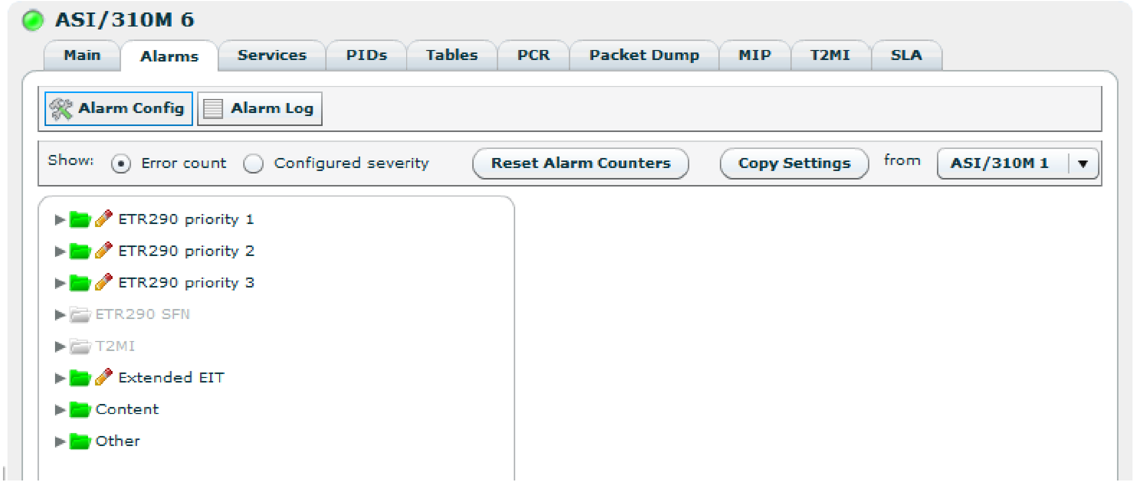


Figure 9.52 Input alarm configuration

The following configuration options are available:

Show

The radio buttons Error count and Configured severity allows the user to configure what to be shown in the input alarm tree (see figure 9.53).

Error count

Display the accumulated number of errors since last alarm counter reset.

Configured severity

Display the configured alarm severity.

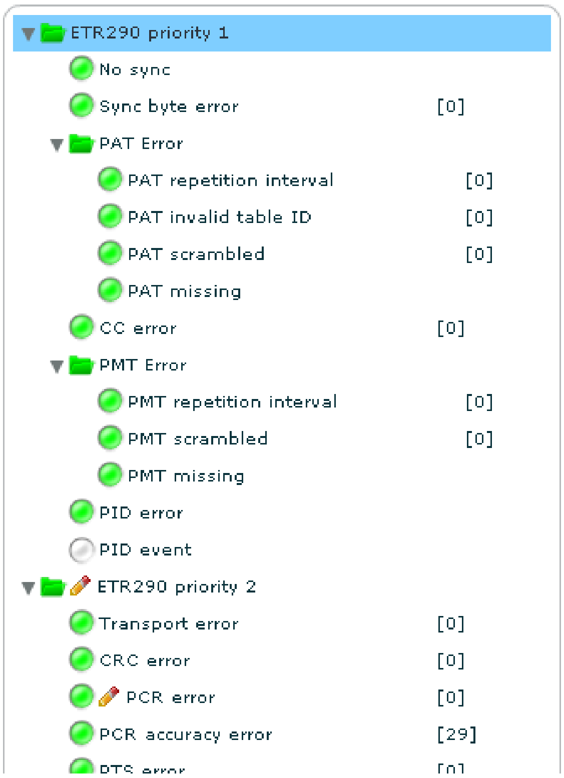
Reset Alarm Counters

Reset the alarm counters for all alarms belonging to the selected input.

Copy Settings *from* Input

This is a convenient way to copy alarm settings for a specific input to the current input. Use the Input drop-down list to choose from which input to copy the settings. The settings are copied by hitting the Copy Settings button. This includes all severity and limit overrides both on alarm level and on PID level.

The input alarm tree is found in the main part of the page. It consists of a tree displaying all alarms.



```
▼ ETR290 priority 1
    ● No sync
    ● Sync byte error                 [0]
  ▼ PAT Error
      ● PAT repetition interval         [0]
      ● PAT invalid table ID            [0]
      ● PAT scrambled                   [0]
      ● PAT missing
    ● CC error                        [0]
  ▼ PMT Error
      ● PMT repetition interval         [0]
      ● PMT scrambled                   [0]
      ● PMT missing
    ● PID error
    ○ PID event
▼ ETR290 priority 2
    ● Transport error                 [0]
    ● CRC error                       [0]
    ● PCR error                       [0]
    ● PCR accuracy error              [29]
    ● PTS error                       [0]
```

Figure 9.53 Input alarm tree

A section of the expanded input alarm tree is shown in figure 9.53. By clicking on the alarm nodes in the tree the details for the selected alarm is shown in the Alarm details section (figure 9.54).

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

The alarm counters for a specific group are reset by left-clicking an alarm group in the alarm tree and choosing the Reset Counters option. The counters for the individual alarms are reset using the same procedure for an alarm node.

Alarm node

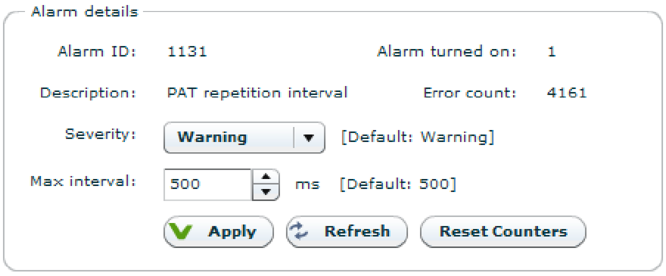
These have a coloured indicator showing the alarms current status. In addition, the alarms configured severity or the current error count is shown in brackets to the right.

The right hand side of the page shows details about a single selected alarm (see figure 9.54). The frame appears when a particular alarm is clicked. Its content may vary according to the alarm selected.

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 C.3.



Alarm details

Alarm ID:	1131	Alarm turned on:	1
Description:	PAT repetition interval	Error count:	4161
Severity:	Warning	[Default: Warning]	
Max interval:	500 ms	[Default: 500]	

Figure 9.54 Alarm details

Alarm

Name of the alarm.

Description

A short description of the alarm.

Severity

Overrides the default severity for the given alarm. The default severity is in brackets to the right of the drop down list. The factory default value for the severity is Use global default. The globally configured alarm severity is then always used.

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.

Max interval (alarm dependent label)

This field is shown for table repetition alarms. The number entered in the box determines the maximum time (milliseconds) allowed between two occurrences of the same table. The default value is shown to the right.

Max rate (alarm dependent label)

This field is shown for PID rate alarms. The number entered in the box determines the maximum rate allowed for a given PID above which an alarm is raised. The default value is shown to the right.

Min rate (alarm dependent label)

This field is shown for PID rate alarms. The number entered in the box determines the minimum rate allowed for a given PID below which an alarm is raised. The default value is shown to the right.

Alarm turned on
: Number of times the alarm has triggered. If the alarm is filtered this counter will not increase.

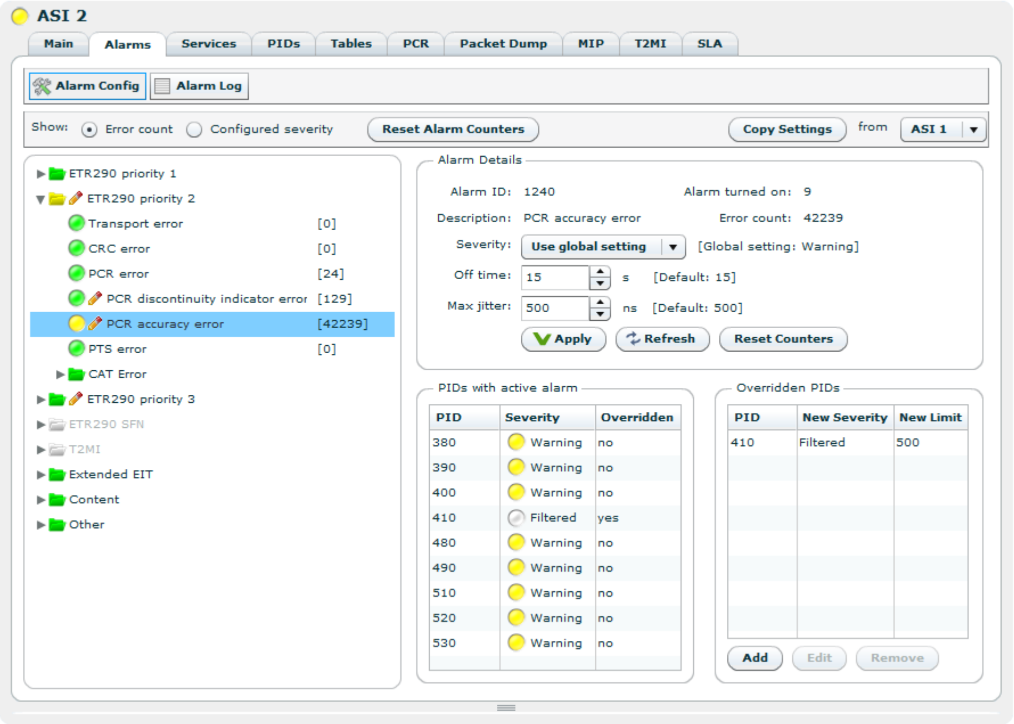
Error count
: For alarms that are checked continuously, this counter shows the number of times an alarm condition has been violated. This counter will increase even if the alarm is filtered.

Global setting
: This field shows the value configured for this alarm in the global settings. If the alarm severity level is set to *global default* in the “Severity” pull-down list, this is the value that will be used.

In addition, if the alarm contains a limit, e.g. max interval, a numeric input at the bottom is displayed. This lets the user override the default limit, which is shown in brackets to the right.

Reset counters
: This button lets the user reset the "Alarm turned on" and "Error count" counters for this alarm.

"PID" and "Service"alarms (**Figure 9.55**) allow overriding of sub items. For such alarms two tables are shown below the alarm details.



Show: ● Error count ○ Configured severity

- ETR290 priority 1
- ETR290 priority 2
  - Transport error [0]
  - CRC error [0]
  - PCR error [24]
  - PCR discontinuity indicator error [129]
  - PCR accuracy error [42239]
  - PTS error [0]
  - CAT Error
- ETR290 priority 3
- ETR290 SFN
- T2MI
- Extended EIT
- Content
- Other

Alarm Details

Alarm ID: 1240 Alarm turned on: 9
Description: PCR accuracy error Error count: 42239
Severity: Use global setting [Global setting: Warning]
Off time: 15 s [Default: 15]
Max jitter: 500 ns [Default: 500]

PIDs with active alarm

PID	Severity	Overridden
380	Warning	no
390	Warning	no
400	Warning	no
410	Filtered	yes
480	Warning	no
490	Warning	no
510	Warning	no
520	Warning	no
530	Warning	no

Overridden PIDs

PID	New Severity	New Limit
410	Filtered	500

Figure 9.55 Alarm severity per sub-ID (typically Service or PID)

The Service/PID with active alarms table shows all currently active alarms on sub-items for the selected alarm. The following columns are found in the table.

Service/PID
: The id of the sub-item.

Severity
: The current severity of the item.

Overridden
: Indicates whether the sub item has been overridden.

If no override already exists an override can be added by right-clicking an item. An item already overridden can be edited or removed.

The Overridden PIDs/Services section shows currently overridden sub items. The following columns are found in the table:

Service/PID
: The id of the Sub item.

New severity
: The new severity, i.e. the severity after the sub item has been overridden.

New limit
: If the alarm has a configurable limit, also the limit of the sub item can be overridden and that new limit will also be shown.

  An override can be edited or removed by right-clicking on the entry in the list. Alternatively this can be done by hitting the Edit and Remove button, respectively. An override can also be added hitting the Add button and manually entering the ID and overridden values.

9.5.2.3 IP

This tab is only visible if an IP input is selected.

The tab contains the sub pages Main, Ping and Regulator. If the IP Forward Error Correction feature is available the FEC sub page selection is also visible. In addition, an IP statistics sub page is available.

The Main sub page is shown in figure 9.56.

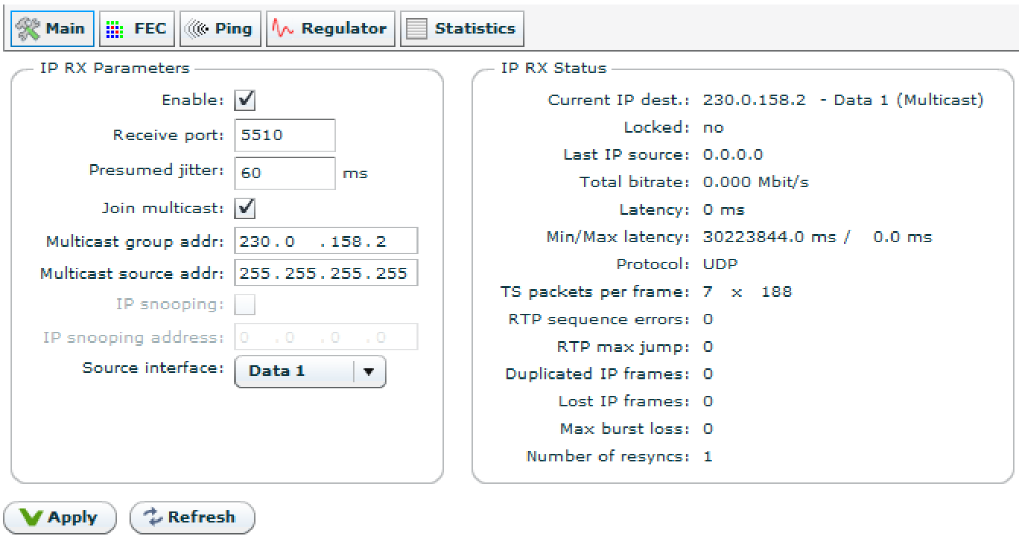
This page allows configuration of the IP parameters for the IP input and shows detailed IP status information for the input.

The IP RX Parameters field:

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

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

Presumed jitter
: The maximum amount of jitter you expect on the ip link. This value controls the amount of buffering that will be applied.



IP RX Parameters

Enable: ☑
Receive port: 5510
Presumed jitter: 60 ms
Join multicast: ☑
Multicast group addr: 230 . 0 . 158 . 2
Multicast source addr: 255 . 255 . 255 . 255
IP snooping: □
IP snooping address: 0 . 0 . 0 . 0
Source interface: Data 1

IP RX Status

Current IP dest.: 230.0.158.2 - Data 1 (Multicast)
Locked: no
Last IP source: 0.0.0.0
Total bitrate: 0.000 Mbit/s
Latency: 0 ms
Min/Max latency: 30223844.0 ms / 0.0 ms
Protocol: UDP
TS packets per frame: 7 x 188
RTP sequence errors: 0
RTP max jump: 0
Duplicated IP frames: 0
Lost IP frames: 0
Max burst loss: 0
Number of resyncs: 1

Figure 9.56 IP Configuration

Join multicast
: If this box is checked the input will join the multicast configured in the following IP field. If the box is not checked the input will listen for unicast traffic.

Multicast group addr
: This parameter is only used if the “Join multicast” box is checked. This is the multicast group the input will join.

Multicast source addr
: This parameter will only be used if the input is set to join a multicast and the unit is currently using IGMP v3. If this parameter is set to something different from 255.255.255.255 or 0.0.0.0, the input will only accept multicast traffic from the IP address specified in this parameter.

IP snooping
: This parameter enables snooping on IP streams not designated for this units. This feature require that the used Network Interface is set to Promiscuous mode.

IP snooping address
: This parameter 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 will not be used.

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

The IP RX Status field:

Locked
: “Yes”, when the unit has locked to the input stream and has correctly estimated the bitrate of the input stream. “No”, when the unit has not been able to receive the input stream correctly.

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.

Total rate
: The total IP rate received on this input.

Latency
: This parameter reflects the network jitter the unit can handle at the moment.

Min/Max latency
: This shows the minimum and maximum latency measured since the statistics was last reset.

Protocol
: Indicates RTP if the received data contains an RTP header, UDP otherwise.

TS packets per frame
: The number of transport stream packets per IP frame and the size of the transport stream packets in the incoming stream.

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.

Duplicated IP frames
: The number of received IP frames with RTP sequence numbers which have already been received.

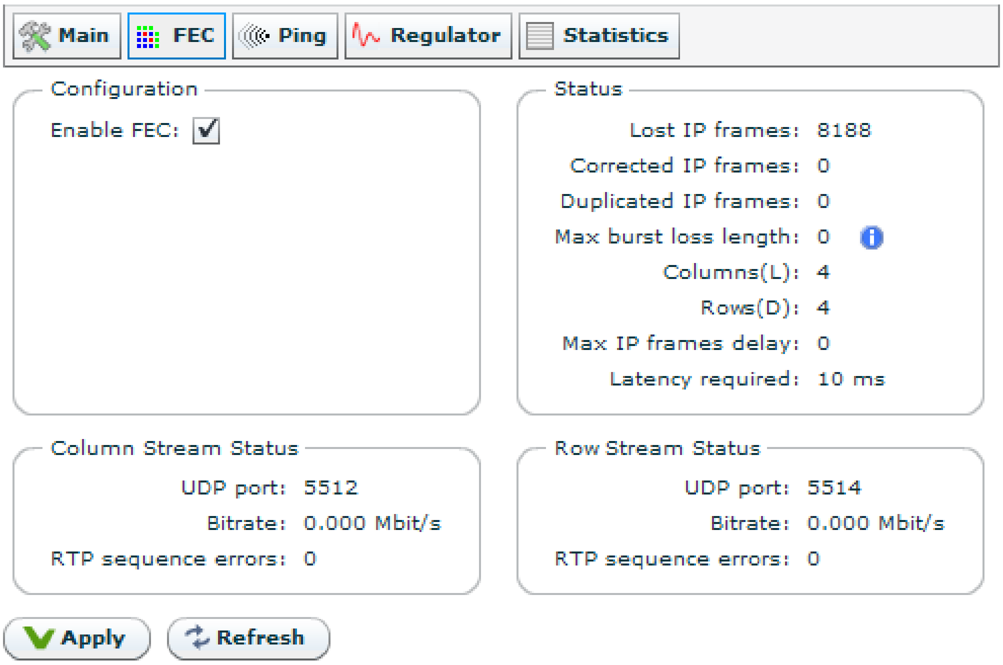
Lost IP frames
: A counter showing the number of IP frames that have been lost, i.e. lost and not corrected by the unit.

Corrected IP frames
: A counter showing the number of IP frames corrected by the FEC engine.

Max burst loss
: The maximum number of consecutive packets lost.

Number of resyncs
: The number of times the buffer has been re-synchronised. Re-synchronisation causes a disruption in the picture. The most typical reason for a re-sync is when no data is received and the buffer runs empty. The reason for re-syncs is tagged in the alarm details for the No Lock alarm.

The FEC sub page is shown in **Figure 9.57**. This page displays the status of the forward error correction processing of the IP input.



Configuration

Enable FEC: ☑

Status

Lost IP frames: 8188
Corrected IP frames: 0
Duplicated IP frames: 0
Max burst loss length: 0
Columns(L): 4
Rows(D): 4
Max IP frames delay: 0
Latency required: 10 ms

Column Stream Status

UDP port: 5512
Bitrate: 0.000 Mbit/s
RTP sequence errors: 0

Row Stream Status

UDP port: 5514
Bitrate: 0.000 Mbit/s
RTP sequence errors: 0

Figure 9.57 Input FEC configuration

The Configuration field provides a single check box to enable or disable input FEC processing. If this box is not checked all other fields in this page is greyed out, i.e. not applicable.

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

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

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

Duplicated IP 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 Length
: The maximum number of consecutive IP frames that have been lost.

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.

Max IP frames delay

The maximum delay of out-of-order IP frames (datagrams).

Latency required

The latency required by the input FEC processor to handle the incoming FEC matrix.

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.

Bitrate

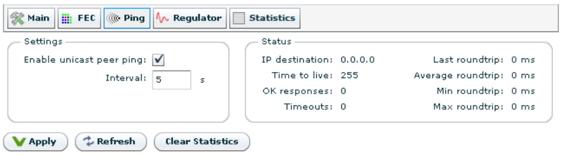
The bitrates of the Column and row FEC data.

RTP sequence errors

Shows the number of disruption in the sequence count of the RTP protocol.

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

The Ping sub page is shown in figure **9.58**.



Settings

Enable unicast peer ping: ☑

Interval: 5 s

Status

IP destination: 0.0.0.0

Time to live: 255

OK responses: 0

Timeouts: 0

Last roundtrip: 0 ms

Average roundtrip: 0 ms

Min roundtrip: 0 ms

Max roundtrip: 0 ms

Figure 9.58 Ping page

Timeouts in MAC address lookup tables can sometimes cause problems when routing one-way traffic. The Ping feature is designed to solve this by transmitting a ping message generating two-way traffic.

The Settings field:

Enable Unicast Peer Ping

Check this box to enable Unicast Peer Ping. This enables regular pinging of the transmitting device.

Interval

Set the interval in seconds between each Ping.

MTU

Sets the Ethernet frame size to use on ICMP messages transmitted.

The Status field displays the status of the on-going pinging session:

IP destination

The address of the device receiving the Ping requests.

Time to live

This figure indicates the number of routing points the Ping message may encounter before it is discarded.

OK responses

Indicates how many valid Ping responses have been received.

Timeouts

Indicates how many of the sent Ping messages timed out, i.e. did not provide a valid response within the allowed time.

Last roundtrip

The time taken from last sending the Ping message until the response is received.

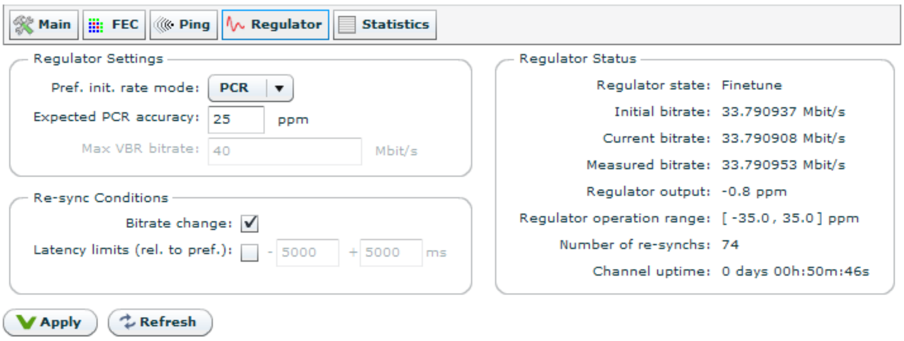
Min roundtrip

The minimum time taken from sending a Ping message until the response is received.

Max roundtrip

The maximum time taken from sending a Ping message until the response is received.

The Regulator sub page is shown if figure 9.59.



Regulator Settings

Pref. init. rate mode: PCR ▾

Expected PCR accuracy: 25 ppm

Max VBR bitrate: 40 Mbit/s

Re-sync Conditions

Bitrate change: ☑

Latency limits (rel. to pref.): ☐ - 5000 + 5000 ms

Regulator Status

Regulator state: Finetune

Initial bitrate: 33.790937 Mbit/s

Current bitrate: 33.790908 Mbit/s

Measured bitrate: 33.790953 Mbit/s

Regulator output: -0.8 ppm

Regulator operation range: [-35.0 , 35.0] ppm

Number of re-synchs: 74

Channel uptime: 0 days 00h:50m:46s

Figure 9.59 Regulator page

In the Regulator Settings field it is possible to adjust the settings of an IP input buffer regulator.

Pref. Init. Rate Mode

From the pull-down list select the preferred algorithm to find the initial bitrate of a received data stream.

PCR

The default mode is PCR, 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.

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.

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.

FAST COARSE
In this mode the units attamps 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.

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.“

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 field:

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 field allows inspecting the status of the buffer regulator.

Regulator state
This parameter shows the current state of the buffer regulator. The 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.

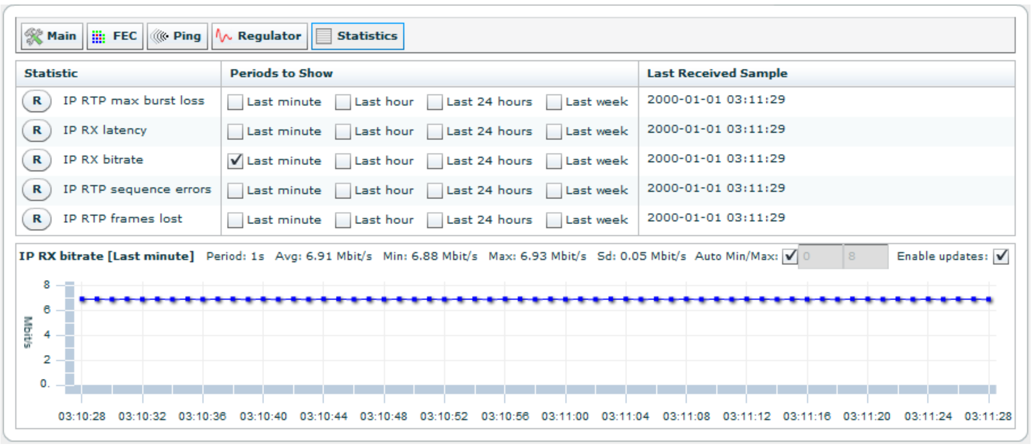
Regulator output
: Indicates the amount of correction the regulator must apply to the output bitrate, with respect to the initially measured input bit rate, in order to avoid buffer under-/overflow.

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 9.5.2.1**).

The Statistics sub page is shown in figure 9.60 if the option Log IP statistics is checked on the channels main page.



Statistic	Periods to Show				Last Received Sample
R IP RTP max burst loss	□ Last minute	□ Last hour	□ Last 24 hours	□ Last week	2000-01-01 03:11:29
R IP RX latency	□ Last minute	□ Last hour	□ Last 24 hours	□ Last week	2000-01-01 03:11:29
R IP RX bitrate	☑ Last minute	□ Last hour	□ Last 24 hours	□ Last week	2000-01-01 03:11:29
R IP RTP sequence errors	□ Last minute	□ Last hour	□ Last 24 hours	□ Last week	2000-01-01 03:11:29
R IP RTP frames lost	□ Last minute	□ Last hour	□ Last 24 hours	□ Last week	2000-01-01 03:11:29

IP RX bitrate [Last minute] Period: 1s Avg: 6.91 Mbit/s Min: 6.88 Mbit/s Max: 6.93 Mbit/s Sd: 0.05 Mbit/s Auto Min/Max: ☑ 0 8 Enable updates: ☑

Figure 9.60 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. 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.

9.5.2.4 Services

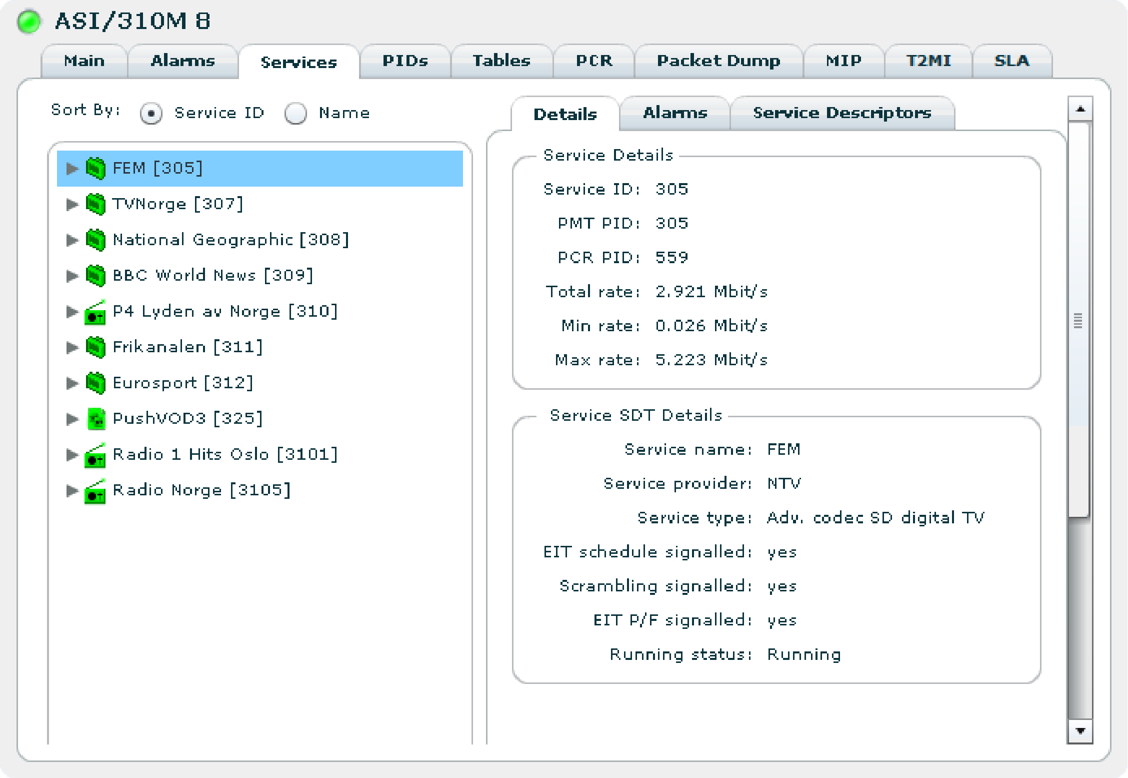
The Services page displays information relative to each service present in the stream.

Alarms tab

The Current alarms section present at the bottom of the page contains a table showing all alarms currently active on the selected service. The columns in the table (Severity, Description, Alarm ID and Details) have the same meaning as described in Section 9.3.2.

9.5.2.4.1 Service List

The Service List tab displays a list of services running in the selected input. Each service type is represented by a symbol coloured to show the current alarm status of the service (figure 9.61).



Sort By: ● Service ID ○ Name

- ▶ FEM [305]
- ▶ TVNorge [307]
- ▶ National Geographic [308]
- ▶ BBC World News [309]
- ▶ P4 Lyden av Norge [310]
- ▶ Frikanalen [311]
- ▶ Eurosport [312]
- ▶ PushVOD3 [325]
- ▶ Radio 1 Hits Oslo [3101]
- ▶ Radio Norge [3105]

Service Details

Service ID: 305
PMT PID: 305
PCR PID: 559
Total rate: 2.921 Mbit/s
Min rate: 0.026 Mbit/s
Max rate: 5.223 Mbit/s

Service SDT Details

Service name: FEM
Service provider: NTV
Service type: Adv. codec SD digital TV
EIT schedule signalled: yes
Scrambling signalled: yes
EIT P/F signalled: yes
Running status: Running

Figure 9.61 Service details overview when service list is not expanded.

Sort by

Selecting the SID 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.

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:

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

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

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

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

In ATSC mode the second section is named Channel Details and shows the following parameters from the VCT table if it is present and analysed:

- Channel name
- Major channel number
- Minor channel number
- Service type
- Modulation mode
- Channel TSID
- Access controlled
- Hidden
- Hide guide

Alarms tab

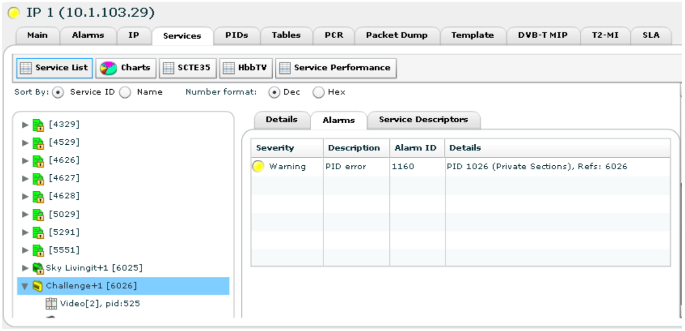
The Alarms shown in figure 9.62 tab lists all the current alarms related to the selected service. The following information is provided:

Severity
: The severity of the alarm.

Description
: Bref description of the alarm.

Alarm ID
: The alarm identifier.

Details
: Some additional details.



Sort By: ● Service ID ○ Name   Number format: ● Dec ○ Hex

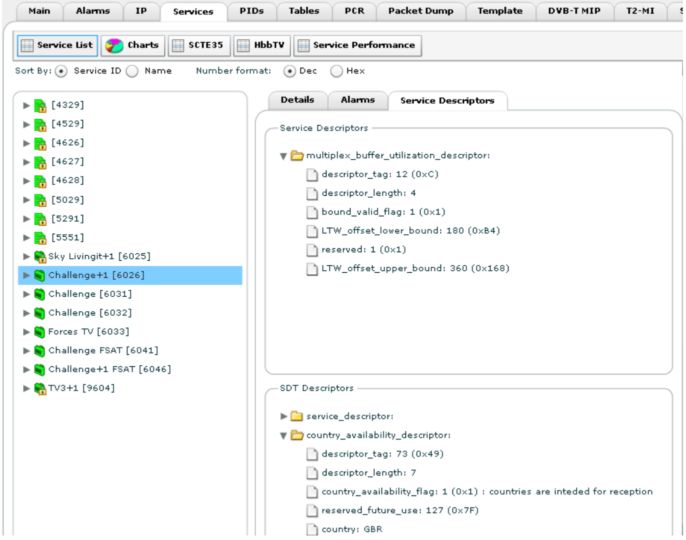
- [4329]
- [4529]
- [4626]
- [4627]
- [4628]
- [5029]
- [5291]
- [5551]
- Sky Livingit+1 [6025]
- Challenge+1 [6026]
  - Video[2], pid:525

Severity	Description	Alarm ID	Details
● Warning	PID error	1160	PID 1026 (Private Sections), Refs: 6026

Figure 9.62 Service alarms overview

Descriptors tab

The Descriptors shown in figure 9.63 tab displays the list of the PMT and SDT descriptors of the service.



Sort By: ● Service ID ○ Name   Number format: ● Dec ○ Hex

```
▶ [4329]
▶ [4529]
▶ [4626]
▶ [4627]
▶ [4628]
▶ [5029]
▶ [5291]
▶ [5551]
▶ Sky Livingit+1 [6025]
▶ Challenge+1 [6026]
▶ Challenge [6031]
▶ Challenge [6032]
▶ Forces TV [6033]
▶ Challenge FSAT [6041]
▶ Challenge+1 FSAT [6046]
▶ TV3+1 [9604]
```

Service Descriptors

```
▼ multiplex_buffer_utilization_descriptor:
    descriptor_tag: 12 (0xC)
    descriptor_length: 4
    bound_valid_flag: 1 (0x1)
    LTW_offset_lower_bound: 180 (0xB4)
    reserved: 1 (0x1)
    LTW_offset_upper_bound: 360 (0x168)
```

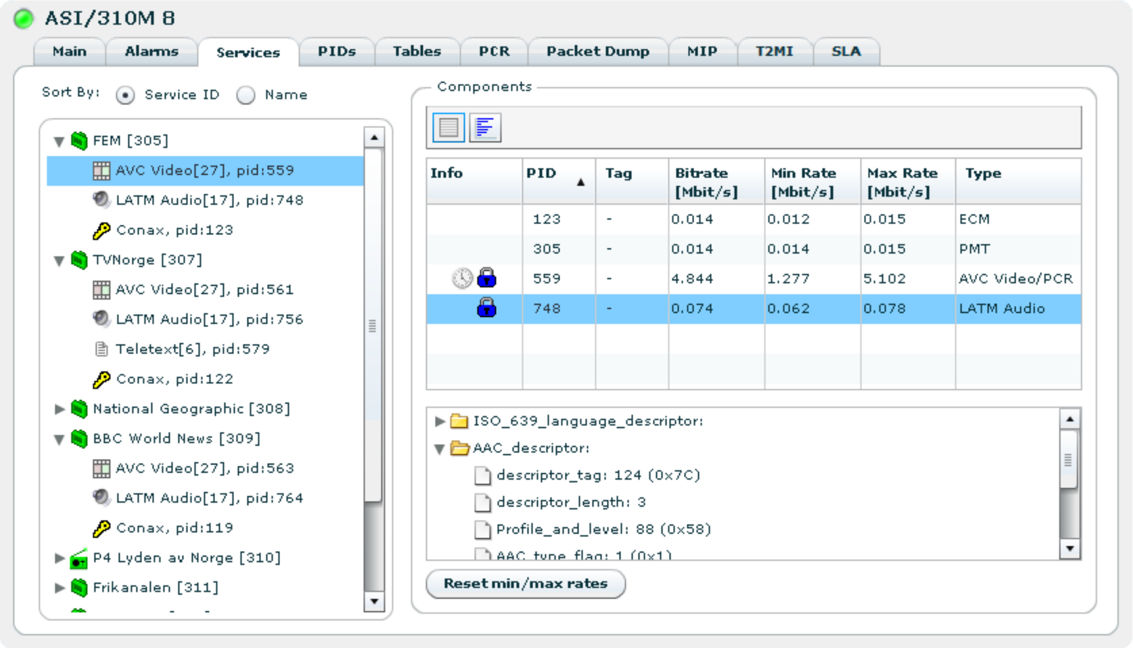
SDT Descriptors

```
▶ service_descriptor:
▼ country_availability_descriptor:
    descriptor_tag: 73 (0x49)
    descriptor_length: 7
    country_availability_flag: 1 (0x1) : countries are inteded for reception
    reserved_future_use: 127 (0x7F)
    country: GBR
```

Figure 9.63 Service descriptors overview

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 9.64.



Sort By: ● Service ID ○ Name

```
▼ FEM [305]
    AVC Video[27], pid:559
    LATM Audio[17], pid:748
    Conax, pid:123
▼ TVNorge [307]
    AVC Video[27], pid:561
    LATM Audio[17], pid:756
    Teletext[6], pid:579
    Conax, pid:122
▶ National Geographic [308]
▼ BBC World News [309]
    AVC Video[27], pid:563
    LATM Audio[17], pid:764
    Conax, pid:119
▶ P4 Lyden av Norge [310]
▶ Frikanalen [311]
```

Components

Info	PID ▲	Tag	Bitrate [Mbit/s]	Min Rate [Mbit/s]	Max Rate [Mbit/s]	Type
	123	-	0.014	0.012	0.015	ECM
	305	-	0.014	0.014	0.015	PMT
🕓 🔒	559	-	4.844	1.277	5.102	AVC Video/PCR
🔒	748	-	0.074	0.062	0.078	LATM Audio

```
▶ ISO_639_language_descriptor:
▼ AAC_descriptor:
    descriptor_tag: 124 (0x7C)
    descriptor_length: 3
    Profile_and_level: 88 (0x58)
    AAC_type_flag: 1 (0x1)
```

Figure 9.64 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.

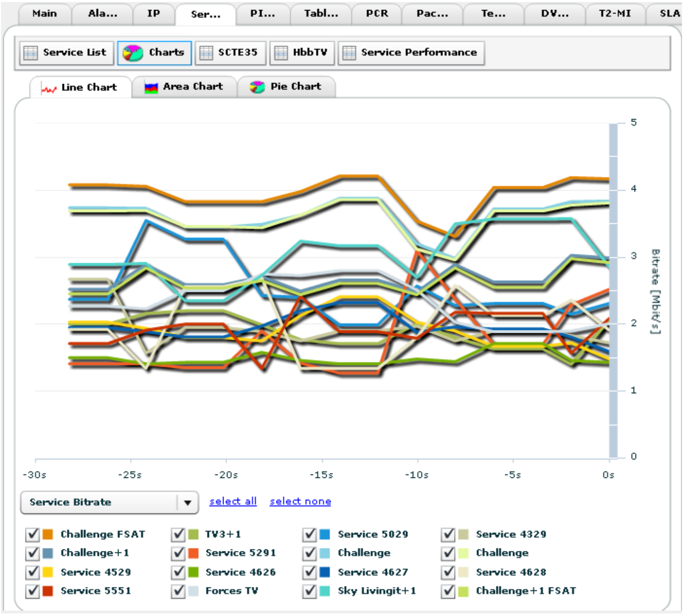
Clicking on a component in the left hand list of services and components opens a Components view on the right hand side. On the top of this view is a toolbar with two buttons to switch between Table and Rate views.

These views contain almost exactly the same information as the corresponding view on the PIDs page, Section 9.5.2.5. The only difference is that in grid view a list of descriptors may be displayed below the Components table when clicking on a component. A tree structure of descriptors is displayed, if present, in the selected component.

9.5.2.4.2 Charts

The Chart sub-page presents a graphical representation of the bit-rate of each services inside a stream.

The line chart shown figure 9.65 displays the bit-rate of each service over time. It is possible to select which services to display and which component (service, video, audio, or video and audio).



Service Bitrate ▾

☑ Challenge FSAT	☑ TV3+1	☑ Service 5029	☑ Service 4329
☑ Challenge+1	☑ Service 5291	☑ Challenge	☑ Challenge
☑ Service 4529	☑ Service 4626	☑ Service 4627	☑ Service 4628
☑ Service 5551	☑ Forces TV	☑ Sky Livingit+1	☑ Challenge+1 FSAT

Figure 9.65 Line chart

The area chart shown figure 9.66 displays the contribution of each service in the total bit-rate of the stream over time. It is possible to select which services to display and which component (service, video, audio, or video and audio).

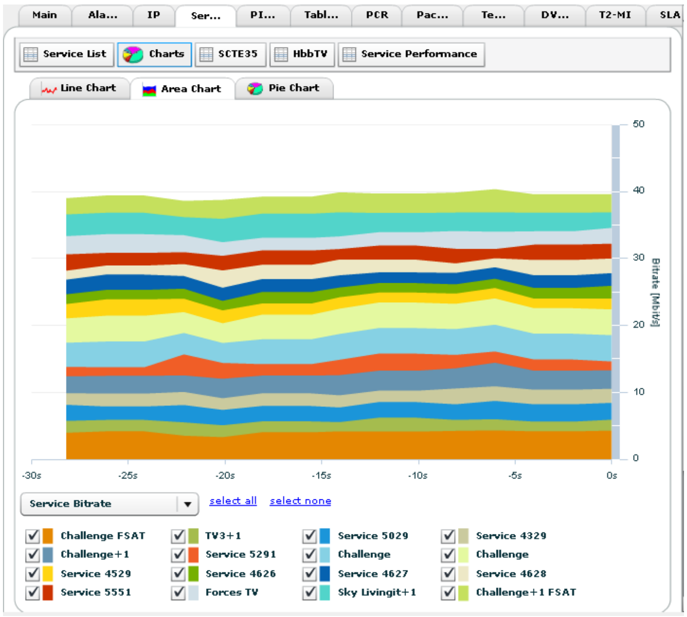


Figure 9.66 Area chart

The pie chart shown figure 9.67 displays the current contribution of each service in the total bit-rate of the stream. By selecting one service on the chart, a second pie chart presents the current contribution of each component in the toltal bit-rate of the service.

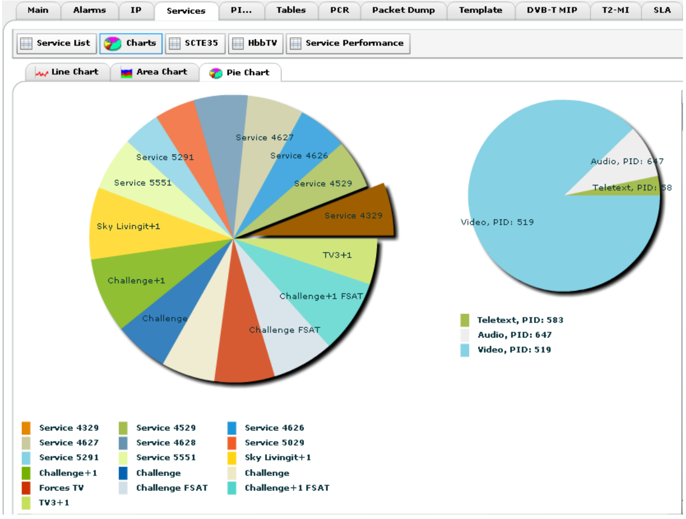
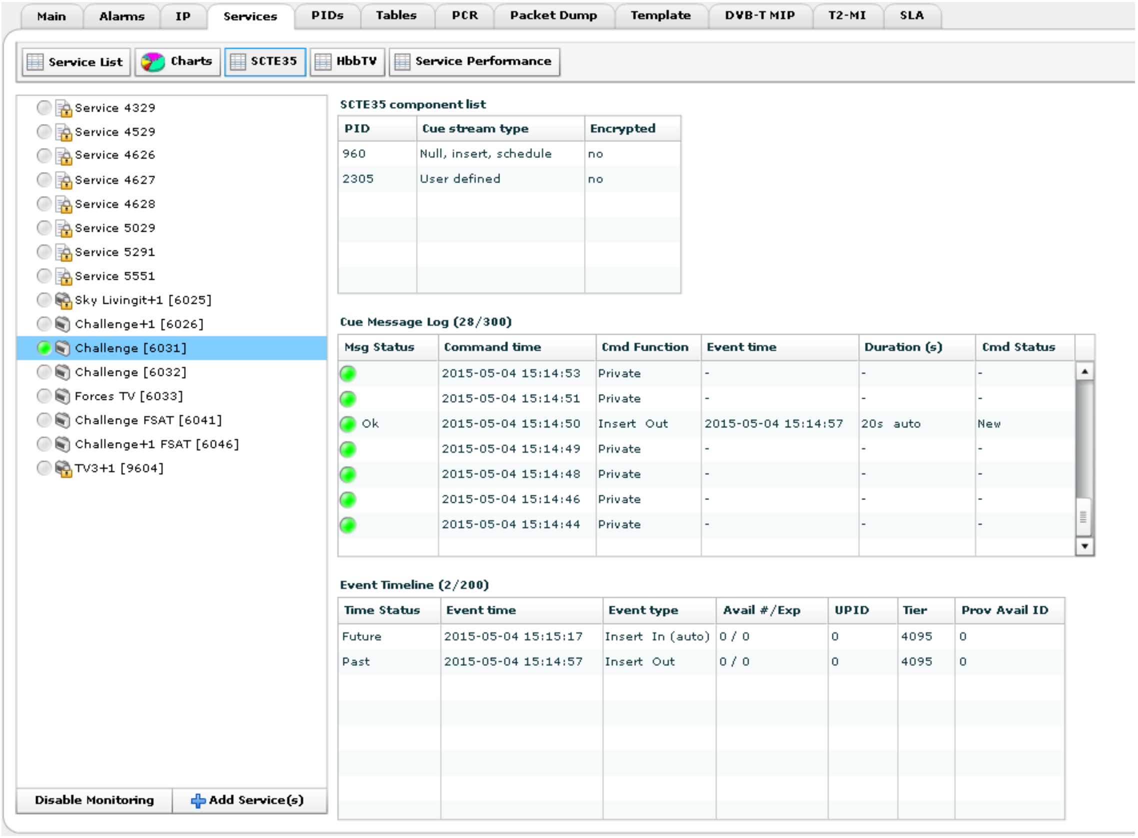


Figure 9.67 Pie chart

9.5.2.4.3 SCTE35

The SCTE35 sub-page shown Figure 9.68 displays information relative to the SCTE35 cue messages part of the selected service.



Service 4329
Service 4529
Service 4626
Service 4627
Service 4628
Service 5029
Service 5291
Service 5551
Sky Livingit+1 [6025]
Challenge+1 [6026]
Challenge [6031]
Challenge [6032]
Forces TV [6033]
Challenge FSAT [6041]
Challenge+1 FSAT [6046]
TV3+1 [9604]

SCTE35 component list

PID	Cue stream type	Encrypted
960	Null, insert, schedule	no
2305	User defined	no

Cue Message Log (28/300)

Msg Status	Command time	Cmd Function	Event time	Duration (s)	Cmd Status
●	2015-05-04 15:14:53	Private	-	-	-
●	2015-05-04 15:14:51	Private	-	-	-
● Ok	2015-05-04 15:14:50	Insert Out	2015-05-04 15:14:57	20s auto	New
●	2015-05-04 15:14:49	Private	-	-	-
●	2015-05-04 15:14:48	Private	-	-	-
●	2015-05-04 15:14:46	Private	-	-	-
●	2015-05-04 15:14:44	Private	-	-	-

Event Timeline (2/200)

Time Status	Event time	Event type	Avail #/Exp	UPID	Tier	Prov Avail ID
Future	2015-05-04 15:15:17	Insert In (auto)	0 / 0	0	4095	0
Past	2015-05-04 15:14:57	Insert Out	0 / 0	0	4095	0

Figure 9.68 SCTE35 analysis details

To start/stop analyzing a service depress the Enable SCTE35/Disable SCTE35 button, or Add Service(s) if the service is not currently present in the service list.

The SCTE35 sub-page contains three tables.

SCTE35 component list table

The first table, called SCTE35 component list, lists the components of the selected service that are registered in the PMT as SCTE35 components. For each component listed, the following information are provided:

PID
: PID of the SCTE35 component registered in the PMT.

Cue stream type
: The SCTE35 stream type defined by the Cue Identifier Descriptor. When the descriptor is not present, the value Undefined is stated.

Encrypted
: Indicates whether the cue messages transmitted over this component are encrypted.

Cue Message Log

The second table, Cue Message Log, is a log of all the SCTE35 compliant messages found in the selected service (excluding *bandwith_reservation* and *splice_null* messages). For each message, the following information is displayed:

Msg Status

Information about the validity of the message. A green marker indicates that the command conveyed by the message abides by the constraints imposed by SCTE35, while a red marker indicates a violation. More information is displayed by a status specifier:

- No specifier: Encrypted message or private command (green marker).
- Ok: The command abides by the arm time constraint defined in the specification (green marker).
- Immediate: The command is an immediate command (green marker).
- Late: The command violates the arm time condition imposed by SCTE35 (red marker).
- Invalid: Invalid timing information or CRC error: no valid *splice_time* found in a command that requires one (red marker).

> **Note:** The value of the arm time is configurable in the corresponding alarm (TS/Scte35/Arm time violation).

> **Note:** Only *splice_insert* and *splice_schedule* commands have timing constraints. For the other commands, the marker is green without any specifier.

Command time

Local time at which the message has been recieved.

Cmd Function

Function of the command conveyed by the message. One of

- Insert In/Out: *splice_insert* command,
- Schedule In/Out: *splice_schedule* command,
- Private: *private_command* command,
- Encrypted: encrypted command: the actual function is unknown,
- CRC error: the CRC check failed

> **Note:** *splice_null* and *bandwith_reservation* commands are not logged.

Event time
: In the case of a *splice_insert* command, the local time at which the splicing point is inserted.

Duration
: If specified in the command, duration of the avail in seconds. If the *auto_return* flag is set, then the specifier (auto) follows the duration value.

Cmd Status
: Command status. One of

- New (command defining a new event),
- Redundant (redundant command),
- Update (command updating an existing event),
- Cancel (command cancelling an existing event).

The remaining of the parameters are available as tool-tips:

Splice Event ID
: Splice event ID of the splicing point being defined.

Avail #
: Avail number, and number of avails expected.

Tier
: Tier of the splicing point being defined.

Unique Program ID
: Unique program ID of the splicing point being defined.

Provider Avail ID
: Provider avail ID of the splicing point being defined.

PTS Time / UCTS Time
: PTS timestamp /offset if provided.

DTFM
: In parenthesis is displayed the DTFM preroll of the splicing point being defined followed by the DTFM sequence of the splicing point being defined (if any).

Event Timeline

The last table, Event Timeline, displays the list of splicing events that are to be, or have been, inserted by a splicing device. The splicing events present in the list are the events defined by a valid *splice_insert* command (*splice_schedule* commands are not supported).

Note: While Cue Message Log table is a log of the scte35 commands monitored on a selected service, Event Timeline table increases the abstraction level by providing an exact list of actions the splicing device is suppose to perform (or have performed).

Note: Each event listed in the Event Timeline table reflects the **last valid** command monitored (with the same *event_id*). Any command with a red marker is ignored and does not spawn any event in this table.

Event Timeline contains the following fields:

Time Status
: Time status of the event (field updated in real time). One of

- Future (the event, scheduled or inserted in the future, can be updated or cancelled),
- Imminent (the event is about to happen and cannot be updated or cancelled any more),
- Past (the event already happened).

Event time
: Local time at which the splice point is to be inserted.

Event type
: Type of the event. One of

- Insert In/Out (inserted In or Out-point),
- Schedule In/Out (scheduled, but not inserted, splice In or Out-point).

Note: Insert In can be followed by the specifier (auto) meaning that this In-point has been implied by a *splice_insert* command carrying a duration and a set *auto_return* flag.

Avail #/Exp
: Avail number, and number of avails expected.

UPID
: Provider avail ID.

Tier
: Self explanatory.

Prov Avail ID
: Provider avail ID.

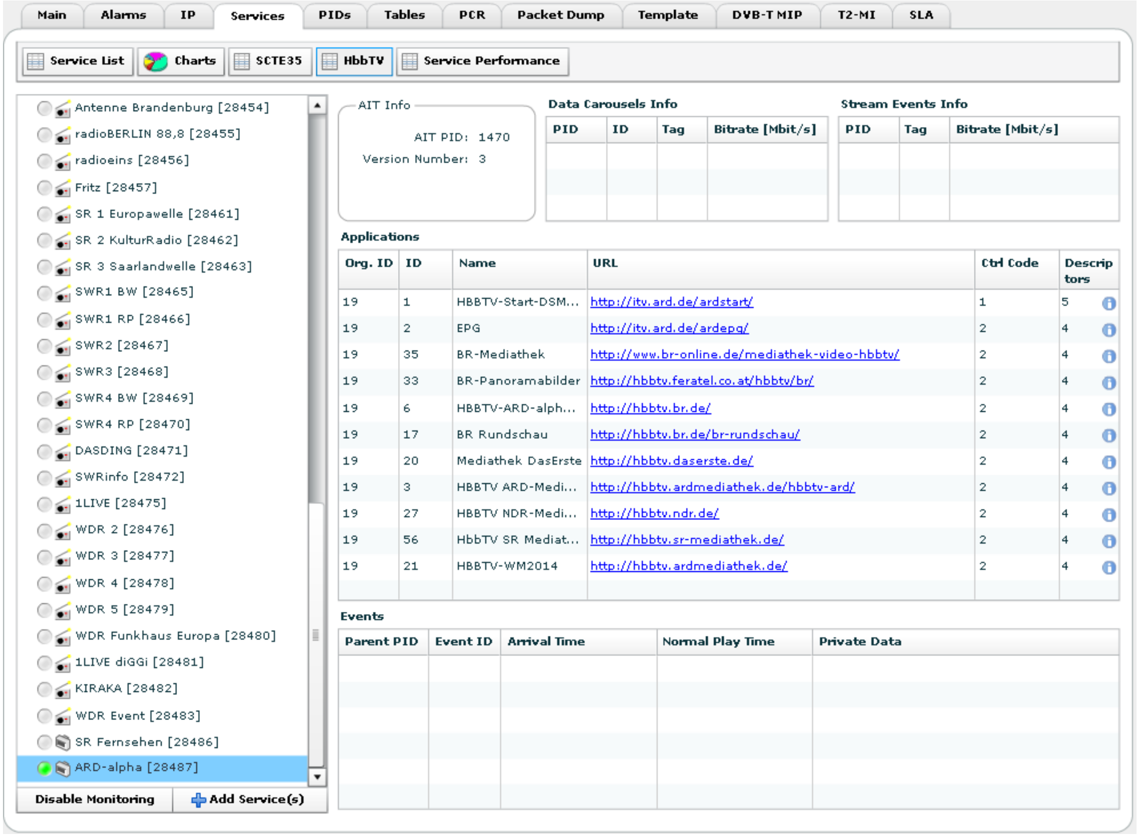
The remaining of the parameters are available as tool-tips:

Splice Event ID
: Splice event ID of the splicing point being defined.

Duration
: Duration of the break if provided.

DTFM
: In parenthesis is displayed the DTFM preroll of the splicing point being defined followed by the DTFM sequence of the splicing point being defined (if any).

9.5.2.4.4 HBBTV



Antenne Brandenburg [28454]
radioBERLIN 88,8 [28455]
radioeins [28456]
Fritz [28457]
SR 1 Europawelle [28461]
SR 2 KulturRadio [28462]
SR 3 Saarlandwelle [28463]
SWR1 BW [28465]
SWR1 RP [28466]
SWR2 [28467]
SWR3 [28468]
SWR4 BW [28469]
SWR4 RP [28470]
DASDING [28471]
SWRinfo [28472]
1LIVE [28475]
WDR 2 [28476]
WDR 3 [28477]
WDR 4 [28478]
WDR 5 [28479]
WDR Funkhaus Europa [28480]
1LIVE diGGi [28481]
KIRAKA [28482]
WDR Event [28483]
SR Fernsehen [28486]
ARD-alpha [28487]

AIT Info

AIT PID: 1470
Version Number: 3

Data Carousels Info

PID	ID	Tag	Bitrate [Mbit/s]

Stream Events Info

PID	Tag	Bitrate [Mbit/s]

Applications

Org. ID	ID	Name	URL	Ctrl Code	Descrip tors
19	1	HBBTV-Start-DSM...	http://itv.ard.de/ardstart/	1	5
19	2	EPG	http://itv.ard.de/ardepg/	2	4
19	35	BR-Mediathek	http://www.br-online.de/mediathek-video-hbbtv/	2	4
19	33	BR-Panoramabilder	http://hbbtv.feratel.co.at/hbbtv/br/	2	4
19	6	HBBTV-ARD-alph...	http://hbbtv.br.de/	2	4
19	17	BR Rundschau	http://hbbtv.br.de/br-rundschau/	2	4
19	20	Mediathek DasErste	http://hbbtv.daserste.de/	2	4
19	3	HBBTV ARD-Medi...	http://hbbtv.ardmediathek.de/hbbtv-ard/	2	4
19	27	HBBTV NDR-Medi...	http://hbbtv.ndr.de/	2	4
19	56	HbbTV SR Mediat...	http://hbbtv.sr-mediathek.de/	2	4
19	21	HBBTV-WM2014	http://hbbtv.ardmediathek.de/	2	4

Events

Parent PID	Event ID	Arrival Time	Normal Play Time	Private Data

Figure 9.69 HBBTV details

The HBBTV sub-page shown **Figure 9.69** summarizes HBBTV contents in five tables. The first one, AIT Info, is a summary of relevant information extracted from the Application Information Table, the fields contained are:

AIT PID
: PID of the AIT sub-stream registered in the PMT.

AIT Component Tags
: List of component tags signaled by the AIT on the Transport Protocol Descriptors found on the common descriptors and application descriptors.

Version Number
: AIT version number

The second table, Data Carousels Info, displays the list of existing data carousels on the service, the following information is extracted from the PMT descriptors:

PID
: Data Carousel PID

ID
: Data Carousel ID

Component Tag
: Data Carousel Component Tag found on

The third table, Stream Events Info, displays the list of existing Stream Events on the service, the following information is extracted from the PMT descriptors:

PID
: Stream Event PID

Component Tag
: Stream Event Component Tag found on the PMT

The fourth table, Applications, displays the list of existing applications found on the AIT, the following information is displayed:

Org ID
: Organization ID

ID
: Application ID

Name
: Application Name

URL
: Display Application URL extracted of a Transport Protocol Descriptor if present.

Ctrl Code
: Control Code currently been signaled by the application.

Descriptors
: Number of Descriptors found in a given application. Hovering over the field will show the descriptors IDs and descriptors tags.

The last table, Events", shows the events received by the stream events, in case no stream events PIDs are included in the HBBTV service this table will be empty. The information displayed on the table is extracted from the Stream Event Descriptors:

Event Parent PID
: PID of the Stream Event responsible of the event.

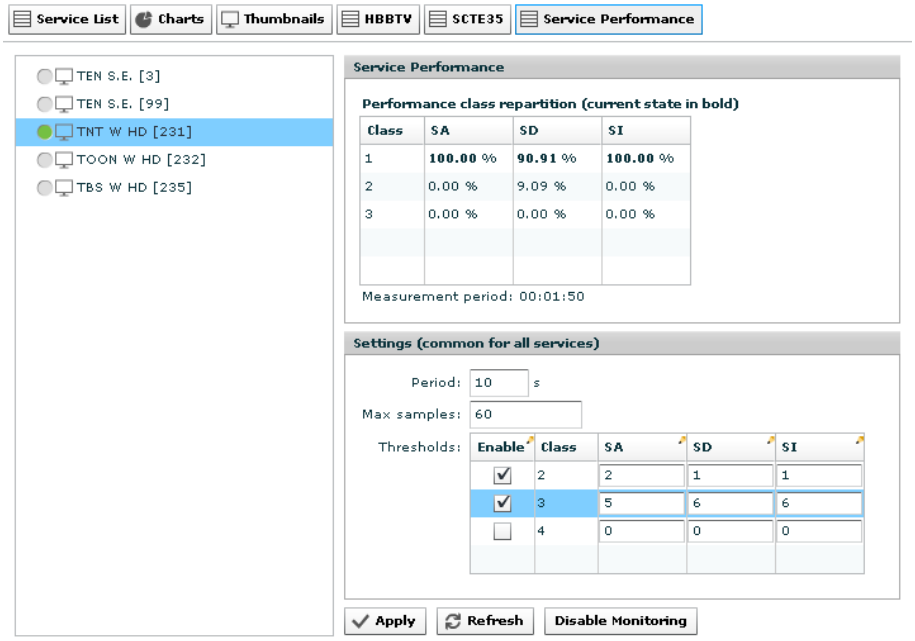
Event ID
: Event ID

Arrival Time
: Arrival Time of the event

Normal Play Time
: Normal play time if included in the event

Private Data
: Private data found in the event displayed as a string

9.5.2.4.5 Service Performance (Simplified alarms)



○ TEN S.E. [3]
○ TEN S.E. [99]
● TNT W HD [231]
○ TOON W HD [232]
○ TBS W HD [235]

Service Performance

Performance class repartition (current state in bold)

Class	SA	SD	SI
1	**100.00 %**	**90.91 %**	**100.00 %**
2	0.00 %	9.09 %	0.00 %
3	0.00 %	0.00 %	0.00 %

Measurement period: 00:01:50

Settings (common for all services)

Period: 10 s

Max samples: 60

Thresholds:

Enable	Class	SA	SD	SI
☑	2	2	1	1
☑	3	5	6	6
□	4	0	0	0

Figure 9.70 Service performance details

Description

The Service Performance sub-page shown Figure 9.70 displays information about the qualitative availability of a stream based on ETSI's recommendation relative to the evaluation of service performance [8].

Three statistical parameters – SA, SD, SI – are monitored providing the user with a way to quantify respectively the degree of availability, degradation and impairment of a service. The statistical parameters SA, SD and SI are based on the count of three subsets of alarms defined Table 9.4.

To start/stop analyzing the service performance, depress the Enable Monitoring / Disable Monitoring button. The Settings section at the bottom of the sub-page let the user parametrize the analysis, which is common for each services of the stream.

Period
: Parameter which expresses in seconds the period the sampling of SA, SD and SI.

Table 9.4 Definition of the parameters SA, SD and SI.

Note: In order to abide by the definition of the errors defined in [8], none of the alarms specified in Table 9.4 should be filtered or their limit modified (cf. Section 9.4.2). In addition, make sure that the tables PMT, PAT, NITa, NITo, SDTa and SDTo are analyzed (cf. Section 9.5.2.6).

Note: The user may however prefer to use a customized set of alarms by filtering some of them (cf. Section 9.4.2).

Parameter	Sub-parameter	Alarms ID
Service Availability (SA)	TS_sync_loss	1110 (ASI) / 151, 155 (IP)
	PAT_error	1131, 1132, 1133
	PMT_error	1151, 1152
Service Degradation (SD)	CRC_error	1220
	PCR_error	1230, 1231
	NIT_error	1311, 1312, 1313, 1316, 1317
	SDT_error	1351, 1352, 1353, 1356, 1357
Service Impairment (SI)	Continuity_count_error	1140
	Transport_error	1210

Max samples

Parameter which expresses the maximal number of samples.

Thresholds

For each parameter, a set of thresholds can be defined in the table Thresholds delimiting up to four classes.

Note: This table is common for all the services of the stream.

Note: When defining the thresholds, keep in mind that a table missing generates an error value of 100. As a result, typical threshold values are somewhere between 1 and 100 (included).

The Performance class repartition table displays the result of the statistical analysis for the selected service. For each parameter, the repartition in the different classes defined in the table Thresholds is expressed in percentage. The current class of each parameter based on the last sample is displayed in bold.

Alarms

The purpose of the table Thresholds is to enable the user set up thresholds which can optionally trigger an alarm. Three alarms can be configured to alert the operators that a service is:

- lost (Service Availability Error): triggered when the parameter SA is beyond a class defined in the Alarms page.
- degraded (Service Degradation Error): triggered when the parameter SD is beyond a class defined in the Alarms page.
- impaired (Service Impairment Error): triggered when the parameter SI is beyond a class defined in the Alarms page.

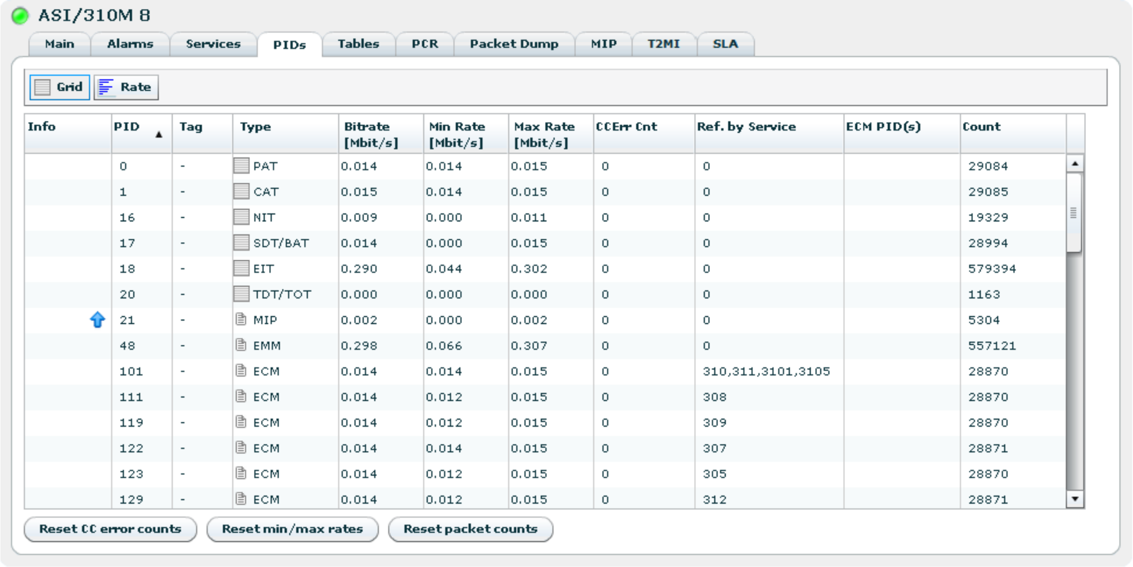
The statistical parameters SA, SD and SI are based on the count of three subsets of error defined in [8].

9.5.2.5 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.

9.5.2.5.1 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
	0	-	PAT	0.014	0.014	0.015	0	0		29084
	1	-	CAT	0.015	0.014	0.015	0	0		29085
	16	-	NIT	0.009	0.000	0.011	0	0		19329
	17	-	SDT/BAT	0.014	0.000	0.015	0	0		28994
	18	-	EIT	0.290	0.044	0.302	0	0		579394
	20	-	TDT/TOT	0.000	0.000	0.000	0	0		1163
⇧	21	-	MIP	0.002	0.000	0.002	0	0		5304
	48	-	EMM	0.298	0.066	0.307	0	0		557121
	101	-	ECM	0.014	0.014	0.015	0	310,311,3101,3105		28870
	111	-	ECM	0.014	0.012	0.015	0	308		28870
	119	-	ECM	0.014	0.012	0.015	0	309		28870
	122	-	ECM	0.014	0.014	0.015	0	307		28871
	123	-	ECM	0.014	0.012	0.015	0	305		28870
	129	-	ECM	0.014	0.012	0.015	0	312		28871

Figure 9.71 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.

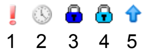


Figure 9.72 Status icons in PID details

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 couter reset.

Beneath the PID table are three buttons:

Reset CC error counts

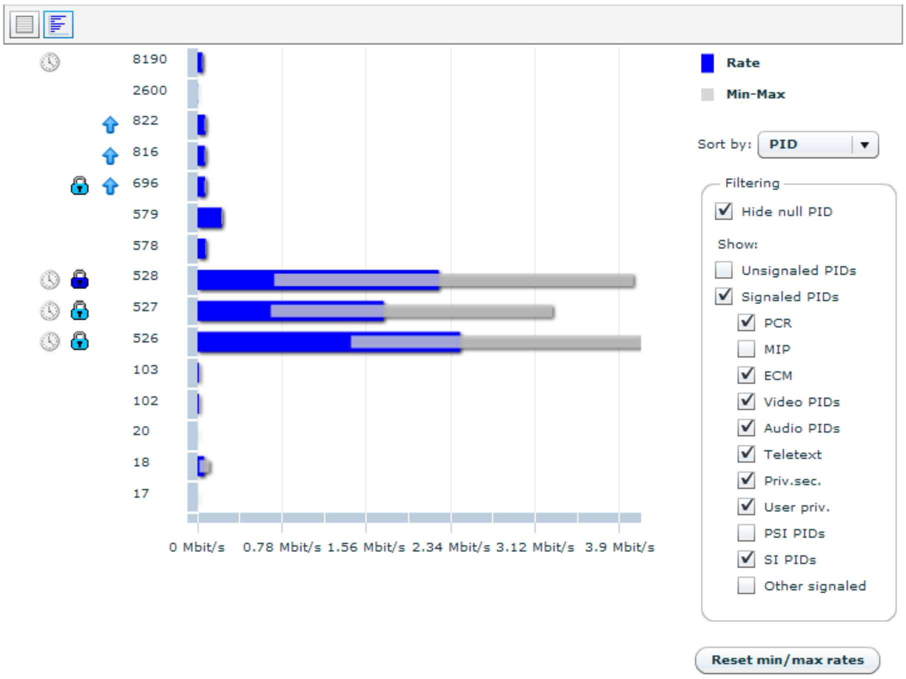
This resets the CC error counters for all packet streams.

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.

9.5.2.5.2 PID rates

The PID rates sub-tab is shown in figure 9.73. To the left is the bar chart showing the PIDs and to the right are some options for configuring the view.



Sort by: PID

Filtering

☑ Hide null PID

Show:

☐ Unsignaled PIDs
☑ Signaled PIDs
☑ PCR
☐ MIP
☑ ECM
☑ Video PIDs
☑ Audio PIDs
☑ Teletext
☑ Priv.sec.
☑ User priv.
☐ PSI PIDs
☑ SI PIDs
☐ Other signaled

Figure 9.73 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 9.72 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.

To the right of the chart, a field of options are provided to configure the view. The Sort by drop-down menu on top lets the user sort the bar chart by different parameters. The Filtering frame lets the user choose which PIDs to show. Checking the Hide null PID check box removes the null PID from the chart. Unchecking any of the other check boxes removes the corresponding PIDs from the chart. Below the Filtering frame the Reset min/max bitrates button is provided. Hitting this button resets the min and max rates counters of all PIDs.

9.5.2.6 Tables

The Tables page shows detailed information about all the tables that are currently residing in the input SI/PSIP 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.

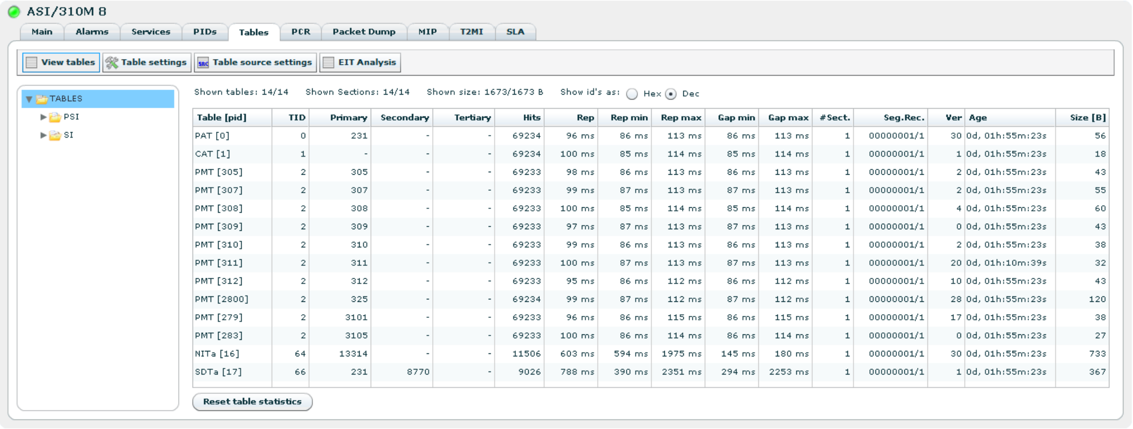
"Tables" tab
: The button switches to a detailed view of the tables present on the input and analysed by the device.

"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/PSIP tables.

"EIT Analysis" tab
: This button switches to a page showing EIT analysis.

The ViewTables sub page is shown in figure 9.74



Shown tables: 14/14 Shown Sections: 14/14 Shown size: 1673/1673 B Show id's as: ○ Hex ● Dec

Table [pid]	TID	Primary	Secondary	Tertiary	Hits	Rep	Rep min	Rep max	Gap min	Gap max	#Sect.	Seg.Rec.	Ver	Age	Size [B]
PAT [0]	0	231	-	-	69234	96 ms	86 ms	113 ms	86 ms	113 ms	1	00000001/1	30	0d, 01h:55m:23s	56
CAT [1]	1	-	-	-	69234	100 ms	85 ms	114 ms	85 ms	114 ms	1	00000001/1	1	0d, 01h:55m:23s	18
PMT [305]	2	305	-	-	69233	98 ms	86 ms	113 ms	86 ms	113 ms	1	00000001/1	2	0d, 01h:55m:23s	43
PMT [307]	2	307	-	-	69233	99 ms	87 ms	113 ms	87 ms	113 ms	1	00000001/1	2	0d, 01h:55m:23s	55
PMT [308]	2	308	-	-	69233	100 ms	85 ms	114 ms	85 ms	114 ms	1	00000001/1	4	0d, 01h:55m:23s	60
PMT [309]	2	309	-	-	69233	97 ms	87 ms	113 ms	87 ms	113 ms	1	00000001/1	0	0d, 01h:55m:23s	43
PMT [310]	2	310	-	-	69233	99 ms	86 ms	113 ms	86 ms	113 ms	1	00000001/1	2	0d, 01h:55m:23s	38
PMT [311]	2	311	-	-	69233	100 ms	87 ms	113 ms	87 ms	113 ms	1	00000001/1	20	0d, 01h:10m:39s	32
PMT [312]	2	312	-	-	69233	95 ms	86 ms	112 ms	86 ms	112 ms	1	00000001/1	10	0d, 01h:55m:23s	43
PMT [2800]	2	325	-	-	69234	99 ms	87 ms	112 ms	87 ms	112 ms	1	00000001/1	28	0d, 01h:55m:23s	120
PMT [279]	2	3101	-	-	69233	96 ms	86 ms	115 ms	86 ms	115 ms	1	00000001/1	17	0d, 01h:55m:23s	38
PMT [283]	2	3105	-	-	69233	100 ms	86 ms	114 ms	86 ms	114 ms	1	00000001/1	0	0d, 01h:55m:23s	27
NITa [16]	64	13314	-	-	11506	603 ms	594 ms	1975 ms	145 ms	180 ms	1	00000001/1	30	0d, 01h:55m:23s	733
SDTa [17]	66	231	8770	-	9026	788 ms	390 ms	2351 ms	294 ms	2253 ms	1	00000001/1	1	0d, 01h:55m:23s	367

Figure 9.74 Table details, overview.

Figure 9.74 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 sections
: The number of PSI/SI/PSIP table sections displayed in the list.

Shown size
: The size(in bytes) of the tables that fall into the chosen folder compared to the total size of the tables.

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.

Hits
: Number of section starts found on this sub-table.

Rep
: Repetition interval. This is the last interval measured between two section 0 of the sub-table.

Rep min
: Minimum repetition interval. The minimum value measured since the statistics was last reset.

Rep max
: Maximum repetition interval. Maximum value since statistics was last reset.

Gap min
: Minimum gap between sections. The minimum time measured between the last packet of a section to the first packet of the next section for this sub-table.

Gap max
: Maximum gap between sections. Same as above but maximum value measured.

# Sect.
: Number of sections.

Seg.Rec.
: Segments received. This column is only relevant for EIT schedule, which is logically divided into 32 segments. The field contains two values formatted as `M/N` . M is a 32 bit bit mask in hexadecimal format, with one bit per complete segment received of the EIT schedule sub-table, the LSB of the mask representing the first segment. If the EIT sub-table contains data for all 4 days that it represents, the mask should read 0xFFFFFFFF, meaning that at least one section is present per segment. N is the expected number of segments that should be present.

Size [B]
: Size of the table, in bytes.

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.

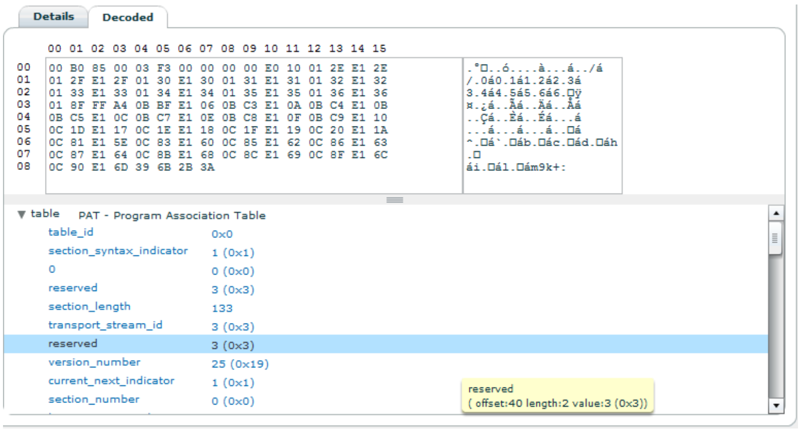
The first pane with label Details shows detailed information regarding the selected table. This pane re-iterates the details found in the TABLES column of the tree for this entry.

The second pane labelled "Decoded" allows exporting a detailed section dump. The 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 9.75 shows the decoded table.



```
    00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00  00 B0 85 00 03 F3 00 00 00 00 E0 10 01 2E E1 2E   .°□..ó....à...á../á
01  01 2F E1 2F 01 30 E1 30 01 31 E1 31 01 32 E1 32   /.0á0.1á1.2á2.3á
02  01 33 E1 33 01 34 E1 34 01 35 E1 35 01 36 E1 36   3.4á4.5á5.6á6.□ÿ
03  01 8F FF A4 0B BF E1 06 0B C3 E1 0A 0B C4 E1 0B   ¤.¿á..Ãá..Äá..Åá
04  0B C5 E1 0C 0B C7 E1 0E 0B C8 E1 0F 0B C9 E1 10   ..Çá..Èá..Éá...á
05  0C 1D E1 17 0C 1E E1 18 0C 1F E1 19 0C 20 E1 1A   ...á...á...á..□á
06  0C 81 E1 5E 0C 83 E1 60 0C 85 E1 62 0C 86 E1 63   ^.□á`.□áb.□ác.□ád.□áh
07  0C 87 E1 64 0C 8B E1 68 0C 8C E1 69 0C 8F E1 6C   .□
08  0C 90 E1 6D 39 6B 2B 3A                           ái.□ál.□ám9k+:
```

```
▼ table     PAT - Program Association Table
    table_id                    0x0
    section_syntax_indicator    1 (0x1)
    0                           0 (0x0)
    reserved                    3 (0x3)
    section_length              133
    transport_stream_id         3 (0x3)
    reserved                    3 (0x3)
    version_number              25 (0x19)
    current_next_indicator      1 (0x1)
    section_number              0 (0x0)
```

reserved
(offset:40 length:2 value:3 (0x3))

Figure 9.75 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.

The Table source settings sub page is shown in figure 9.76

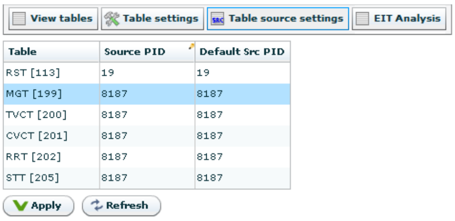


Table	Source PID	Default Src PID
RST [113]	19	19
MGT [199]	8187	8187
TVCT [200]	8187	8187
CVCT [201]	8187	8187
RRT [202]	8187	8187
STT [205]	8187	8187

Figure 9.76 Non-standard table source PID configuration.

This page allows you to configure non-standard input PID values for the section filtering of individual SI/PSIP tables.

The page is shown in figure 9.76 and contains a grid with the following columns:

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.

The Table settings sub page is shown in figure 9.77

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.

Figure 9.77 shows the page as displayed in DVB mode.

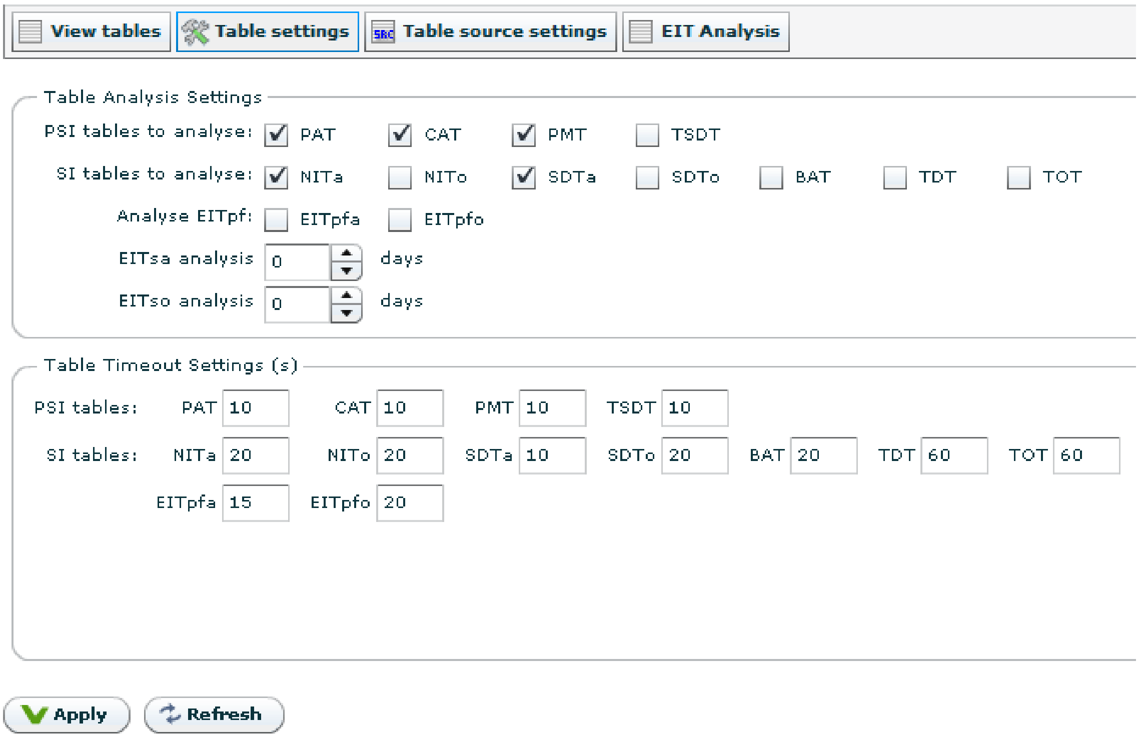


Table Analysis Settings

PSI tables to analyse: ☑ PAT ☑ CAT ☑ PMT □ TSDT

SI tables to analyse: ☑ NITa □ NITo ☑ SDTa □ SDTo □ BAT □ TDT □ TOT

Analyse EITpf: □ EITpfa □ EITpfo

EITsa analysis 0 days

EITso analysis 0 days

Table Timeout Settings (s)

PSI tables: PAT 10 CAT 10 PMT 10 TSDT 10

SI tables: NITa 20 NITo 20 SDTa 10 SDTo 20 BAT 20 TDT 60 TOT 60

EITpfa 15 EITpfo 20

Figure 9.77 Table analysis configuration.

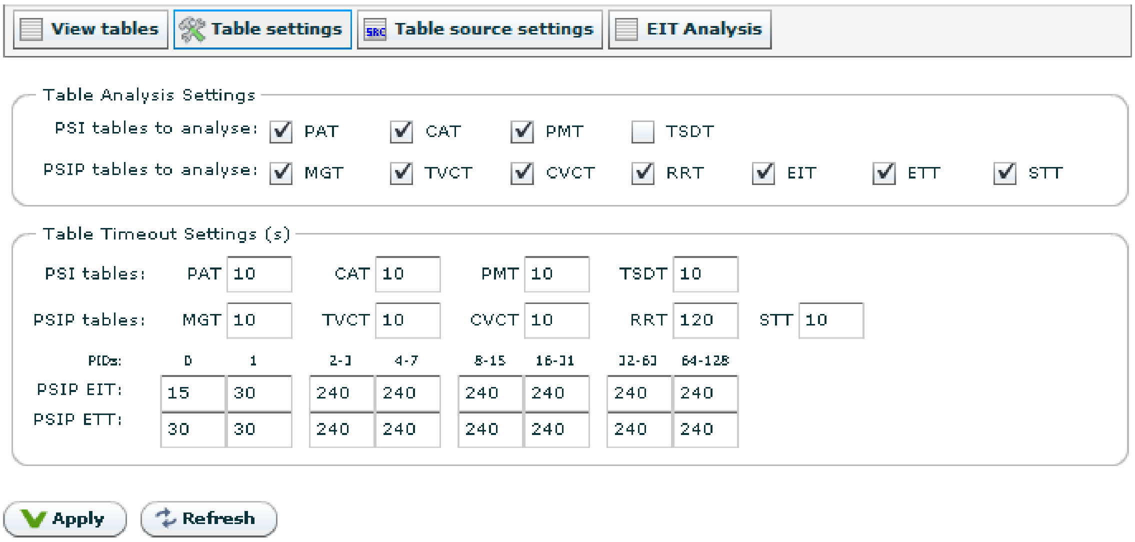


Table Analysis Settings

PSI tables to analyse: ☑ PAT ☑ CAT ☑ PMT □ TSDT

PSIP tables to analyse: ☑ MGT ☑ TVCT ☑ CVCT ☑ RRT ☑ EIT ☑ ETT ☑ STT

Table Timeout Settings (s)

PSI tables: PAT 10 CAT 10 PMT 10 TSDT 10

PSIP tables: MGT 10 TVCT 10 CVCT 10 RRT 120 STT 10

PIDs:	0	1	2-3	4-7	8-15	16-31	32-63	64-128
PSIP EIT:	15	30	240	240	240	240	240	240
PSIP ETT:	30	30	240	240	240	240	240	240

Figure 9.78 Table analysis configuration in ATSC mode.

In DVB/ATSC mode the page looks different, as shown in figure 9.78

- To be able to see programs and program components you must analyse at least PAT and PMT.

- To see the service name for the services you have to configure analysis of SDTa (SDT actual) for DVB services, or TVCT/CVCT for ATSC services
- 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.

9.5.2.6.1 EIT Analysis

The EIT Analysis sub page is shown in figure 9.79, which has the following columns:

SID
: The program number/service id of the service

Table Section
: Indicates the Table section EIT belongs to.

events.

The total duration of the gaps is shown in brackets.

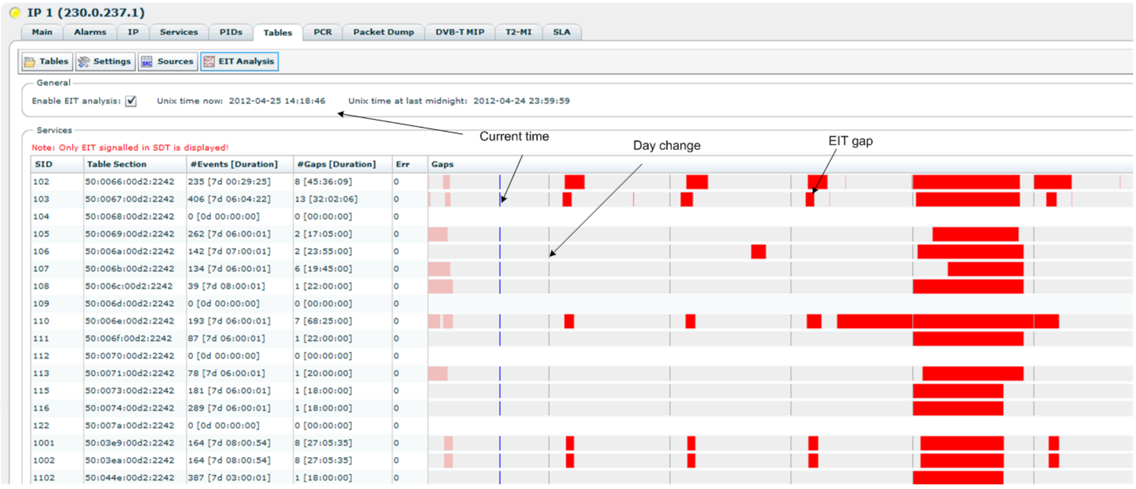
Err
: Indicates the total number of errors for the corresponding service.

Gaps
: Shows gaps in time

> **Note:** Only EIT signalled in SDT is displayed.

In figure 9.79, the blue line indicates the current time. This is the same as the Unix time now field at the top. The red field indicates that a EIT gap is found in the EPG. Gaps that appear in the past (i.e before the blue line) are not counted in the #Gaps [Duration] field. The black line indicates a change of day (00:00:00 hours), and the grey area indicates how much time event information is present for a specific service id.

A tooltip will open if you place your mouse over a gap or over the field Err. Holding your mouse over a gap will show a list of gaps for the specific service id with the corresponding start time and duration. In the case of Err, this will open a tooltip that shows detected errors in the EIT. As you can see from the screenshot the tooltip in this example shows a problem with Illegal following event start time.



Enable EIT analysis: ☑ Unix time now: 2012-04-25 14:18:46 Unix time at last midnight: 2012-04-24 23:59:59

Note: Only EIT signalled in SDT is displayed!

SID	Table Section	#Events [Duration]	#Gaps [Duration]	Err	Gaps
102	50:0066:00d2:2242	235 [7d 00:29:25]	8 [45:36:09]	0	
103	50:0067:00d2:2242	406 [7d 06:04:22]	13 [32:02:06]	0	
104	50:0068:00d2:2242	0 [0d 00:00:00]	0 [00:00:00]	0	
105	50:0069:00d2:2242	262 [7d 06:00:01]	2 [17:05:00]	0	
106	50:006a:00d2:2242	142 [7d 07:00:01]	2 [23:55:00]	0	
107	50:006b:00d2:2242	134 [7d 06:00:01]	6 [19:45:00]	0	
108	50:006c:00d2:2242	39 [7d 08:00:01]	1 [22:00:00]	0	
109	50:006d:00d2:2242	0 [0d 00:00:00]	0 [00:00:00]	0	
110	50:006e:00d2:2242	193 [7d 06:00:01]	7 [68:25:00]	0	
111	50:006f:00d2:2242	87 [7d 06:00:01]	1 [22:00:00]	0	
112	50:0070:00d2:2242	0 [0d 00:00:00]	0 [00:00:00]	0	
113	50:0071:00d2:2242	78 [7d 06:00:01]	1 [20:00:00]	0	
115	50:0073:00d2:2242	181 [7d 06:00:01]	1 [18:00:00]	0	
116	50:0074:00d2:2242	289 [7d 06:00:01]	1 [18:00:00]	0	
122	50:007a:00d2:2242	0 [0d 00:00:00]	0 [00:00:00]	0	
1001	50:03e9:00d2:2242	164 [7d 08:00:54]	8 [27:05:35]	0	
1002	50:03ea:00d2:2242	164 [7d 08:00:54]	8 [27:05:35]	0	
1102	50:044e:00d2:2242	387 [7d 03:00:01]	1 [18:00:00]	0	

Figure 9.79 EIT Analysis.

Associated with the information displayed in the error field there is an alarm configuration for each error type, in addition to a gap alarm. These alarms are shown in figure 9.80.

9.5.2.7 Template

The Template page shown Figure 9.81 offers the possibility to automatically or manually define a template for each stream. An alarm is triggered in case of discrepancy between the template and the stream being monitored.

The template can be configured manually by filling out the various fields, or by using the snapshot functionality. Depressing the Snapshot button at the bottom the page fills out automatically the template with the properties of the stream at the moment when the button is depressed.

Each field is paired with a check-box letting the user decide whether a field should be part of the template or ignored.

In the case where a mismatch occurs for a field, it gets framed with red and a tool-tip explicits what value the field currently takes and what value was expected. The green and red chips indicate the status of a template or service (green meaning that the related element matches completely the template, while red meaning that at least one field mismatches the template). The tool-tips over the red chips provides a condensed information about the related element.

The templates are checked every 5 seconds.

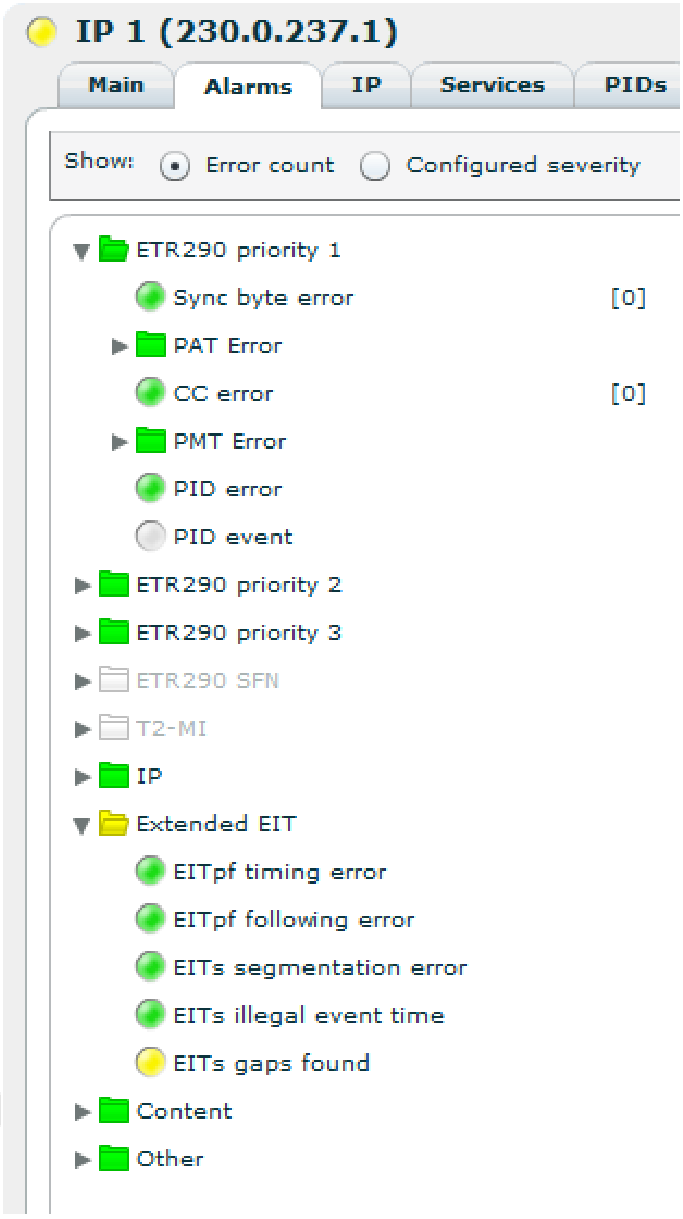
General Settings section

The General Settings section gathers information about the template and the transport stream.

Template enabled
    Manually enables/disables a template.

Template label
    User-defined label for the template.

The remaining fields let the user define the expected



Show: ● Error count ○ Configured severity

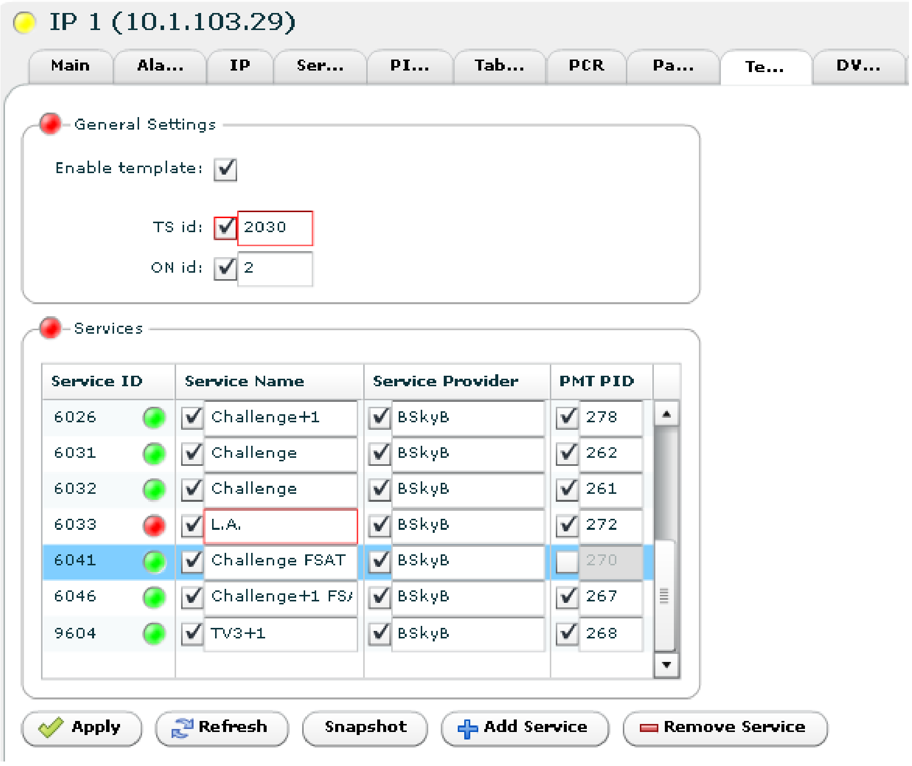
- ▼ ETR290 priority 1
  - Sync byte error [0]
  - ▶ PAT Error
  - CC error [0]
  - ▶ PMT Error
  - PID error
  - PID event
- ▶ ETR290 priority 2
- ▶ ETR290 priority 3
- ▶ ETR290 SFN
- ▶ T2-MI
- ▶ IP
- ▼ Extended EIT
  - EITpf timing error
  - EITpf following error
  - EITs segmentation error
  - EITs illegal event time
  - EITs gaps found
- ▶ Content
- ▶ Other

Figure 9.80 EIT Analysis related alarms.

- TS id
- Original Network id

Services section

The Services section located at the bottom of the page let the user defines the properties of each services to be monitored.



General Settings

Enable template: ☑

TS id: ☑ 2030

ON id: ☑ 2

Services

Service ID		Service Name	Service Provider	PMT PID
6026	🟢	☑ Challenge+1	☑ BSkyB	☑ 278
6031	🟢	☑ Challenge	☑ BSkyB	☑ 262
6032	🟢	☑ Challenge	☑ BSkyB	☑ 261
6033	🔴	☑ L.A.	☑ BSkyB	☑ 272
6041	🟢	☑ Challenge FSAT	☑ BSkyB	□ 270
6046	🟢	☑ Challenge+1 FS/	☑ BSkyB	☑ 267
9604	🟢	☑ TV3+1	☑ BSkyB	☑ 268

Figure 9.81 Template monitor

The table on the left of the section lists the services that are included in the template. It is possible to manually add or remove a service from the list by depressing respecitvely the buttons Add service or Remove service.

For each service the following properties are optionally monitored:

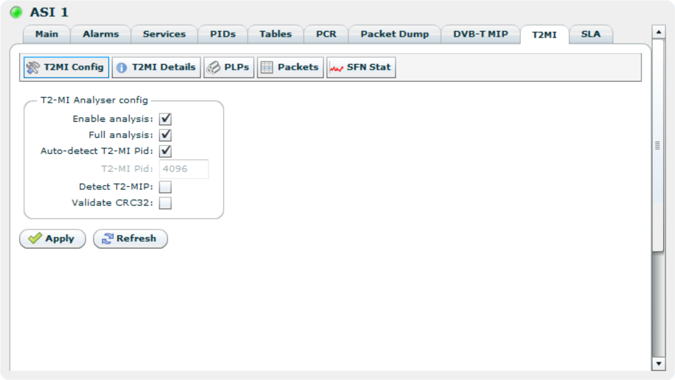
- the service name
- the service provider name
- the PMT pid

Note: Any service part of the stream but not present in the service list of the template is ignored.

9.5.2.8 T2-MI

The T2-MI analysis page contains five subpages: T2MI Config, T2MI Details, PLPs, Packets and SFN Stat.

T2-MI Config



T2-MI Analyser config

Enable analysis: ☑
Full analysis: ☑
Auto-detect T2-MI Pid: ☑
T2-MI Pid: 4096
Detect T2-MIP: ☐
Validate CRC32: ☐

Figure 9.82 T2-MI Analysis configuration

The **T2MI Config** subpage is shown in 9.82. It allows the user to configure the T2-MI analysis feature by providing the following options:

Enable analysis
Allows the user to enable/disable T2-MI analysis. When enabled, the T2-MI analyser analyses all T2-MI packets in the stream, but skips CRC32 validation on Baseband frames.

Full analysis
Allows the user to enable/disable full T2-MI analysis. With full T2-MI analysis enabled, the payload of the BB frames will also be possible to analyse through PLP extraction.

Auto-detect T2-MI pid
Allows the user to enable/disable automatic detection of the T2-MI pid value. When enabled, the analyser will search for the T2-MI data pid from the PAT and PMT signalling.

T2-MI pid
Allows the user to manually specify the T2-MI pid value.

Detect T2-MIP
By enabling T2-MIP detection, the analyser will search for the T2-MIP contained in the T2-MI stream. Enabling this option will also activate the T2-MIP alarms. Requires full analysis.

Validate CRC32
Allows the user to enable/disable CRC32 validation on Baseband frames. Be aware that CRC32 validation is a very CPU intensive operation.

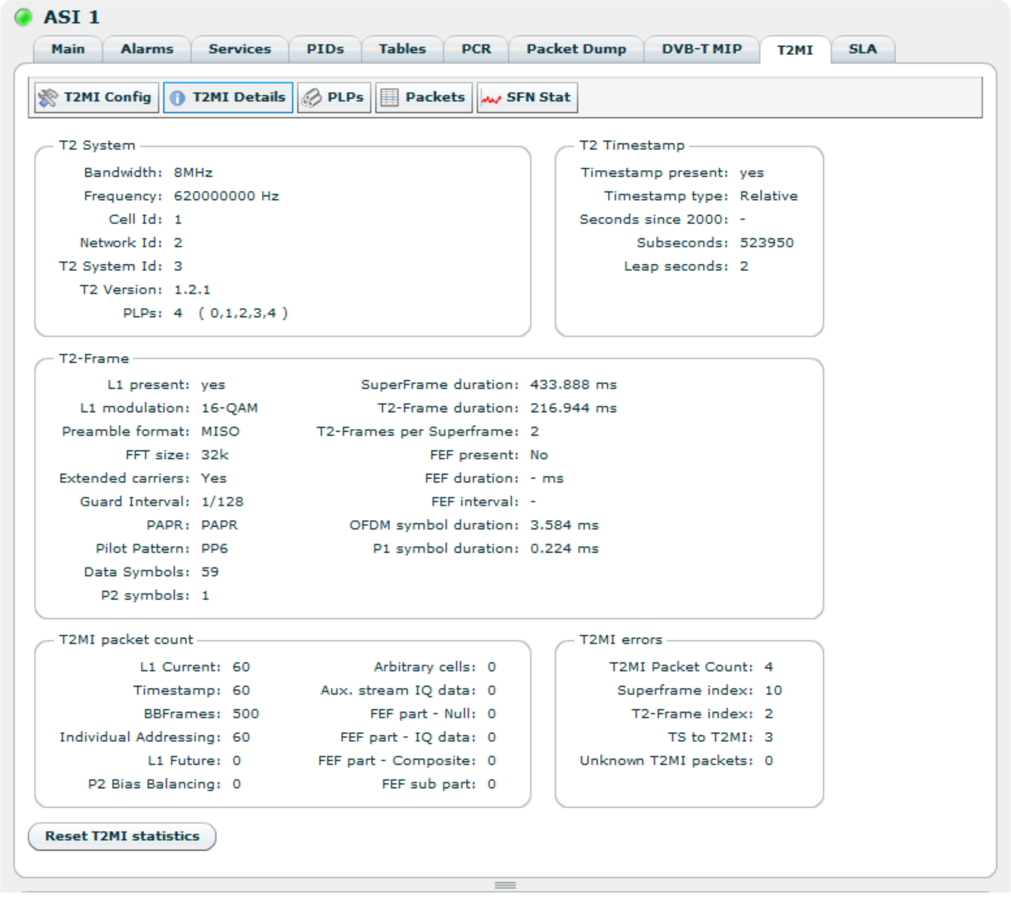
T2-MI Details

The **T2MI Details** page provides five different sections, as shown in 9.83.

The T2 System section displays information about the T2 System:

Bandwidth
This field allows the setting of the bandwidth of the transmission channel. Possible values are 1.7MHz, 5MHz, 6MHz, 7MHz, 8MHz, 10MHz.

Frequency
This field identifies the frequency of the transmission channel.



T2 System

Bandwidth: 8MHz
Frequency: 620000000 Hz
Cell Id: 1
Network Id: 2
T2 System Id: 3
T2 Version: 1.2.1
PLPs: 4 (0,1,2,3,4)

T2 Timestamp

Timestamp present: yes
Timestamp type: Relative
Seconds since 2000: -
Subseconds: 523950
Leap seconds: 2

T2-Frame

L1 present: yes
L1 modulation: 16-QAM
Preamble format: MISO
FFT size: 32k
Extended carriers: Yes
Guard Interval: 1/128
PAPR: PAPR
Pilot Pattern: PP6
Data Symbols: 59
P2 symbols: 1
SuperFrame duration: 433.888 ms
T2-Frame duration: 216.944 ms
T2-Frames per Superframe: 2
FEF present: No
FEF duration: - ms
FEF interval: -
OFDM symbol duration: 3.584 ms
P1 symbol duration: 0.224 ms

T2MI packet count

L1 Current: 60
Timestamp: 60
BBFrames: 500
Individual Addressing: 60
L1 Future: 0
P2 Bias Balancing: 0
Arbitrary cells: 0
Aux. stream IQ data: 0
FEF part - Null: 0
FEF part - IQ data: 0
FEF part - Composite: 0
FEF sub part: 0

T2MI errors

T2MI Packet Count: 4
Superframe index: 10
T2-Frame index: 2
TS to T2MI: 3
Unknown T2MI packets: 0

Figure 9.83 T2-MI Analysis details

Cell ID
: This field identifies a geographic cell in a DVB-T2 network.

Network ID
: This field identifies the current DVB-T2 network.

T2 System ID
: This field identifies the DVB-T2 system within the DVB-T2 network.

T2 version
: This field identifies the version of the DVB-T2 specification.

PLPs
: The number of PLPs signalled in L1 current. Additionally, the PLP IDs detected in a stream is listed here.

The T2 Timestamp section contains the following parameters:

Timestamp Present
: This field indicates whether Timestamp is present.

Timestamp type

This field indicates the type of the time stamp to be sent to the modulator. Possible values are:

- Null: Seconds and subsecond field set to 1's.
- Relative: Seconds field set to 0's, while subsecond field locked to 1PPS.
- Absolute: Seconds field locked to SNTP, subsecond field locked to 1PPS.

Seconds since 2000

If the timestamp is of type Absolute type, this field shows the number of seconds since 2000 excluding leap seconds.

Subseconds

If the timestamp is of type Absolute or Relative type, this field shows the subseconds field of the T2-MI Timestamp.

Leap seconds

The number of leap seconds signalled in the T2-MI Timestamp packet.

The T2-Frame section contains the following parameters:

L1 present

This field indicates whether L1 is present.

L1-modulation

This field indicates the used modulation for the L1 signalling. Possible values are:

- Binary Phase Shift Keying (BPSK)
- Quadrature Phase Shift Keying (QPSK)
- 16 Quadrature Amplitude Modulation (16-QAM)
- 64 Quadrature Amplitude Modulation (64-QAM)

Preamble format

The preamble is a DVB-T2 preamble that indicates whether the P2 part should be transmitted in MISO (Multiple Input Single Output) or SISO (Single Input Single Output)format.

FFT size

This field indicates the nominal FFT size of the symbols. Possible values are 1K, 2K, 4K, 8K, 16K, 32K.

Extended carriers

The extended carrier mode allows an optimum use of the channel bandwidth together with the higher FFT sizes (supported for 8K, 16K and 32K FFT).

Guard interval

Guard intervals are used to ensure that distinct transmissions do not interfere with one another. It can be seen as a hard limit to the channel extent that can be tolerated by the system.

PAPR
Two Peak-to-average power ratio (PAPR) reduction techniques are supported in DVB-T2:

- for DVB-T2 version 1.1.1 supported techniques are Active Constellation Extension (ACE) and Tone Reservation (TR). The two techniques are not mutually exclusive and a combination of them can be used.
- for DVB-T2 version 1.2.1 supported techniques are L1-ACE/P2-TR, L1-ACE/ACE-PAPR, L1-ACE/TR-PAPR, L1-ACE/ACE and TR

Pilot pattern
Pilot patterns are used by the receiver to estimate changes in channel response in both time and frequency dimensions. There are eight patterns available.

Data Symbols
Number of symbols in one T2 Frame used for Data symbols.

P2 Symbols
Number of symbols in one T2 Frame used for P2.

Superframe duration
Duration of one Super Frame in microseconds. Sum of T2-Frames and FEF parts.

T2-Frame duration
Duration of one T2 Frame in microseconds.

T2-Frames per Superframe
Number of T2 Frames per superframe.

FEF present
States whether Future Extension Frames are detected in the stream.

FEF duration
Duration of the FEF part in milliseconds.

FEF interval
Number of T2-Frames between each FEF part.

OFDM symbol duration
Duration of one OFDM symbol in milliseconds.

P1 symbol duration
Duration of one P1 symbol in milliseconds.

The T2MI Packet Count section contains counters which increases for each packet type recevied.

Finally, The T2MI Errors section provides error counters for the T2-MI stream. Four or five error counters are displayed depending on the the level of analysis chosen. A brief explanation of the error counters are given below.

T2MI Packet Count
This error counter is triggered when the T2-MI packet count field does not update correctly.

Superframe index

Superframe index is incremented if it detects a jump in the superframe index field in a stream.

T2-Frame index

T2-Frame index is incremented if the T2 frames index are not sequential within the boundaries of the signalled T2 frames per superframe.

TS to T2MI

Errors when parsing the T2-MI stream from the outer layer TS.

CRC32

This counter reports T2-MI frame CRC32 errors. This counter is only available in full analysis mode.

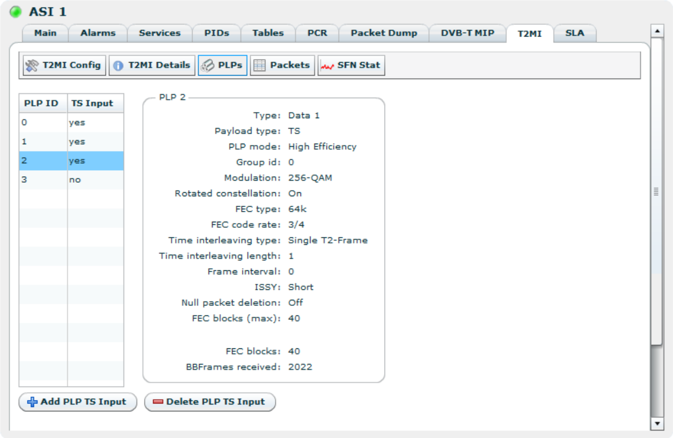
Unknown T2MI packets

If the monitor recieve packets that are not defined in ETSI TS 102 773 1.2.1, this error counter would increment.

At the bottom of the page is a button that allows you to reset all the T2-MI statistics.

PLPs

The **PLPs** subpage shows information about the individual PLP(s) contained in the T2-MI stream, as shown in 9.84. When full T2-MI analysis is enabled, the user can monitor multiple PLPs by adding PLP TS inputs from the left side table. PLPs that are added as TS inputs are visible under the corresponding TS input port shown in the Inputs overview list to the left. These inputs will now have similar page views and monitoring capabilities as for regular TS inputs which are more detailly described in **Section 9.5.2**



PLP ID	TS Input
0	yes
1	yes
2	yes
3	no

PLP 2

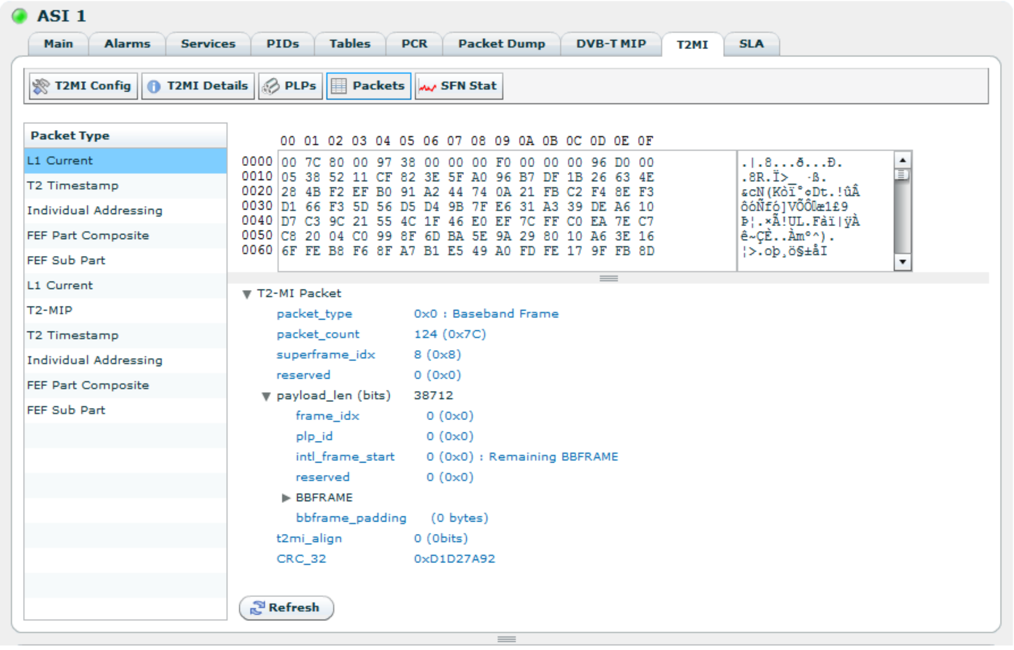
Type: Data 1
Payload type: TS
PLP mode: High Efficiency
Group id: 0
Modulation: 256-QAM
Rotated constellation: On
FEC type: 64k
FEC code rate: 3/4
Time interleaving type: Single T2-Frame
Time interleaving length: 1
Frame interval: 0
ISSY: Short
Null packet deletion: Off
FEC blocks (max): 40

FEC blocks: 40
BBFrames received: 2022

Figure 9.84 PLP analysis

Packets

The **Packets** subpage lets the user analyse the content of various packet types inside a T2-MI stream. Five packet types are available, namely L1 Current, T2 Timestamp, Individual Addressing, FEF Part Composite and FEF Sub Part. The interface offers detailed information of all the packet fields, and hexadecimal representation of the packet as a whole. A screenshot of the Packets sub-page can be seen in 9.85.



```
Packet Type
L1 Current
T2 Timestamp
Individual Addressing
FEF Part Composite
FEF Sub Part
L1 Current
T2-MIP
T2 Timestamp
Individual Addressing
FEF Part Composite
FEF Sub Part
```

```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000 00 7C 80 00 97 38 00 00 00 F0 00 00 00 96 D0 00   .|.8...ð...Ð.
0010 05 38 52 11 CF 82 3E 5F A0 96 B7 DF 1B 26 63 4E   .8R.Ï>_ ·ß.
0020 28 4B F2 EF B0 91 A2 44 74 0A 21 FB C2 F4 8E F3   &cN(Kòï°¢Dt.!ûÂ
0030 D1 66 F3 5D 56 D5 D4 9B 7F E6 31 A3 39 DE A6 10   ôóÑfó]VÕÔæ1£9
0040 D7 C3 9C 21 55 4C 1F 46 E0 EF 7C FF C0 EA 7E C7   Þ¦.×Ã!UL.Fàï|ÿÀ
0050 C8 20 04 C0 99 8F 6D BA 5E 9A 29 80 10 A6 3E 16   ê~ÇÈ..Àm°^).
0060 6F FE B8 F6 8F A7 B1 E5 49 A0 FD FE 17 9F FB 8D   ¦>.oþ¸ö§±åI
```

```
▼ T2-MI Packet
    packet_type          0x0 : Baseband Frame
    packet_count         124 (0x7C)
    superframe_idx       8 (0x8)
    reserved             0 (0x0)
  ▼ payload_len (bits)   38712
        frame_idx            0 (0x0)
        plp_id               0 (0x0)
        intl_frame_start     0 (0x0) : Remaining BBFRAME
        reserved             0 (0x0)
      ▶ BBFRAME
        bbframe_padding      (0 bytes)
    t2mi_align           0 (0bits)
    CRC_32               0xD1D27A92
```

Figure 9.85 T2-MI Packet viewer

SFN Stat

The **SFN Stat** subpage presents the SFN delay statistics as shown in 9.86. The SFN delay is a measurement of the delay from the gateway to the transmission over air given in milliseconds. This can provide meaningfull information to network operators if the delay tends to drift. It is possible to present the SFN delay over four different periods, ranging from the last minute to the last week.

9.5.2.9 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.

Samples

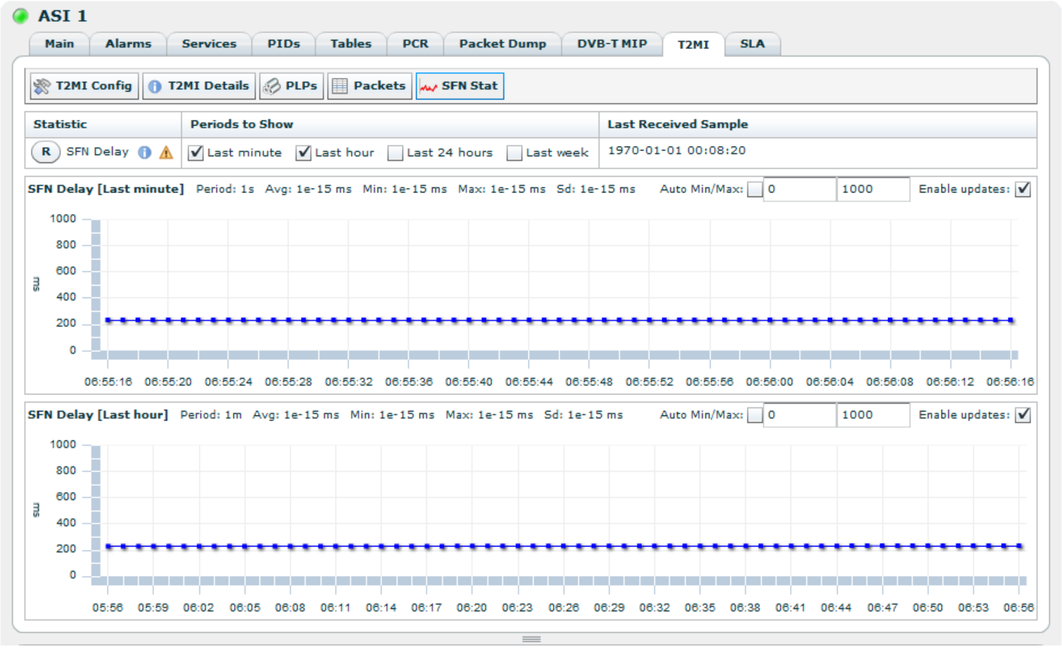
The number of Program Clock Reference samples received

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.

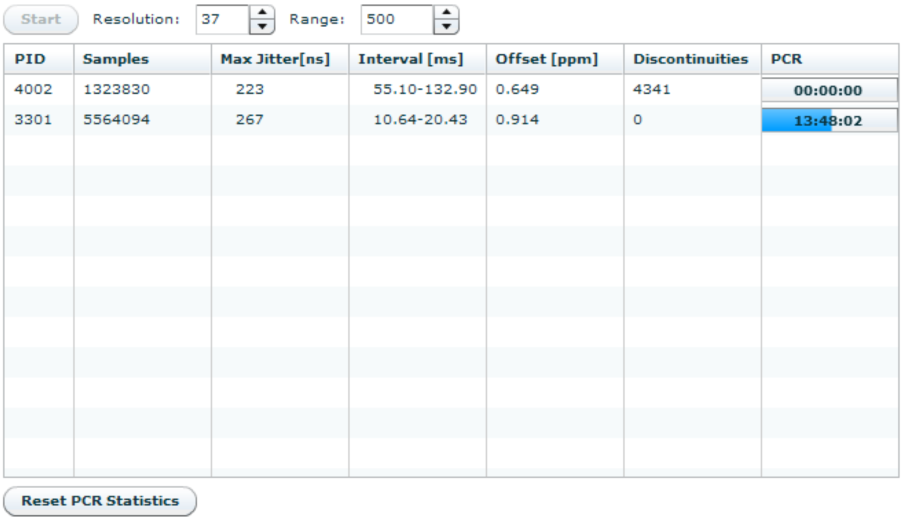


Statistic	Periods to Show	Last Received Sample
R SFN Delay	☑ Last minute ☑ Last hour □ Last 24 hours □ Last week	1970-01-01 00:08:20

SFN Delay [Last minute] Period: 1s Avg: 1e-15 ms Min: 1e-15 ms Max: 1e-15 ms Sd: 1e-15 ms Auto Min/Max: □ 0 1000 Enable updates: ☑

SFN Delay [Last hour] Period: 1m Avg: 1e-15 ms Min: 1e-15 ms Max: 1e-15 ms Sd: 1e-15 ms Auto Min/Max: □ 0 1000 Enable updates: ☑

Figure 9.86 T2-MI SFN Delay Statistics



Resolution: 37 Range: 500

PID	Samples	Max Jitter[ns]	Interval [ms]	Offset [ppm]	Discontinuities	PCR
4002	1323830	223	55.10-132.90	0.649	4341	00:00:00
3301	5564094	267	10.64-20.43	0.914	0	13:48:02

Figure 9.87 PCR PID List

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.

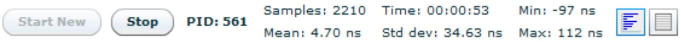
PCR

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 9.89**.

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.



PID: 561

Samples: 2210 Time: 00:00:53 Min: -97 ns

Mean: 4.70 ns Std dev: 34.63 ns Max: 112 ns

Figure 9.88 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 intevals 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.

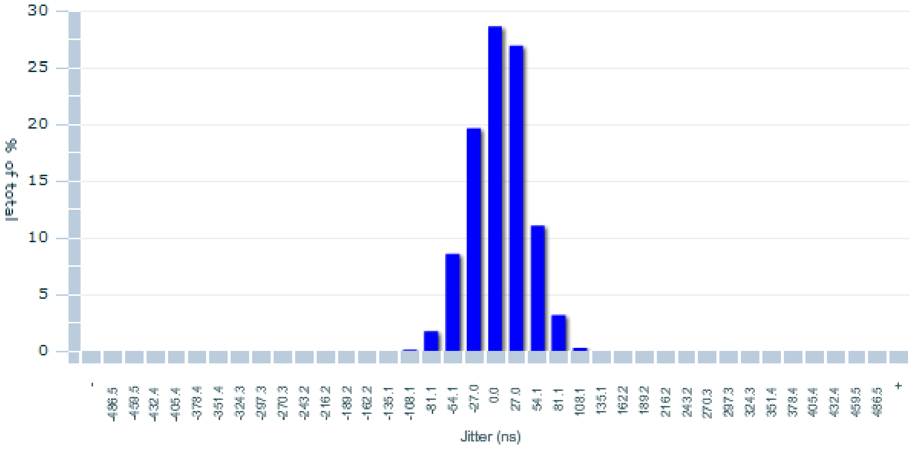
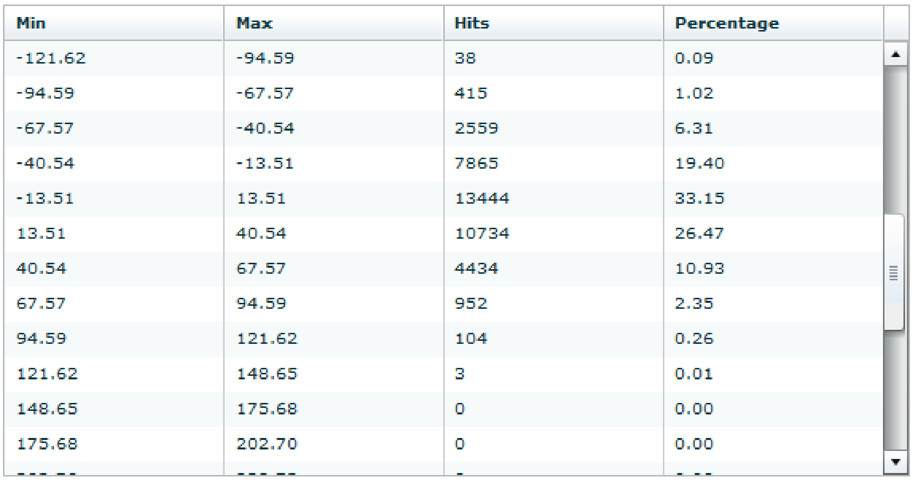


Figure 9.89 PCR Graph view

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 inteval. 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.

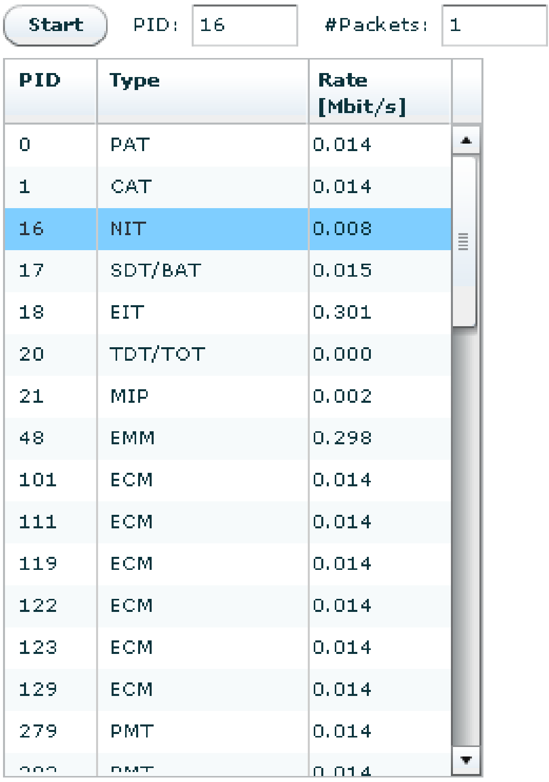


Min	Max	Hits	Percentage
-121.62	-94.59	38	0.09
-94.59	-67.57	415	1.02
-67.57	-40.54	2559	6.31
-40.54	-13.51	7865	19.40
-13.51	13.51	13444	33.15
13.51	40.54	10734	26.47
40.54	67.57	4434	10.93
67.57	94.59	952	2.35
94.59	121.62	104	0.26
121.62	148.65	3	0.01
148.65	175.68	0	0.00
175.68	202.70	0	0.00

Figure 9.90 PCR Table view

9.5.2.10 Packet Dump

The packet dump page offers dumping the contents of a sequence of packets from a selected packet stream.

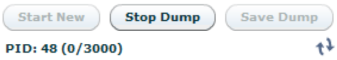


PID: 16 #Packets: 1

PID	Type	Rate [Mbit/s]
0	PAT	0.014
1	CAT	0.014
16	NIT	0.008
17	SDT/BAT	0.015
18	EIT	0.301
20	TDT/TOT	0.000
21	MIP	0.002
48	EMM	0.298
101	ECM	0.014
111	ECM	0.014
119	ECM	0.014
122	ECM	0.014
123	ECM	0.014
129	ECM	0.014
279	PMT	0.014
[illegible]	PMT	0.014

Figure 9.91 Packet Dump

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.



PID: 48 (0/3000)

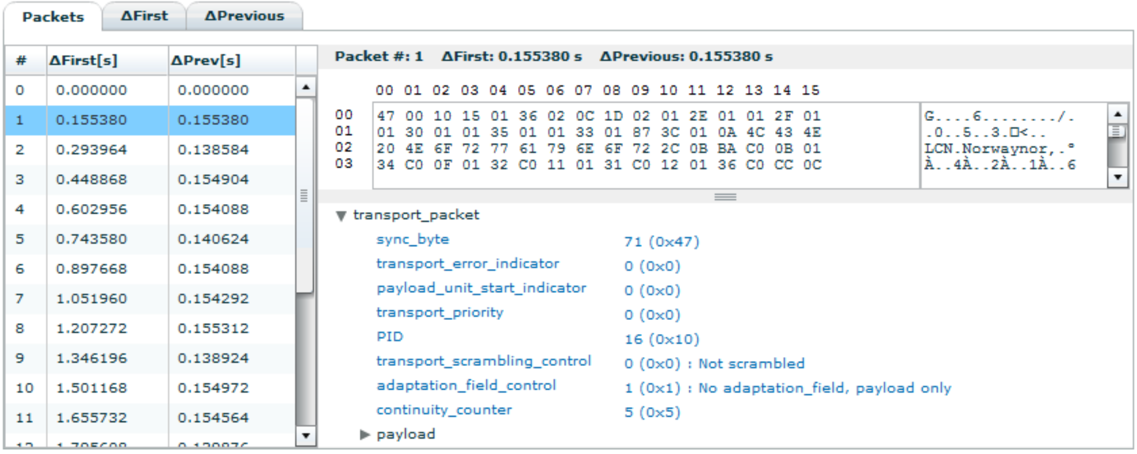
Figure 9.92 Packet Dump Progress

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 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.



#	ΔFirst[s]	ΔPrev[s]
0	0.000000	0.000000
1	0.155380	0.155380
2	0.293964	0.138584
3	0.448868	0.154904
4	0.602956	0.154088
5	0.743580	0.140624
6	0.897668	0.154088
7	1.051960	0.154292
8	1.207272	0.155312
9	1.346196	0.138924
10	1.501168	0.154972
11	1.655732	0.154564

Packet #: 1 ΔFirst: 0.155380 s ΔPrevious: 0.155380 s

```
    00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
00  47 00 10 15 01 36 02 0C 1D 02 01 2E 01 01 2F 01   G....6......../.
01  01 30 01 01 35 01 01 33 01 87 3C 01 0A 4C 43 4E   .0..5..3.□<..
02  20 4E 6F 72 77 61 79 6E 6F 72 2C 0B BA C0 0B 01   LCN.Norwaynor,.°
03  34 C0 0F 01 32 C0 11 01 31 C0 12 01 36 C0 CC 0C   À..4À..2À..1À..6
```

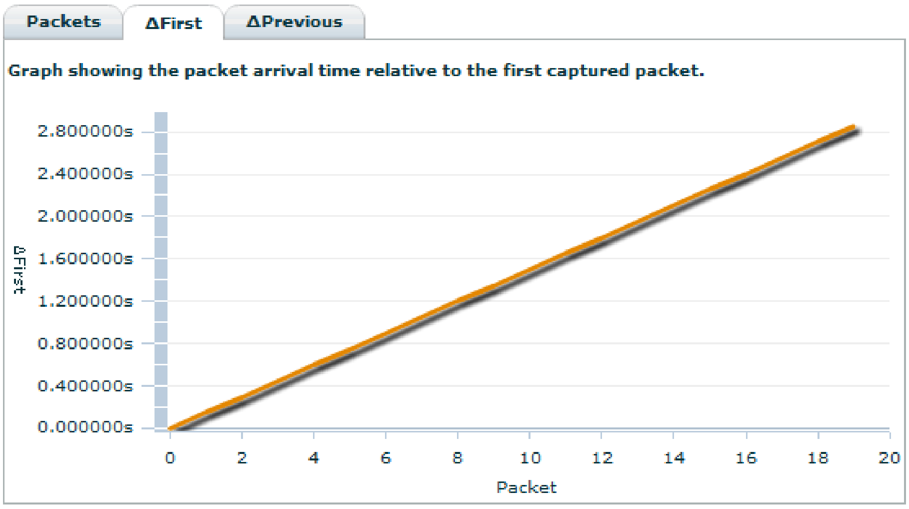
```
▼ transport_packet
    sync_byte                       71 (0x47)
    transport_error_indicator       0 (0x0)
    payload_unit_start_indicator    0 (0x0)
    transport_priority              0 (0x0)
    PID                             16 (0x10)
    transport_scrambling_control    0 (0x0) : Not scrambled
    adaptation_field_control        1 (0x1) : No adaptation_field, payload only
    continuity_counter              5 (0x5)
  ▶ payload
```

Figure 9.93 Packet Dump Packets

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 preceeding 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.

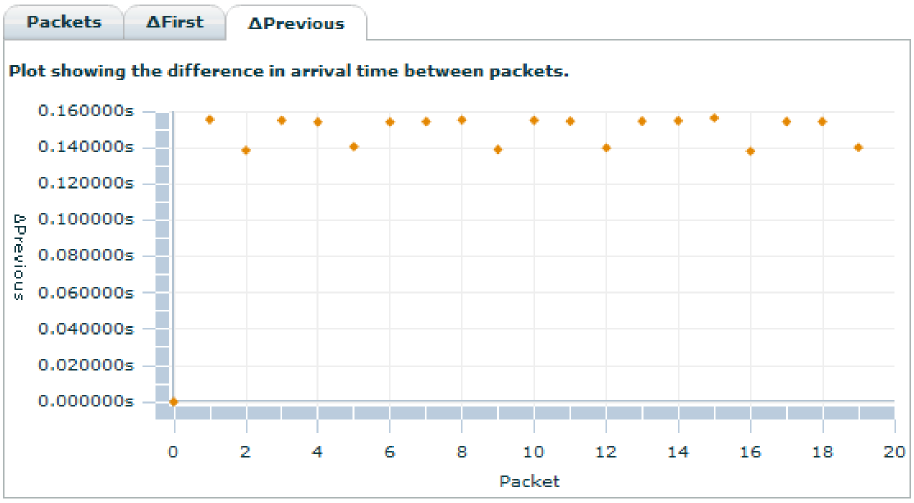
The **Delta first** tab shows a graph with the delta first value of all the dumped packets. This gives an indication of the packet rate variation over time of the selected packet stream.



Graph showing the packet arrival time relative to the first captured packet.

Figure 9.94 Packet Dump Delta First

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.



Plot showing the difference in arrival time between packets.

Figure 9.95 Packet Dump Delta Previous

9.5.2.11 MIP

9.5.2.11.1 MIP Details

The MIP analysis page is shown in figure 9.96.

MIP packets are not relevant in ATSC mode, thus this tab will not appear unless the operational mode is set to DVB.

At the top of the page there is a checkbox where you can choose to analyse incoming MIP packets. If you enable MIP analysis, the bottom part of the page gives you information on any incoming MIP packets.

The **MIP Details** view provides four different sections. The Status section displays information pertaining to MIP packet transport:

MIP present
This tells you whether MIP packets are present in the stream. If they are not, all other fields in all three sections show no information.

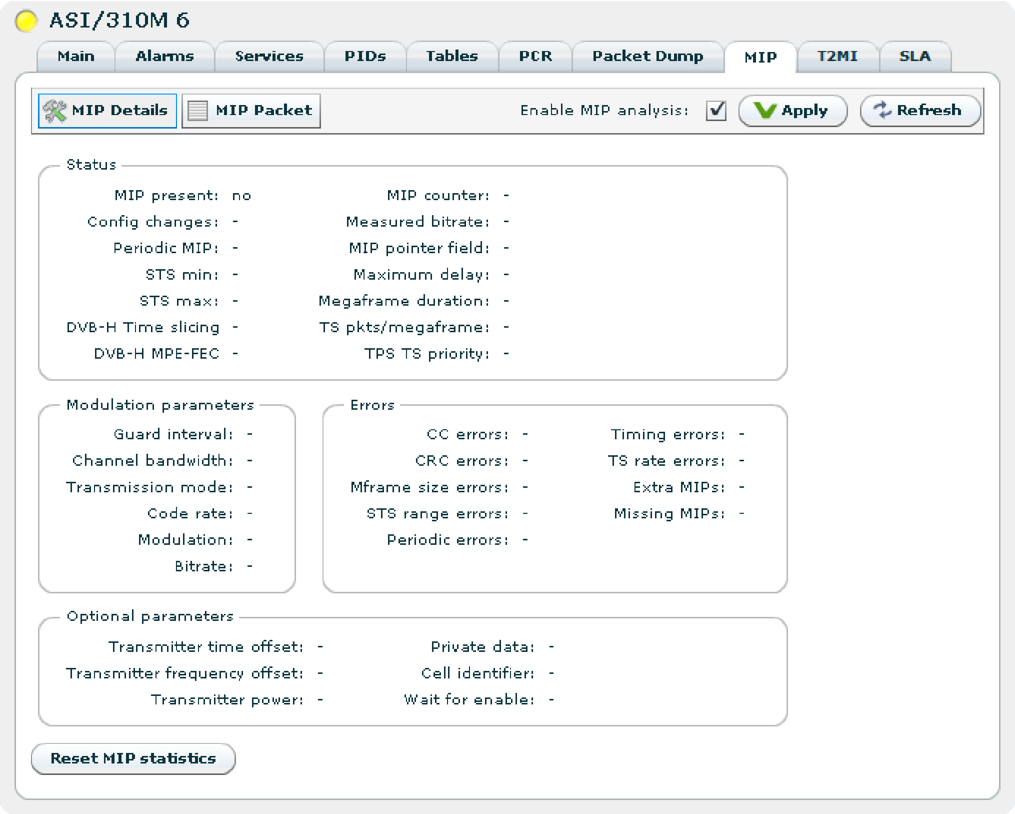
Config changes
The number of configuration changes reported by the transmitter of the MIP packets.

Periodic MIP
This shows whether the time between MIP packets is constant.

Maximum delay
The maximum delay as configured by the transmitter.

STS min
The minimum STS measured.

STS max
The maximum STS measured.



Enable MIP analysis: ☑

Status

MIP present: no
Config changes: -
Periodic MIP: -
STS min: -
STS max: -
DVB-H Time slicing -
DVB-H MPE-FEC -
MIP counter: -
Measured bitrate: -
MIP pointer field: -
Maximum delay: -
Megaframe duration: -
TS pkts/megaframe: -
TPS TS priority: -

Modulation parameters

Guard interval: -
Channel bandwidth: -
Transmission mode: -
Code rate: -
Modulation: -
Bitrate: -

Errors

CC errors: -
CRC errors: -
Mframe size errors: -
STS range errors: -
Periodic errors: -
Timing errors: -
TS rate errors: -
Extra MIPs: -
Missing MIPs: -

Optional parameters

Transmitter time offset: -
Transmitter frequency offset: -
Transmitter power: -
Private data: -
Cell identifier: -
Wait for enable: -

Figure 9.96 MIP Details

DVB-H Time slicing
: Indicates if time slicing is used. Applies to DVB-H transport streams, only.

DVB-H MPE-FEC
: Indicates if MPE-Forward Error Correction is used. Applies to DVB-H transport streams, only.

MIP counter
: The number of MIP packets received.

Measured bitrate
: The measured bitrate of the stream.

MIP pointer field
: This indicates the position of the MIP packet in the megaframe.

Megaframe duration
: The duration of a single megaframe.

TS pkts/megaframe
: The number of transport stream packets that fit in a single megaframe.

TPS TS priority
: In a hierarchically modulated transmission the TS priority may be 1 or 2. Value 1 indicates a high priority transport stream, value 2 means a low priority stream.

The Modulation parameters section shows the modulation parameters that have been set by the transmitter of the transport stream. The parameters are as follows:

Guard interval
: The modulation symbol guard interval to use.

Channel bandwidth
: The bandwidth to use for this channel.

Transmission mode
: The transmission mode to use, i.e. the number of carriers per symbol.

Code rate
: The code rate to use. Values from 1/2 to 7/8 are possible.

Modulation
: The modulation scheme (OFDM constellation) to use for this output.

Bitrate
: The bitrate resulting from the modulation parameter settings.

The Errors section shows the counters for several alarms related to the MIP packets:

CC errors
: The number of Continuity Count errors on the MIP packets since the last MIP statistics reset.

CRC errors
: The number of checksum errors in the MIP packets since the last MIP statistics reset.

Mframe size errors
: The number of megaframes received, with incorrect size.

STS range errors
: The number of STS range errors since the last MIP statistics reset.

Periodic errors
: The number of periodic errors since the last MIP statistics reset.

Timing errors
: The number of timing errors since the last MIP statistics reset.

TS rate errors
: The number of transport stream rate errors since the last MIP statistics reset.

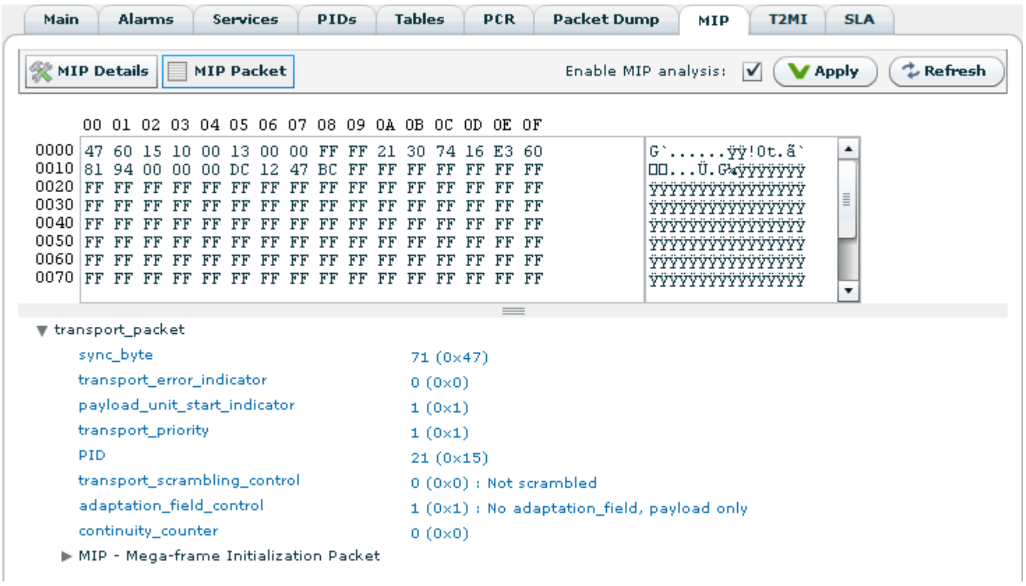
Extra MIPs
: The number of extra MIP packets since the last MIP statistics reset.

Missing MIPs
: The number of missing MIP packets since the last MIP statistics reset.

At the bottom of the page is a button that allows you to reset all the counters that are shown in the MIP Details page.

9.5.2.11.2 MIP Packet

The MIP Packet view presents a listing of the MIP packet contents.



Enable MIP analysis: ☑

```
     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000 47 60 15 10 00 13 00 00 FF FF 21 30 74 16 E3 60   G`......ÿÿ!0t.ã`
0010 81 94 00 00 00 DC 12 47 BC FF FF FF FF FF FF FF   □□...Ü.G¼ÿÿÿÿÿÿÿ
0020 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0030 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0040 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0050 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0060 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0070 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

```
▼ transport_packet
    sync_byte                         71 (0x47)
    transport_error_indicator         0 (0x0)
    payload_unit_start_indicator      1 (0x1)
    transport_priority                1 (0x1)
    PID                               21 (0x15)
    transport_scrambling_control      0 (0x0) : Not scrambled
    adaptation_field_control          1 (0x1) : No adaptation_field, payload only
    continuity_counter                0 (0x0)
  ▶ MIP - Mega-frame Initialization Packet
```

Figure 9.97 MIP Packet dump

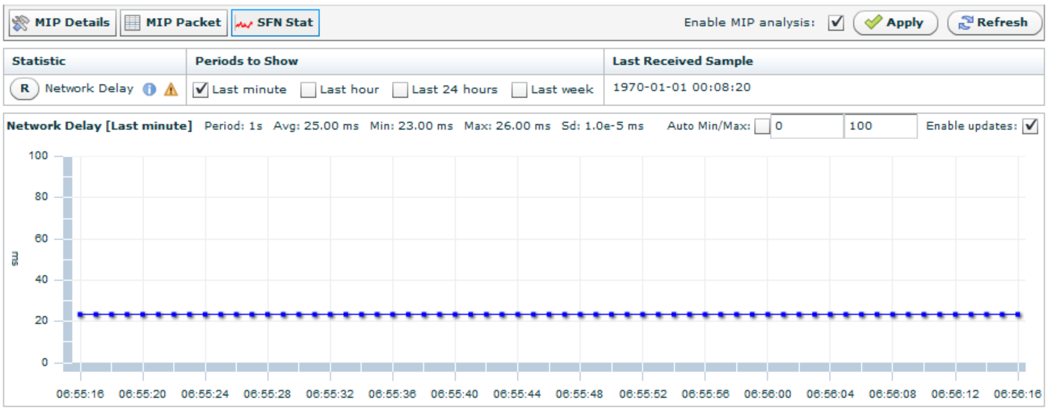
Clicking the Refresh button at the bottom of the page will initiate a dump of the next MIP packet occuring in the selected transport stream. The listing shows the raw data of the packet byte by byte. At the bottom is shown a decoded view of the packet Transport Stream header. The remaining parts of the packet may be decoded by clicking on the arrows to the left.

If no MIP packet is present in the stream an alert appers at the top of the page. Any data present in the packet dump field then has no relevance.

9.5.2.11.3 SFN Stat

The SFN stat page measures the Network Delay since the SFN adapter. The Network delay is the number of milliseconds passed since the MIP was first inserted in the stream by the SFN adapter. This measurement requires that an external PPS is connected. This external PPS must be locked to that of the SFN adapter. There are configurable alarms that may be triggered if the Network delay goes above or below a configured value. If the measured Network Delay is increasing or decreasing over time, either the TNS546 or the SFN adapter has lost its external PPS reference.

Subtracting the Network Delay from the Maximum delay (Found on the MIP Details page) gives the remaining time until the signal should be transmitted on air.



Enable MIP analysis: ☑

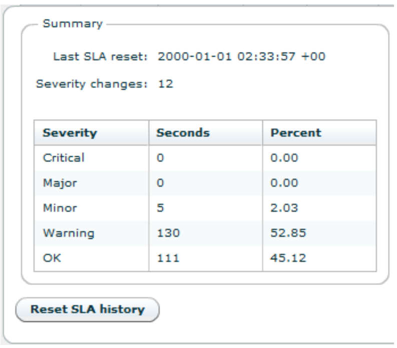
Statistic	Periods to Show	Last Received Sample
R Network Delay	☑ Last minute ☐ Last hour ☐ Last 24 hours ☐ Last week	1970-01-01 00:08:20

Network Delay [Last minute] Period: 1s Avg: 25.00 ms Min: 23.00 ms Max: 26.00 ms Sd: 1.0e-5 ms Auto Min/Max: ☐ 0 100 Enable updates: ☑

Figure 9.98 MIP SFN Stat

9.5.2.12 SLA

The SLA monitor page is shown in figure 9.99



Summary

Last SLA reset: 2000-01-01 02:33:57 +00

Severity changes: 12

Severity	Seconds	Percent
Critical	0	0.00
Major	0	0.00
Minor	5	2.03
Warning	130	52.85
OK	111	45.12

Figure 9.99 SLA Monitor

The Service Level Agreement page shows historical information about the status of the unit's inputs.

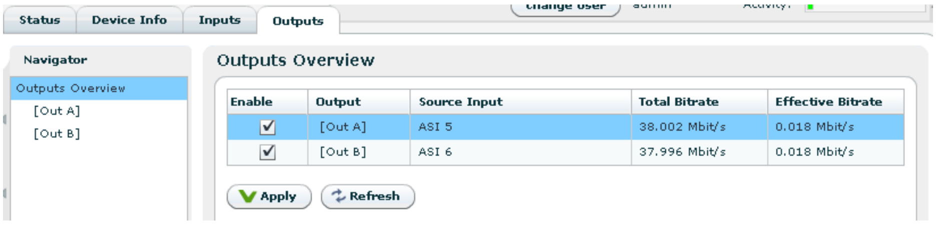
At the top you can see the last time the SLA history was reset. Below is the number of severity changes that has occured since the last SLA history reset. At the bottom is a table that shows the time the input has been in the five different alarm states since the last SLA history reset. The first column shows the severity in question. The second column shows the total number of seconds the unit has been in this state. The last column shows the percentage of the total time that the unit has been in this state. The alarm level notification is counted as OK.

Below the summary box is a button that allows you to reset the SLA history.

9.6 Outputs

This 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 of the device.

9.6.1 Outputs Overview



Outputs Overview

Enable	Output	Source Input	Total Bitrate	Effective Bitrate
☑	[Out A]	ASI 5	38.002 Mbit/s	0.018 Mbit/s
☑	[Out B]	ASI 6	37.996 Mbit/s	0.018 Mbit/s

Figure 9.100 Outputs Overview

This page shows a short summary of all the TS outputs of the device. The table has the following columns:

Enable
: This shows whether the output is enabled or not. The output signal may be enabled or disabled for a port by clicking this check box and hitting apply.

Output
: The name of the output which is the user defined name, see below.

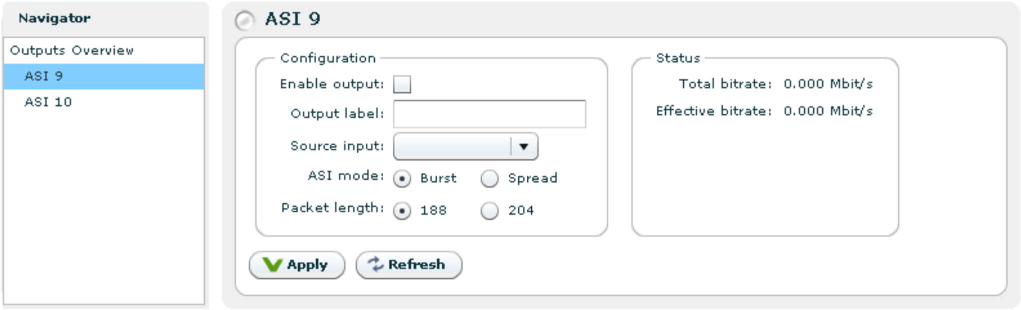
Source input
: The name of the port which transport stream is being transferred to the output.

Total Bitrate
: The total bitrate of the transport stream currently transmitted on the output in Mbit/s.

Effective Bitrate
: The effective bitrate (excluding null packets) of the transport stream currently transmitted on the output in Mbit/s.

9.6.2 Output

When selecting an output a new page is displayed on the right hand side with information about the selected output, see figure Figure 9.101.



ASI 9

Enable output: ☐

Output label:

Source input: ▼

ASI mode: ● Burst ○ Spread

Packet length: ● 188 ○ 204

Total bitrate: 0.000 Mbit/s

Effective bitrate: 0.000 Mbit/s

Figure 9.101 Output settings

The *Configuration* field provides the following options:

Enable output
: Check this box to enable the output signal

Output label
: The user can define a name for the ouput port

Source input
: From this pull down list select the input signal to route to the output port

ASI mode
: Click one of the radio buttons to select if the packets shall appear in bursts or evenly spread in the output transport stream

Packet length
: Click one of the radio buttons to select the output packet length

The *Status* field provides the measured output bit rate:

Total bitrate
: Total output bitrate

Effective bitrate
: Bitrate of that part of the transport stream that carries information. I.e. null packets are not counted.

10 SNMP

The product supports SNMP – Simple Network Management Protocol – for remote control and supervision. 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.

10.1 SNMP agent characteristics

The SNMP agent supports the SNMPv2c (Community based SNMPv2) protocol. All custom MIBS are written in SMIv2 format. The SNMP agent will accept both SNMPv1 and SNMPv2 messages. The SNMP agent uses the normal UDP sockets for communication and listens for requests at UDP port 161.

Both legacy SNMPv1 traps and SNMPv2 notifications are supported. It is however recommended to use the new SNMPv2 notification types for new deployments.

10.2 MIB naming conventions

All custom MIB files start with the prefix `VIGW`. MIBs that defines data structures that are not connected to one specific product start with `VIGW-PLAT`. Most MIBs are of generic type and therefore starts with this prefix.

Some MIB-files are very custom and corresponds to a specific product only. These MIBs start stats with the prefix `VIGW-PROD`.

From Nevion you will receive a set of MIB files. There may be more MIB files than the TNS546 support, but the relevant MIB files are listed here.

10.3 MIB overview

This section describes the different MIBs. Detailed description of MIBs is included later on in this document.

10.3.1 Supported standard MIBs

RFC1213-MIB

MIB-II according to RFC1213.

10.3.2 Custom MIBs

VIGW-TC-MIB

Describes common textual conventions (data types etc.) used throughout the entire MIB set. For example, definition of alarm status numbers are defined in this MIB.

VIGW-BASE-MIB

Defines the top level MIB structure including the enterprise specific root node for device control (1.3.6.1.4.1.22909).

VIGW-UNIT-MIB

This is a generic MIB module that defines parameters supported by all products. It is the main source for alarm and status related information. The following objects are examples of contents in this MIB:

- Top level alarm status
- Table of current alarms
- History of last transmitted TRAP messages
- Trap destination list
- Force reset of the unit
- TRAP/NOTIFICATION definitions
- Other, general product information:
  - Serial number
  - SW version

Note: When setting values in the unitAddressTable it is important to send all values for one interface in the same request. This is to prevent the unit from entering an undefined intermediate state.

VIGW-PLAT-TS-MIB

This MIB contains Transport Stream related information for each of the transport stream inputs. It is supported by transport stream related products that are able to analyse incoming transport streams. For each input transport stream, the following information is available:

- Transport stream sync status and total/effective bitrate.
- Present PIDs with information about bit rates and CC errors.
- Present services with information about service name and service ID.

VIGW-PLAT-TSOUT-MIB

This MIB is supported by products that can generate an outgoing transport stream. Parameters include:

- Control of output bitrate and other ASI parameters (spread/burst mode).
- Control of MIP insertion (if enabled in the product)
  - OFDM modulation parameters

  - Enable/disable of MIP insertion

- Control of PSI/SI/PSIP table playout

VIGW-PLAT-T2MI-MON-MIB

This MIB contains configuration of the T2-MI Analysis module, and read out of the T2-MI Analysis status. Parameters include:

- Enable/disable analysis and configure T2-MI PID.

- Read T2-Frame parameters and PLP configuration

10.4 SNMP related configuration settings

The SNMP related configuration parameters are located on the Device Info/SNMP settings page in the GUI.

10.4.1 Community strings

The community strings are used to provide simple password protection for SNMP read and write requests. The strings can be configured from the GUI. It is also possible to configure the community strings to be used for trap messages.

10.4.2 Trap destination table

The Trap Destination table lets the user configure the external entities that should receive SNMP traps from the device. The table is both accessible via `VIGW-UNIT-MIB` and the product GUI (Device Info/SNMP settings). A maximum of 8 different destinations are supported.

10.4.3 Trap configuration

All supported traps are currently defined in the `VIGW-UNIT-MIB`. Via the GUI you can control the trap forwarding. For detailed information about each trap and the corresponding variable bindings, please see **Section 10.5**.

Trap version

This parameter controls the TRAPs that will be sent from the device in case of alarm conditions.

SNMPv1 (Legacy)

If this option is selected, the unit will send the traps located under the `vigwLegacyTraps` MIB node. These traps are included mostly for historical reasons and it is not recommended to use these for new deployments.

SNMPv2

This is the recommended setting. The traps defined under the node `unitNotifications` will be used while the traps under the node `vigwLegacyTraps` will be disabled.

Status change traps

If enabled, the unit will transmit unitAlarmStatusChanged traps whenever the top level alarm status is changed for the unit.

Alarm event forwarding

This setting controls how internal alarm event will be forwarded as TRAP messages. Adjust this value if you want to control the number of traps sent from the unit. The settings are only used when SNMPv2 is selected as TRAP version. The settings are:

Disabled

No specific event traps are transmitted when alarms are raised or cleared. (The unitAlarmStatusChanged trap may however be transmitted).

Basic

The device forwards alarms as traps on a basic level. No information about subid3 will be transmitted.

Detailed

The device forwards alarms as traps. If there are sub-entries that are using the subid3 value, each sub.entry will be transmitted in separate trap messages.

10.5 Alarm/status related SNMP TRAPs

All TRAP messages are defined in VIGW-UNIT-MIB. This section describes each trap message.

10.5.1 The main trap messages

The main (SNMPv2) trap messages are defined under the unitNotifications node in VIGW-UNIT-MIB. The messages are described briefly in **Table 10.1**.

Table 10.1 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.

10.5.2 Severity indications

All alarm event traps (i.e. all traps defined in **Table 10.1** except `unitAlarmStatusChanged`) contain a severity field which is encoded according to the definition below:

Severity	Description
1	Cleared
2	Indeterminate
3	Warning
4	Minor
5	Major
6	Critical

10.5.3 Alarm event fields

A description of the fields in the alarm event traps is presented in **Table 10.2**. 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 10.2.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.
`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.

Table 10.2.b Variables in SNMPv2 traps and their meanings

Field	Description
`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.
`unitAlarmStatus`	This variable contains the new, top level alarm status of the unit *after* the condition leading to this trap messsage. It may be used to quickly update the top level status for the device after receiving the trap message.

10.5.4 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.

10.5.5 Legacy trap messages

Note: The information in this section relates to trap definitions that are marked as deprecated in `VIGW-UNIT-MIB`. They are included for backwards compatibility with earlier product versions and should not be used for new deployments.

The legacy traps are defined under the `vigwLegacyTraps` node. Transmission of these traps is specified by selecting "SNMPv1 (Legacy)" for the trap version field. The format of these traps follow the SNMPv1 trap format.

In contrast to the SNMPv2 alarm messages, the SNMPv1 messages has its severity implicitly encoded in the trap type.

The trap messages are defined in **Table 10.3**.

Table 10.3 List of legacy (SNMPv1) traps

`alarmCleared`	This trap is sent when an alarm goes off (i.e. is cleared) in the system. The binding `unitTrapHistoryRefNumber` matches the corresponding `unitTrapHistoryRefNumber` in the "raise" trap message.
`alarmIndeterminate`	This trap is sent when an alarm with severity level "notification" (level 2) is generated.
`alarmWarning`	This trap is sent when an alarm with severity level "warning" is generated.
`alarmMinor`	This trap is sent when an alarm with severity level "minor" is generated.
`alarmMajor`	This trap is sent when an alarm with severity level "major" is generated.
`alarmCritical`	This trap is sent when an alarm with severity level "critical" is generated.

All these trap messages contain variable bindings from the `unitTrapHistoryTable`. This table is filled up with historical trap messages, only when SNMPv1 mode is selected.

The fields in these traps are fetched from the `unitAlarmTrapHistoryTable`. The meaning of these fields correspond to the fields in the `unitEventHistoryTable` for SNMPv2 traps and are not described in more detail here.

10.6 Using net-snmp to access MIB information

Net-SNMP is a useful collection of free command line tools that can be downloaded from http://www.net-snmp.org/. The WEB site provides installation packages for several operating systems, including Windows.

The most important tools that can be utilized in scripts etc. is `snmpget` for get operations and `snmpset` for set operations.

The WEB site and the tools provides extensive usage information. We do however present some examples in this chapter for convenience.

10.6.1 Reading a parameter with snmpget

The command line tool to read an SNMP parameter is `snmpget`. The following example shows how the command is used to read system up time from a device:

```
snmpget -v 2c -c public <ip-address> sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (250792000) 29 days, 0:38:40.00
```

Note the following parameters used:

`-v 2c`
This indicates that the version to be used is 2c. This is important as the default value is 3, which is currently not supported.

`-c public`
This is the community string (password) used for the request. It should match the configured SNMP agent settings. The default value is "public".

`<ip-address>`
This is the IP address for the device to read from.

`sysUpTime.0`
: This is the OID for the parameter to read. Since we read a scalar value, we need to add `.0` to the OID from the MIB. Note that it is legal to use a numerical OID in this list; the OID must match the parameter definition in the MIB file.

10.6.2 Writing a parameter with snmpset

The command line tool to set an SNMP parameter is `snmpset`. The following example shows how the command is used to change the system name (`sysName`) for a device:

```
snmpset -v 2c -c private <ip-address> sysName.0 s "New name"
SNMPv2-MIB::sysName.0 = STRING: Siggens
```

Note the following parameters used:

`-v 2c`
: This indicates that the version to be used is 2c. This is important as the default value is 3, which is currently not supported.

`-c private`
: This is the community string (password) used for the request. It should match the configured SNMP agent settings. The default value for write access is “private”.

`<ip-address>`
: This is the IP address for the device.

`sysName.0`
: This is the OID for the parameter to change. Since we read a scalar value, we need to add `.0` to the OID from the MIB. Note that it is legal to use a numerical OID in this list; the OID must match the parameter definition in the MIB file.

`s "New name"`
: This is the parameter type and value. We use “s” to indicate a string and “New name” is the actual string value. The type should match the type defined in the MIB file.

11 Examples of Use

11.1 Intro

This chapter offers a small selection of different practical examples of use of the TNS546, with corresponding recommended configuration steps, pointing to section in **Chapter 9** where the relevant configuration pages are described.

11.2 Installation in a system

When installing the device in a new environment, there are a few parameters that typically need to be configured. These steps are the same for all the cases studied below.

1. Set the IP address as described in section **8.3**
2. Assign a name for the device. See section **9.4.1**.
3. If you are unsure of the state of the device, set it back to factory default configuration as described in section **9.4.8.1**.
4. Configure a time zone and a source for the real time clock, to assure alarm log entries get correct time stamping. See section **9.4.3**.
5. Configure the alarm settings you wish to use for the inputs. See section **9.5.2.2**.

12 Preventive Maintenance and Fault-finding

This chapter provides the schedules and instructions, where applicable, for routine inspection, cleaning and maintenance of the TNS546, to be carried out by the operator of the unit.

12.1 Preventive maintenance

12.1.1 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.

12.1.2 Cleaning

- Remove power from the unit.
- Clean the external surfaces of the TNS546 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.

12.1.3 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

12.1.4 Warranty

The TNS546 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.

12.2 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.

12.2.1 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.

12.2.2 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 TNS546 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 TNS546. Call a Service Engineer.

     No
     : The problem lies with the cable. Replace the cable.

The PSU does not have any internal user changeable fuses.

12.2.3 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.

12.3 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.

12.4 Returning the unit

Before shipping the TNS546 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 TNS546.
   - Name and address of the owner
   - Model number
   - Serial number
   - Description of service required or failure indication.
2. Package the TNS546.
   - 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 Technical Specification

A.1 Physical details

A.1.1 Half-width version

Height	43 mm, 1U
Width	222 mm excluding fixing brackets. Two units may be sideways mounted behind a common front panel
Overall width	485 mm including fixing brackets
Depth	320 mm excluding connectors
Overall depth	340 mm including connectors
Approximate weight	2.5 kg
Rack-mount case	19 inch width, 1 U height

A.1.2 Full-width (dual power) version

Height	43 mm, 1U
Width	444 mm excluding fixing brackets
Overall width	485 mm including fixing brackets
Depth	320 mm excluding connectors
Overall depth	340 mm including connectors
Approximate weight	5 kg
Rack-mount case	19 inch width, 1 U height

A.2 Environmental conditions

Table A.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

A.3 Power

A.3.1 AC Mains supply

Table A.2 AC Power Supply Specification

Rated voltage	100-240 VAC
Voltage tolerance limits	85-264 VAC
Rated frequency	50/60 Hz
Rated current	0.7 A
Power consumption	< 50 W

A.3.2 DC supply

Table A.3 DC Power Supply Specification

Rated voltage	48 VDC
Voltage tolerance limits	36-72 VDC
Power consumption	< 60 W

Table A.4 Physical details

Pin	Placement	Specification
1	top	+ (positive terminal)
2	middle	- (negative terminal)
3	bottom	Chassis Ground

A.4 Input/output ports

A.4.1 DVB ASI port

Table A.5 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

A.4.2 SMPTE 310M port

Table A.6 SMPTE 310M Port Specification

Type	SMPTE 310M, Coaxial cable
Connector type	BNC 75 Ω socket
Signal	Compliant with SMPTE 310M-2004
Data rate	19,392658 Mbit/s
Packet length	188 bytes
Max cable length (Belden 8281 type)	300 m typical

A.4.3 Ethernet management port

Table A.7 Ethernet Management Port Specification

Type	10/100Base-T
Connector type	RJ45

A.4.4 Ethernet data port

Table A.8 Ethernet Data Port Specification

Type	10/100/1000Base-T
Connector type	RJ45

Table A.9 Optional SFP Ethernet Data Port Specification

Type	Gigabit Ethernet
Connector type	Small Form-Factor Pluggable (SFP) slot to carry copper or optical SFP, compatible with approved modules conforming to the Small Form-factor Pluggable Transceiver Multi Source agreements (Sept. 14, 2000).

A.4.5 Serial USB interface

Table A.10 USB port specification

Type	USB 1.1
Compatibility	Compatible with USB 2.0
Connector type	Mini USB Connector

A.5 Alarm ports

A.5.1 Alarm relay/reset port specification

Table A.11 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 A.12 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

A.6 External reference

A.6.1 10MHz/1 PPS input

Connector type	BNC 50 Ω socket

A.7 Compliance

A.7.1 Safety

The equipment has been designed to meet the following safety requirements: **Table A.13**.

Table A.13 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.

A.7.2 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.

A.7.3 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.

A.7.4 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 B 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.

B.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.

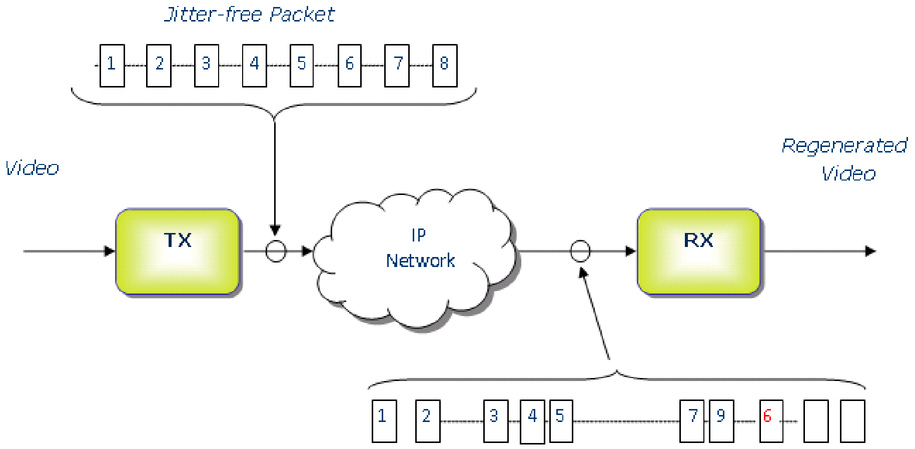


Figure B.1 Impairments of an IP packet stream

In **Figure B.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.

B.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 [14] and 2022-2 [13]. SMPTE 2022-1 focuses on improving IP packet loss ratio (PLR) performance using forward error correction techniques.

B.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.

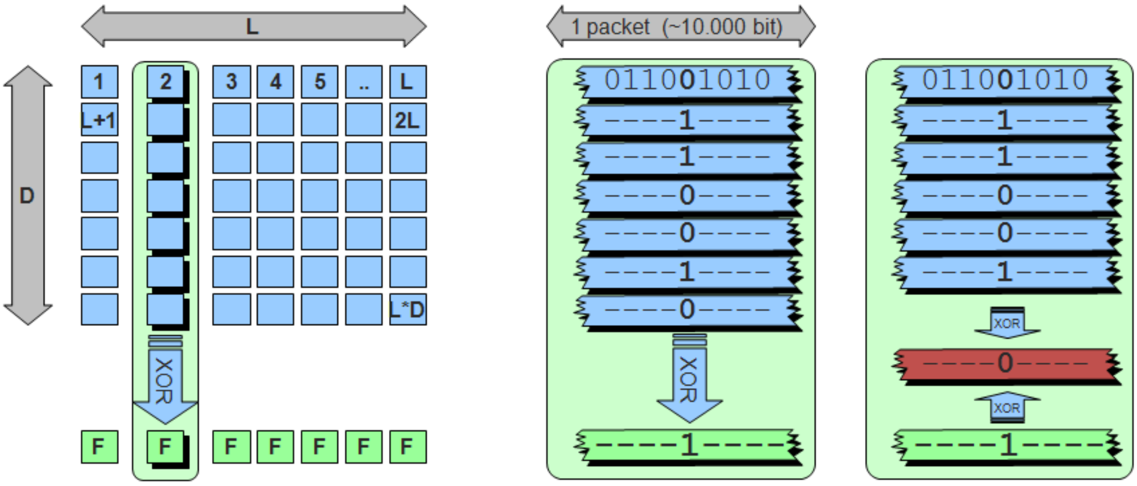


Figure B.2 IP packet FEC calculation matrix

Figure B.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 B.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.

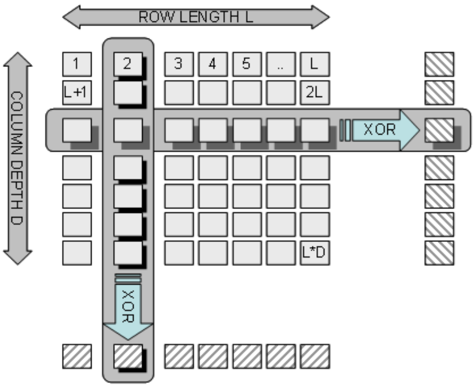


Figure B.3 Two-dimensional FEC calculation matrix

Figure B.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 [14] 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 B.4, which also provides additional advantages.

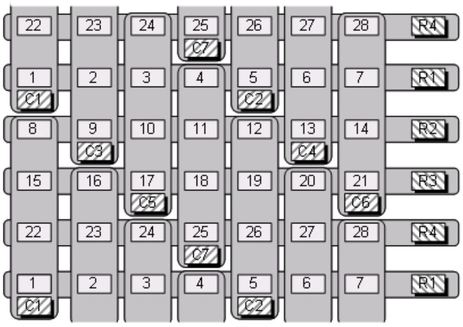


Figure B.4 FEC matrix with column offset

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.

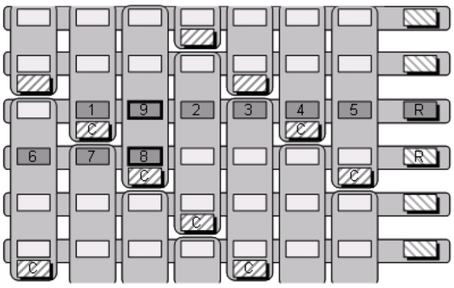


Figure B.5 Offset FEC matrix with missing packets

Figure B.5 shows an offset matrix with missing packets. The numbered items indicats 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 B.6 shows this.

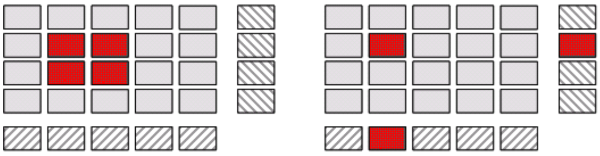


Figure B.6 Uncorrectable error patterns

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.

B.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 B.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.

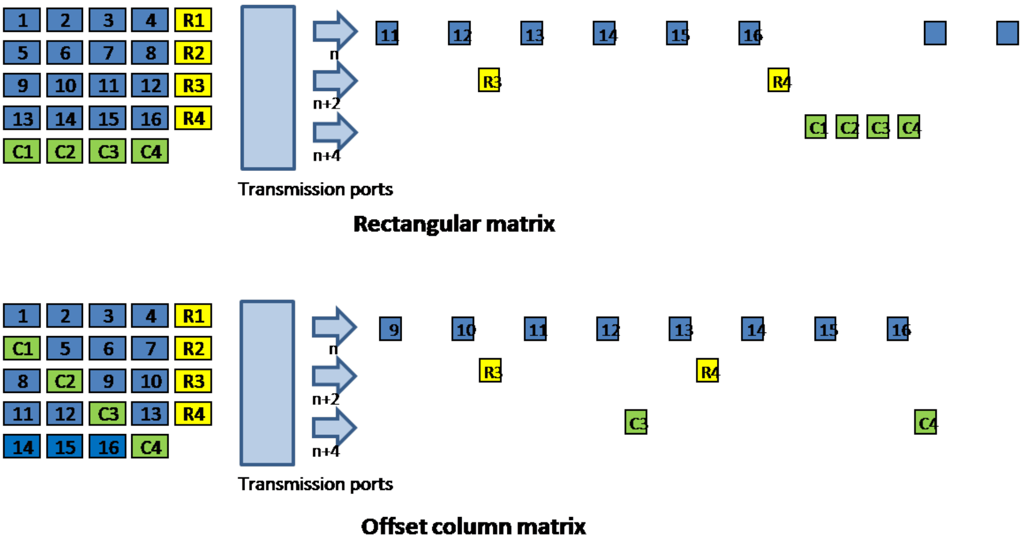


Figure B.7 FEC data transmission

B.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.

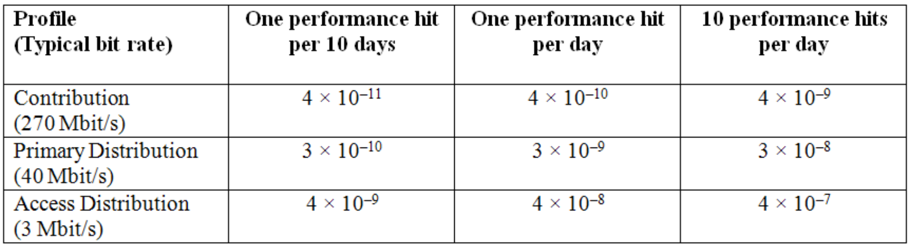
There are three main factors that cause packet loss:

- 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 x 10^{-6}, but occasionally a link may become degraded showing PLR figures like 3 x 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 B.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 [15]. 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 B.8 Recommended error performance (as per ITU)

B.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 B.9** shows how the depth of a one-dimensional FEC matrix affects the error correcting capability.

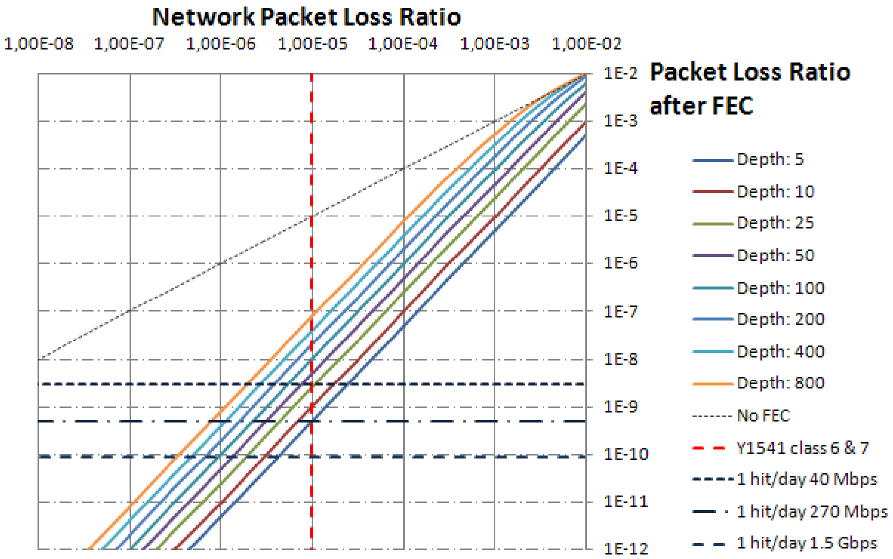


Figure B.9 Error improvement using column FEC only

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 that 10 hits per day (i.e. packet loss rate of 4x10^{-7}, as recommended in Figure B.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.

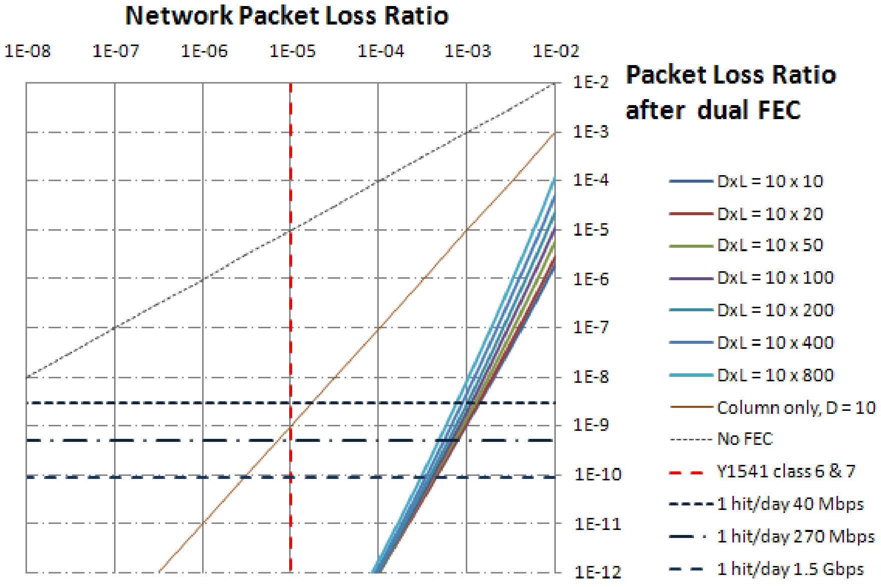


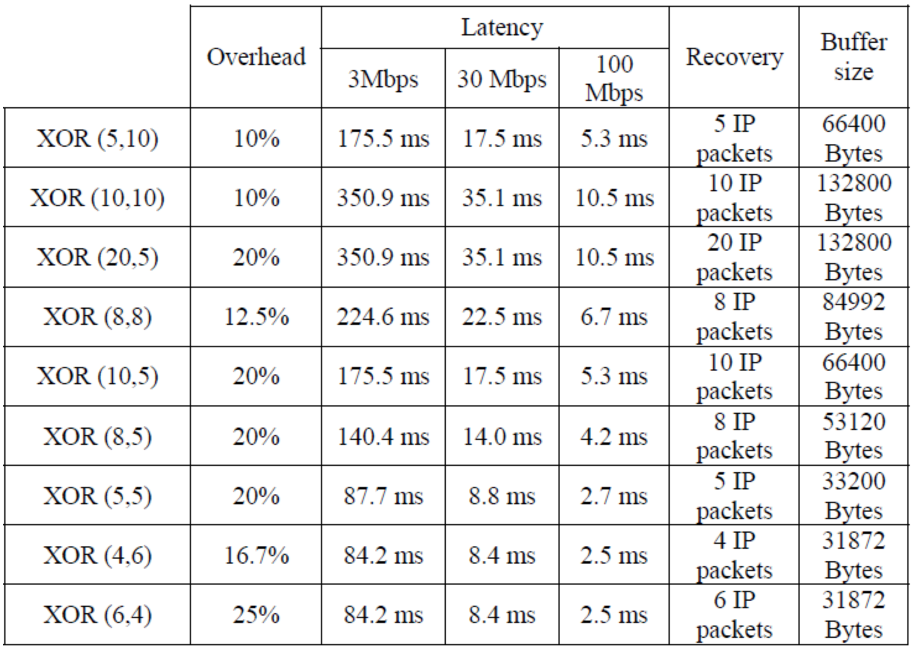
Figure B.10 Error improvement using two-dimensional FEC

Figure B.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 unneccessary FEC overhead.

B.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 B.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 B.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 B.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 C Alarms

The TNS546 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 C.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 C.3 shows the possible alarms that can be signalled by the TNS546. For each alarm type, essential information is presented. The different fields are described in Table C.2.

Table C.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 C.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”
107	Output parameter conflict	Critical	*Description:* *Type:* Port *Clear event:* Yes *Subid3:* “IP Dest”
108	Destination hostname unresolved	Warning	*Description:* Unable to DNS resolve hostname specified as destination. *Type:* Port *Clear event:* Yes *Subid3:* “IP Dest”
130	Ethernet link down	Critical	*Description:* No link on Ethernet layer. *Type:* Port *Clear event:* Yes
131	Ethernet output overflow	Critical	*Description:* The total bitrate of the streams to transmit is too high compared to the available ethernet bitrate. *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
134	Ethernet link problem	Critical	*Description:* Problem on the ethernet link *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”
148	No FEC Column received	Major	*Description:* No FEC Column packets received on Ethernet input for stream. If FEC engine enabled it expects to find FEC Column on Data UDP port+2. *Type:* Port *Clear event:* Yes
149	No FEC Row received	Ok	*Description:* No FEC Row packets received on Ethernet input for stream. If FEC engine enabled it expects to find FEC Row on Data UDP port+4. *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

Table C.3.b Alarms

Alarm ID	Text	Def. severity	Details	
151	No data received	Critical	*Description:*	No data received on Ethernet input for stream. See details field on alarm for description.
			Type:	Port
			Clear event:	Yes
153	Ethernet input overflow	Critical	*Description:*	The total bitrate of the IP input streams is too high.
			Type:	Undetermined
			Clear event:	Yes
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
155	No lock	Critical	*Description:*	The incoming packet stream is absent or incompatible with the expected format.
			Type:	Port
			Clear event:	Yes
157	Too low latency for FEC	Warning	*Description:*	The preferred latency is set lower than the latency required to fully utilize the current FEC. Increase Receive buffer size to resolve.
			Type:	Port
			Clear event:	Yes
158	SFN mode config error	Warning	*Description:*	Lock to MIP bitrate mode requires configuration and locking to an external 1PPS source (Device Info-Clock Regulator).
			Type:	Port
			Clear event:	Yes
160	SNTP server unreachable	Warning	*Description:*	The unit is not receiving answers from the SNTP server.
			Type:	System
			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
164	Illegal board configuration detected	Critical	*Description:*	A board configuration that is incompatible with this product has been detected.
			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

Table C.3.c Alarms

Alarm ID	Text	Def. severity	Details
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”
169	Virtual alarm relay activated	Note	*Description:* A virtual alarm relay has been activated. *Type:* System *Clear event:* Yes *Subid3:* “Relay ID”
200	No GPS 1PPS ref. signal	Critical	*Description:* The 1PPS reference signal is lost (The regulator has however not lost synchronization). *Type:* System *Clear event:* Yes
201	Lost GPS 1PPS sync.	Critical	*Description:* The clock synchronization mechanism has been resynchronized due to too large phase error. *Type:* System *Clear event:* Yes
209	GPI pin triggered	Ok	*Description:* GPI alarm has been triggered from pin 9 *Type:* System *Clear event:* Yes
210	Emergency switch active	Note	*Description:* A user has activated the remote emergency switch. *Type:* System *Clear event:* Yes
211	Emergency switch unreachable	Warning	*Description:* The device is not able to communicate with the remote emergency switch. *Type:* System *Clear event:* Yes
212	Emergency switch rule config error	Warning	*Description:* An error has been detected in the configuration of the emergency switch. *Type:* System *Clear event:* Yes
220	Time adjusted for DST	Note	*Description:* Device local time adjusted due to daylight saving. *Type:* System *Clear event:* No
501	User logged in	Note	*Description:* This event is generated when a user logs on to the system. *Type:* System *Clear event:* No

Table C.3.d Alarms

Alarm ID	Text	Def. severity	Details
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
505	Config changed	Note	*Description:* A modification has been made to the configuration of the device. *Type:* System *Clear event:* No
517	Alarm log cleared	Note	*Description:* Alarm log was cleared, user in details *Type:* System *Clear event:* No
518	System is starting up	Critical	*Description:* This alarm is set when the system is starting. Once booted correctly, the alarm is cleared. *Type:* System *Clear event:* Yes
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
526	Action performed	Note	*Description:* Action performed by user. Used to log generic important events, see details field on each alarm event for additional information. *Type:* System *Clear event:* No
527	New SW license pending	Note	*Description:* New SW licenses have been loaded but requires a re-boot to be activated. *Type:* System *Clear event:* Yes
528	New SW license installed	Note	*Description:* New SW licenses have been loaded and installed without requiring reboot. *Type:* System *Clear event:* Yes
535	Alarm log almost full	Note	*Description:* Alarm log almost full, overwrite of older alarms will take place *Type:* System *Clear event:* No

Table C.3.e Alarms

Alarm ID	Text	Def. severity	Details
536	Heartbeat trap	Note	*Description:* Heartbeat to signal the system is still functional *Type:* System *Clear event:* No
1100	Sync unstable	Major	*Description:* Two separate sync-losses in 10s. *Type:* Port *Clear event:* Yes
1101	TS unstable	Minor	*Description:* Lots of PIDs appearing/disappearing or CC errors. *Type:* Port *Clear event:* Yes
1110	No sync	Critical	*Description:* No valid ASI 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

Table C.3.f Alarms

Alarm ID	Text	Def. severity	Details	
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
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 PID Event alarm. See test 1.6 in ETSI TR 101 290 v1.2.1.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
1161	PID event	Ok	*Description:*	This alarm is currently used to configure the time before a PID is assumed to have disappeared. See PID error alarm.
			Type:	Port
			Clear event:	Yes
			Subid3:	"PID"
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"
1221	CRC error on update	Warning	*Description:*	CRC on a table section error occurred in CAT, PAT, PMT, NIT, EIT, BAT, SDT or TOT table. CRC only checked again on table update. 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"

Table C.3.g Alarms

Alarm ID	Text	Def. severity	Details
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"
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"
1250	PTS error	Warning	*Description:* PTS repetition period more than the configured value. ETR290 specifies the limit to 700 ms. See test 2.5 in ETSI TR 101 290 v1.2.1. *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

Table C.3.h Alarms

Alarm ID	Text	Def. severity	Details
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
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

Table C.3.i Alarms

Alarm ID	Text	Def. severity	Details
1359	BAT missing	Warning	*Description:* *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”
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

Table C.3.j Alarms

Alarm ID	Text	Def. severity	Details
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
1524	MIP PID not present	Warning	*Description:* The MIP PID is not present. *Type:* Port *Clear event:* Yes
1525	MIP CRC error	Critical	*Description:* A CRC error has been detected in the MIP. *Type:* Port *Clear event:* Yes
1526	MIP new parameters	Note	*Description:* An update has been detected in the parameters contained in MIP (TPS field or maximum delay field). *Type:* Port *Clear event:* Yes
1527	MIP CC error	Warning	*Description:* TS packet header CC error has been detected on the MIP PID. *Type:* Port *Clear event:* Yes
1528	MIP STS range error	Warning	*Description:* The STS field indicates a value larger than a second. *Type:* Port *Clear event:* Yes
1529	MIP pointer error	Warning	*Description:* The number of TS packets in the megaframe does not match the parameters in MIP. *Type:* Port *Clear event:* Yes
1530	MIP timing error	Warning	*Description:* STS values in consecutive MIPs have wrong timing values. *Type:* Port *Clear event:* Yes
1531	Extra MIP	Warning	*Description:* An extra MIP has been detected within a megaframe. *Type:* Port *Clear event:* Yes
1532	Missing MIP	Warning	*Description:* No MIP is detected. *Type:* Port *Clear event:* Yes

Table C.3.k Alarms

Alarm ID	Text	Def. severity	Details
1533	MIP periodicity error	Warning	*Description:* The MIP periodicity is not correct. *Type:* Port *Clear event:* Yes
1534	MIP ts rate error	Warning	*Description:* The rate of the transport stream does not match the rate signaled in the MIP. *Type:* Port *Clear event:* Yes
1535	MIP network delay too high	Ok	*Description:* Measured Network delay higher than configured maximum delay. Network delay is the time elapsed since the SFN adapter. Important: Both the monitor and the SFN adapter must be locked to the same external reference. *Type:* Port *Clear event:* Yes
1536	MIP network delay too low	Ok	*Description:* Measured Network lower higher than configured maximum delay. Network delay is the time elapsed since the SFN adapter. Important: Both the monitor and the SFN adapter must be locked to the same external reference. *Type:* Port *Clear event:* Yes
1542	MIP size error	Warning	*Description:* There is not enough space in the MIP packet for all configured transmitter function loops. *Type:* Port *Clear event:* Yes
1543	MIP Inserter time reference problem	Warning	*Description:* MIP Inserter time reference problem. *Type:* Port *Clear event:* Yes
1570	T2-MI Packet type error	Warning	*Description:* Error if either L1-Current or T2-Timestamp are missing for one or more T2-Frames. *Type:* Port *Clear event:* Yes
1571	Packet payload error	Warning	*Description:* Error if a BBFrames of a PLP is present in a T2-Frame when it should not, or not present when it should. *Type:* Port *Clear event:* Yes *Subid3:* "PLP"
1572	Payload error	Warning	*Description:* Error if there are any BB frames without their PLP id signaled in L1-Current. *Type:* Port *Clear event:* Yes
1573	PLP num blocks	Warning	*Description:* Error if the number of received BB frame packets does not match the number in the L1-post signalling *Type:* Port *Clear event:* Yes *Subid3:* "PLP"

Table C.3.1 Alarms

Alarm ID	Text	Def. severity	Details
1574	T2-MI Transmission order	Warning	*Description:* Error T2-MI packets come in the wrong order. *Type:* Port *Clear event:* Yes
1575	Timestamp error	Warning	*Description:* Error if at least one T2-Timestamp has a different timestamp than the other T2-Timestamps belonging to the same superframe. *Type:* Port *Clear event:* Yes
1576	Timestamp discontinuity	Warning	*Description:* Error if the timestamp value does not increase by the superframe duration. *Type:* Port *Clear event:* Yes
1577	T2-Frame length	Warning	*Description:* Error if the T2-Frame length derived from L1 parameters are longer than 250 ms. *Type:* Port *Clear event:* Yes
1578	T2-MIP Timestamp	Warning	*Description:* Error if the timestamp of the T2-MIP is lower than the timestamp in the T2-MI Timestamp packet. *Type:* Port *Clear event:* Yes
1579	T2-MIP Ind. Addr.	Warning	*Description:* Error if the Individual Addressing data in the T2-MIP differs from the data in the T2-MI Individual Addressing packet. *Type:* Port *Clear event:* Yes
1580	T2-MIP continuity	Warning	*Description:* Error if a T2-MIP is not present within a T2 superframe. *Type:* Port *Clear event:* Yes
1581	T2-MIP CRC32	Warning	*Description:* Error if the CRC32 field of the T2-MIP does not match the calculated CRC32. *Type:* Port *Clear event:* Yes
1583	Bandwidth consistency	Warning	*Description:* Error if the maximum possible bit rate which is calculated from the T2-MI DVB-T2 Timestamp and the determining L1 parameters is lower than the bit rate of the stream encapsulated in the T2-MI packets *Type:* Port *Clear event:* Yes
1584	Leap second error	Ok	*Description:* Error if leap second value of the T2-Timestamp is not equal to the configured expected value. *Type:* Port *Clear event:* Yes
1590	T2-MI CRC32 Error	Warning	*Description:* Alarm is triggered if the CRC32 field at the end of each T2-MI packet differs from the CRC32 calculated by the unit. *Type:* Port *Clear event:* Yes

Table C.3.m Alarms

Alarm ID	Text	Def. severity	Details	
1591	Superframe Index	Warning	*Description:*	Alarm is triggered if the T2 superframe indedoes not increase by 1 between successive T2 superframes.
			Type:	Port
			Clear event:	Yes
1592	T2-MI Packet Count	Warning	*Description:*	Alarm is triggered if the T2-MI Packet Count variable does not increase by 1 from one T2-MI packet to the next.
			Type:	Port
			Clear event:	Yes
1593	T2-MI Unpacking Error	Warning	*Description:*	Alarm is triggered if the unit has problems unpacking the T2-MI stream from the outer Transport Stream. This will for example occur if one TS packet is lost or the T2-MI length field is not correct.
			Type:	Port
			Clear event:	Yes
1594	No T2-MI stream	Warning	*Description:*	T2-MI data can not be found on the given T2-MI PID.
			Type:	Port
			Clear event:	Yes
1595	SFN delay too high	Ok	*Description:*	Measured SFN delay higher than configured maximum delay. SFN delay is the time until the signal should be transmitted on air. Important: Both the monitor and the T2-Gateway must be locked to the same external reference.
			Type:	Port
			Clear event:	Yes
1596	SFN delay too low	Ok	*Description:*	Measured SFN delay lower than configured minimum delay. SFN delay is the time until the signal should be transmitted on air. Important: Both the monitor and the T2-Gateway must be locked to the same external reference.
			Type:	Port
			Clear event:	Yes
1597	Frame Index	Warning	*Description:*	Alarm is triggered if the T2-Frame Indechanges abnormally.
			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”

Table C.3.n Alarms

Alarm ID	Text	Def. severity	Details	
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"
1805	Service missing	Ok	*Description:*	A service is missing from the stream (according to configured expected value)
			Type:	Port
			Clear event:	Yes
			Subid3:	"Service"
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"
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
			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"

Table C.3.o Alarms

Alarm ID	Text	Def. severity	Details
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"
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

Table C.3.p Alarms

Alarm ID	Text	Def. severity	Details
2113	CVCT scrambled	Warning	*Description:* See ATSC Recommended Practice A/78. *Type:* Port *Clear event:* Yes
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

Table C.3.q Alarms

Alarm ID	Text	Def. severity	Details
2133	EIT-1 missing	Warning	*Description:* See ATSC Recommended Practice A/78. *Type:* Port *Clear event:* Yes *Subid3:* "Source-ID"
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
3500	Arm time violation	Warning	*Description:* Scte35 command received but may be ignored by the splicing device due to arm time violation. *Type:* Port *Clear event:* Yes *Subid3:* "SID"
3501	Immediate command received	Note	*Description:* Scte35 immediate command received. *Type:* Port *Clear event:* Yes *Subid3:* "SID"
3502	Command without timing information	Warning	*Description:* Scte35 command without any valid timing information. *Type:* Port *Clear event:* Yes *Subid3:* "SID"
3503	Heartbeat miss	Warning	*Description:* Heartbeat miss (scte35_null_command). *Type:* Port *Clear event:* Yes *Subid3:* "SID"

Table C.3.r Alarms

Alarm ID	Text	Def. severity	Details
3504	Command not allowed	Warning	*Description:* Command not allowed on this elementary stream. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3505	Too many PIDs	Warning	*Description:* Too many Scte35 PIDs. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3506	No PTS available	Warning	*Description:* No PTS available in this service. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3507	Invalid cue identifier	Warning	*Description:* Invalid scte35 cue identifier descriptor. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3509	Scheduled event not inserted	Warning	*Description:* Scte35 event (scheduled with splice_schedule command) has not been inserted (with splice_insert) before the scheduled time elapsed. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3510	Event updated	Note	*Description:* Scte35 event updated. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3511	Event canceled	Note	*Description:* Scte35 event canceled. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3512	Return from avail message missing	Warning	*Description:* Splice event in expected due to the presence of a duration field in the splice_insert out command, but no splice_insert in command found for the due date. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3513	Bandwith_reservation message flow interrupted	Major	*Description:* Scte35 bandwidth_reservation message flow interrupted. *Type:* Port *Clear event:* Yes *Subid3:* “PID”
3514	CRC/Syntaerror	Warning	*Description:* Scte35 message invalid due to CRC error or an invalid syntax. *Type:* Port *Clear event:* Yes *Subid3:* “PID”

Table C.3.s Alarms

Alarm ID	Text	Def. severity	Details
3600	Service availability error	Critical	*Description:* Service availability class above the limit. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3610	Service degradation error	Warning	*Description:* Service degradation class above the limit. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
3620	Service impairments error	Note	*Description:* Service impairments class above the limit. *Type:* Port *Clear event:* Yes *Subid3:* “SID”
4100	AIT not found	Warning	*Description:* No information received from AIT PID signalled in the PMT *Type:* Port *Clear event:* Yes *Subid3:* “PID”
4101	Component tag not found in AIT	Warning	*Description:* A data carousel component tag signalled in the PMT was not found in the AIT *Type:* Port *Clear event:* Yes *Subid3:* “SID”
4102	Multiple AITs found	Warning	*Description:* Multiple AITs found in a service *Type:* Port *Clear event:* Yes *Subid3:* “SID”
4500	TS Template Error	Warning	*Description:* Discrepancy with the ongoing TS template. *Type:* Port *Clear event:* Yes *Subid3:* “TPL”
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 D 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]
ETSI TR 101 290; Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems

[9]
ETSI TR 101 891; Digital Video Broadcasting (DVB); Professional Interfaces: Guidelines for the implementation and usage of the DVB Asynchronous Serial Interface (ASI)

[10]
EN 50083-9:2002; Part 9: Interfaces for CATV/SMATV headends and similar professional equipment for DVB/MPEG-2 transport streams

[11]
ATSC A/65; Program and System Information Protocol (PSIP) for Terrestrial Broadcast and Cable

[12]
ATSC Recommended Practice; Document A/78A; Transport Stream Verification

[13]
SMPTE 2022-2-2007: Unidirectional Transport of Constant Bit-Rate MPEG-2 Transport Streams on IP Networks

[14]
SMPTE 2022-1-2007: Forward Error Correction for Real-time Video/Audio Transport over IP Networks

[15]
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

[16]
Pro-MPEG Forum: Pro-MPEG Code of Practice #3 release 2, July 2004: Transmission of Professional MPEG-2 Transport Streams over IP Networks

[17]
Pro-MPEG Forum: Pro-MPEG Code of Practice #4 release 1, July 2004: Transmission of High Bit Rate Studio Streams over IP Networks

[18]
J. Rosenberg, H. Schulzrinne, IETF RFC2733, December 1999: An RTP Payload Format for Generic Forward Error Correction

[19]
Digital Video Broadcasting (DVB); Measurement guidelines for DVB systems ETSI TR 101 290 V1.2.1 (2001-05) Paragraph 5.5