

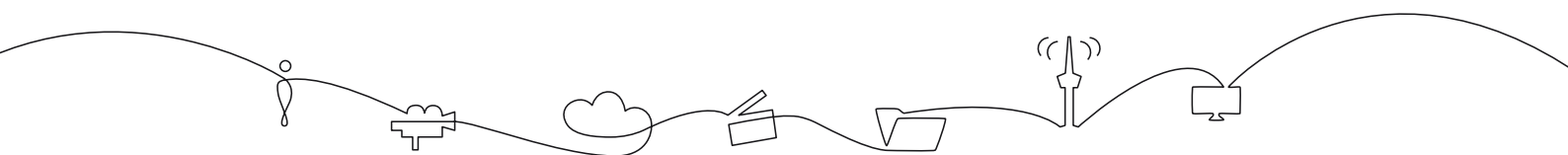
TNS544 TSoIP Switch User's Manual

Revision: 1.4 (3685)

2012-09-03



Valid for SW version 1.4.0 and newer



Contents

1	History	9
2	Introduction	11
2.1	Scope	11
2.2	Warnings, cautions and notes	11
2.3	Heed warnings	12
2.4	Contact information	12
3	Short Product Description	13
3.1	Summary of features	13
3.2	Options	14
3.2.1	Hardware options	14
3.2.2	Software options	15
4	Getting Started	17
4.1	Configure the management interface	17
4.2	Configure device name and time settings	18
4.3	Configure operation	18
4.3.1	Enabling IP inputs	18
4.3.2	Enabling the Switch	19
4.3.3	Enabling IP output	19
5	Installing the Equipment	21
5.1	Inspect the package content	21
5.2	Installation Environment	21
5.3	Equipment installation	22
5.4	Ventilation	22
5.5	Power supply	23
5.5.1	AC power supply	23
5.5.2	Dual AC power supplies	23
5.5.2.1	AC power cable	23
5.5.2.2	Protective Earth/technical Earth	24
5.5.2.3	Connecting to the AC power supply	24
5.5.3	DC power supply	25
5.5.3.1	DC power cable	25
5.5.4	Powering up/down	25
6	Functional Description	27
6.1	Input and output	28
6.1.1	Protocol mapping	29

6.2	Management subsystem	29
6.2.1	Graphical user interface	30
6.2.2	Configuration database	30
6.2.3	Alarm manager	31
6.3	Time synchronisation	31
6.4	The SFP module	32
7	Physical Description	33
7.1	ASI ports	33
7.1.1	ASI input ports	34
7.1.2	ASI output ports	34
7.2	1 PPS Input	34
7.3	Ethernet data ports	35
7.4	Ethernet management port	35
7.5	Power supply	36
7.6	Technical earth	36
7.6.1	Alarm/Reset connector	36
7.6.2	Serial USB interface	37
8	Operating the Equipment	39
8.1	Accessing the graphical user interface	39
8.2	Password protection	39
8.2.1	Resetting the password list	40
8.3	Changing the IP address of the unit	40
8.3.1	Changing IP address via the Web GUI	40
8.3.2	Changing the management port IP address via terminal interface	41
9	WEB Interface	43
9.1	Login	43
9.2	Status header	44
9.3	Status	45
9.3.1	Current Status	45
9.3.2	Alarm log	47
9.4	Device Info	49
9.4.1	Product info	49
9.4.2	Alarms	51
9.4.2.1	Device alarms	52
9.4.2.2	Global configuration	52
9.4.2.3	Relays and LED	53
9.4.2.4	Alarm log settings	55
9.4.3	Time Settings	56
9.4.4	Network	58
9.4.4.1	Interfaces	59
9.4.4.1.1	Main	59

9.4.4.1.2	Alarms	60
9.4.4.1.3	Advanced	61
9.4.4.1.4	Status	61
9.4.4.1.5	VLAN	63
9.4.4.1.6	SFP	64
9.4.4.2	IP Routing	73
9.4.4.3	TXP Settings	74
9.4.4.4	SNMP Settings	75
9.4.4.5	Tools	76
9.4.5	Clock Regulator	78
9.4.5.1	Main	78
9.4.5.2	Alarms	79
9.4.6	Save/Load Config	79
9.4.6.1	Save/Load Configs	79
9.4.6.2	Boot Log	81
9.4.6.3	Stored Configs	81
9.4.7	Maintenance	83
9.4.7.1	General	83
9.4.7.2	Software Upgrade	85
9.4.7.3	Feature Upgrade	86
9.4.8	Users	87
9.4.9	GUI Preferences	88
9.5	Inputs	88
9.5.1	Inputs Overview	88
9.5.1.1	IP Inputs	90
9.5.2	Input	92
9.5.2.1	Main	92
9.5.2.2	Alarms	95
9.5.2.3	IP	100
9.5.2.3.1	FEC	102
9.5.2.3.2	Ping	103
9.5.2.3.3	Regulator	104
9.5.2.4	Services	106
9.5.2.5	PIDs	110
9.5.2.6	Tables	112
9.5.2.7	Tables	113
9.5.2.8	Settings	114
9.5.2.9	Sources	116
9.5.3	Switch	116
9.5.3.1	Main	117
9.5.3.2	Inputs	119
9.5.3.3	Alarms	121
9.6	Outputs	121
9.6.1	Outputs overview	122
9.6.2	(Switch) Output	123
9.6.2.1	Switch Main	123
9.6.2.2	Alarms	125

9.6.3	Output to IP destination	125
9.6.3.1	Main	126
9.6.3.2	FEC	128
9.6.3.3	Ping	130
10	SNMP	133
10.1	SNMP agent characteristics	133
10.2	MIB naming conventions	133
10.3	MIB overview	133
10.3.1	Supported standard MIBs	133
10.3.2	Custom MIBs	133
10.4	SNMP related configuration settings	135
10.4.1	Community strings	135
10.4.2	Trap destination table	136
10.4.3	Trap configuration	136
10.5	Alarm/status related SNMP TRAPs	137
10.5.1	The main trap messages	137
10.5.2	Severity indications	137
10.5.3	Alarm event fields	138
10.5.4	Matching of on/off traps	139
10.5.5	Legacy trap messages	139
11	Preventive Maintenance and Fault-finding	141
11.1	Preventive maintenance	141
11.1.1	Routine inspection	141
11.1.2	Cleaning	141
11.1.3	Servicing	141
11.1.4	Warranty	142
11.2	Fault-finding	142
11.2.1	Preliminary checks	142
11.2.2	PSU LED not lit / power supply problem	143
11.2.3	Fan(s) not working / unit overheating	144
11.3	Disposing of this equipment	144
11.4	Returning the unit	144
A	Glossary	145
B	Technical Specification	151
B.1	Physical details	151
B.1.1	Half-width version	151
B.1.2	Full-width (dual power) version	151
B.2	Environmental conditions	151
B.3	Power	152
B.3.1	AC Mains supply	152
B.3.2	DC supply	152

B.4	Input/output ports	153
B.4.1	DVB ASI port	153
B.4.2	Ethernet management port	153
B.4.3	Ethernet data port	153
B.4.4	Serial USB interface	154
B.5	Alarm ports	154
B.5.1	Alarm relay/reset port specification	154
B.6	External reference	155
B.6.1	10MHz/1 PPS input	155
B.7	Compliance	155
B.7.1	Safety	155
B.7.2	Electromagnetic compatibility - EMC	155
B.7.3	CE marking	156
B.7.4	Interface to "public telecommunication system"	156
C	Forward Error Correction in IP Networks	157
C.1	IP stream distortion	157
C.2	Standardisation	158
C.3	FEC matrix	158
C.4	Transmission aspects	161
C.5	Quality of service and packet loss in IP networks	162
C.6	Error improvement	163
C.7	Latency and overhead	164
D	Quality of Service, Setting Packet Priority	167
D.1	MPLS	167
D.2	Layer 3 routing	167
D.2.1	TNS544 configuration	168
D.3	Layer 2 priority	168
D.3.1	TNS544 configuration	168
E	Alarms	169
F	References	189

1 History

Revision	Date	Comments
1.4	September 2012	– Added description of ASI version
1.2	May 2012	– Initial release

2 Introduction

2.1 Scope

This manual is written for operators and users of the TNS544 TSoIP Switch and provides necessary information for installation, operation and day-to-day maintenance of the unit. The manual covers the functionality of the software version 1.4.0 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@t-vips.com
WEB	www.t-vips.com
Mail and visiting address	T-VIPS AS Nils Hansens vei 2 NO-0667 Oslo Norway

3 Short Product Description

The TNS544 is part of the T-VIPS nSure product line which safeguards the delivery of high-quality video content, by providing 24/7 monitoring and redundancy switching.

The TNS544 provides intelligent redundancy switch-over between MPEG Transport Streams in IP-based video centric networks. It ensures the robust transmission of Transport Streams by continuously monitoring all inputs, switching seamlessly to the back-up stream if errors are detected or services or components are lost.

The TNS544 offers flexible configuration of inputs, number of switches and outputs. It can be delivered with up to four 2:1 or two 4:1 switches in one device. All inputs are monitored simultaneously in each switch. Any delay differences between the inputs are automatically compensated enabling seamless switching without any disturbance to end users. The TNS544 also supports switching between non-identical Transport Streams without having sync loss on the output.

3.1 Summary of features

Features of the TNS544 include:

- Intelligent Transport Stream switching
 - Automatic/manual seamless switching
 - Automatic network delay compensation
 - Fully transparent operation at TS packet level (no PCR restamping or packet re-ordering)
 - Option to ignore Null Packets
- High density and flexible switch configuration
 - Up to 4 independant switches in 1RU half-width 19"
 - Configurable number of inputs per switch (2-4 inputs)
 - Switch inputs may be ASI, IP or any combination of ASI and IP (if equipped with ASI connectors)
 - 4 secured ASI outputs on power loss
 - Output diversity (up to 8 TS over IP outputs per switch and/or up to 4 ASI outputs)
 - Fully configurable alarm based switching criteria
- TS monitoring and error detection
 - Simultaneous monitoring of all input MPEG Transport Streams

- Error detection according to ETSI TR 101 290 specification (priority 1 and Transport_error)
- Content alarms
- Industry-leading support for IP video technologies
 - Two Gigabit Ethernet interfaces for TS over IP
 - IP multicast, unicast and multiple unicast support
 - Optional support for Ethernet over Sonet OC-3 / SDH STM-1
 - IP wrapping of Transport Streams using SMPTE 2022-2
 - Forward Error Correction according to SMPTE 2022-1
 - Support for multiple VLANs (IEEE 802.1Q)
 - TOS/COS field support for traffic prioritisation
- User-friendly configuration and control
 - WEB/XML based remote control
 - SNMP agent for easy integration with NMS systems
 - Integrated with T-VIPS Connect

3.2 Options

The TNS544 is modular and may be equipped according to user requirements. Available hardware and software options are described below.

3.2.1 Hardware options

ASI ports

The TNS544 is fitted with 8 ASI connectors, of which 4 are inputs and 4 are secured outputs. On power loss (or by manual configuration) the outputs are wired to the inputs.

SFP Module

The TNS544 is equipped with an SFP socket. Different types of SFP modules may optionally be delivered to provide optical Gigabit transportation.

Dual power supplies

The TNS544 may optionally be delivered with dual internal wide-ranging AC power supplies. In this case the size of the cabinet is always full-width 1RU. The power supplies cover the voltage range 100-240 VAC, 50/60 Hz.

3.2.2 Software options

The TNS544 functionality depends on the software licences installed. The following table describes the features available as software options. Please refer to [Section 9.4.7.3](#) for more information how to obtain and enable feature upgrades.

Table 3.1 Functionality enabled through software licences

Functionality	Max value	Description
SFP module	-	Enables operation of the Small form-factor pluggable (SFP) transceiver slot.
SFP configuration	-	Enables configuration interface and parameter storage for some specifically supported SFP modules.
Forward Error Correction	-	Controls availability of the FEC feature for IP outputs and IP inputs.
SFN Rate Lock	-	Controls whether the device can use DVB-T MIP timestamps to lock outgoing rate when in IP to ASI mode.
Number of seamless switches	4	Controls the number of active Transport Stream Switching Units.
Connect control	-	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 TNS544.

If you are an experienced user of T-VIPS equipment or similar types of TS switching equipment the following description should enable you to quickly install the TNS544 TSoIP Switch and start operation. If this is your first time to install such equipment you are strongly advised 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 Configure the management interface

Since the TNS544 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, refer to section [8.3.2](#).



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 TNS544. The default IP address of the TNS544 is **10.0.0.10/255.255.255.0**. Configure the PC to be on the same subnet as the TNS544.
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 TNS544 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 Configure device name and time settings

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.

4.3 Configure operation

A TNS544 can be configured with up to 4 switches. A Switch may be sourced from up to 4 inputs, IP and/or ASI, and the output of the Switch may be routed to one or several IP outputs or ASI outputs. Transport streams received on IP are de-encapsulated in to TS packets and the switching occurs on TS level. After switching, the output of the Switch is appropriately encapsulated before being sent to an IP output interface. The TNS544 operation does not distinguish between single program and multi program transport streams.

4.3.1 Enabling IP inputs

This procedure enables an IP input.

1. Browse to Inputs > Inputs Overview > IP Inputs. At the bottom of the page, click the Add IP Input button. Click Apply. An entry for the new input appears in the table, with default values for all parameters.
2. Open the IP input configuration page by clicking on the table entry.
3. In the Main page, IP RX Configuration field, tick the Enable input check box and type an identifying name, e.g. the service name, in the Input label box. Specify the UDP receive port. If the signal to receive is an IP multicast click the Join multicast check box and enter the multicast address in the adjacent field.
4. Select the Ethernet interface from the alternatives in the Source interface pull-down list. Click Apply to activate.
5. The IP RX Status field will indicate if the attached network cable carries a valid signal and the remaining status fields will report the properties and contents of the incoming transport stream.

The coloured indicator at the top of the page shows the overall signal status.

4.3.2 Enabling the Switch

This procedure enables the Switch and adds an IP input.

1. Browse to Inputs > Switch. In the Main page, Switch Configuration field, tick the Enable check box and type an identifying name, e.g. the switch name, in the label box.
2. For automatic switching, tick the Automatic Switch check box. Specify the initial buffering time. Click Apply.
3. The Switch Status field presents a graphical view of the Switch status and Switch Statistics field indicates how many times switching has been occurred for both automatic and manual switches.
4. Go to the Inputs page, Switch Input Configuration field. At the bottom of the page, choose one of the pre-defined IP input and click the Add button. Click Apply. Alternatively, a new IP input can be added buy choosing 'New IP Input'. An entry for the new IP input appears in the table in the Switch Input Status
5. In the Switch Input Status field, the inputs, their alarms levels, groups and delays are illustrated.

For further details on switch setup see chapter [9.5.3](#).

4.3.3 Enabling IP output

This procedure enables IP outputs.

1. Go to the Output > Switch Outputs > Switch Main page and click on the Add Destination button at the bottom of the page.
2. Having confirmed the addition of an IP destination, the IP outputs field changes to allow specifying IP destination parameters.
3. Choose the IP output and tick the Enable box in the Basic IP Configuration field and enter the appropriate destination address in the field provided. Select RTP or UDP protocol and enter the UDP destination port number in the box provided.
4. Click Apply to commit the changes.
5. The IP Status field indicates the default physical interface used. This may be changed by clicking the Manual destination interface in the Basic IP Configuration field and selecting the desired interface from the pull-down list.

The IP status field also indicates when the destination has been reached (Resolved = Yes) and the bit rate of the IP encapsulated transport stream. Several additional IP parameters may be set in the Output > Switch Outputs > IP destination > Switch Main page. See section [9.6.3.1](#) for details.

5 Installing the Equipment



Caution: The TNS544 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 TNS544 is mechanically and electrically in order.
- Verify that you received the following items:
 - TNS544 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 TNS544 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 TNS544.

- 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 TNS544 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 T-VIPS.

5.3 Equipment installation

The TNS544 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 TNS544 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 TNS544.

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 air-space 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 TNS544 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.

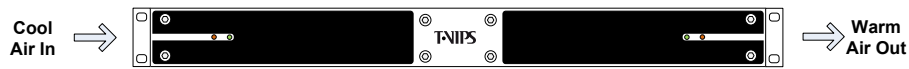


Figure 5.1 Air path through the unit

5.5 Power supply

The TNS544 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 TNS544 has a wide-range power supply accepting the voltage range 100-240 VAC, 50/60 Hz. Please refer to [Appendix B](#) for a detailed specification of the AC power supply.

5.5.2 Dual AC power supplies

Alternatively, the TNS544 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 B](#) for a detailed specification of the AC power supply.

5.5.2.1 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

5.5.2.2 Protective Earth/technical Earth

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



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



Caution: Consult the supply requirements in [Appendix B](#) prior to connecting the unit to the supply.

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

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



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

5.5.2.3 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 TNS544 mains input connector(s) and then to the local mains supply.

5.5.3 DC power supply

The TNS544 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 B](#) for detailed specification of the power supply.

5.5.3.1 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 TNS544 power input connector.

5.5.4 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 TNS544 is designed to perform seamless switching of MPEG-2 Transport Streams TS, where the input may be IP and/or ASI. Seamless switching is supported when using identical input transport streams. Identical input transport streams have the exact same TS packets at the same packet locations in the stream.

The product offers an easy-to-use WEB based user interface giving access to all configuration settings and monitoring results. The TNS544 may be integrated with network management systems via the SNMP interface.

This chapter gives a brief description of the inner workings of the TNS544, to give a better understanding of how the product works, how you use it and what you can use it for.

Figure 6.1 shows a functional block diagram of the main components inside TNS544. The different blocks are described in more detail in the following sections.

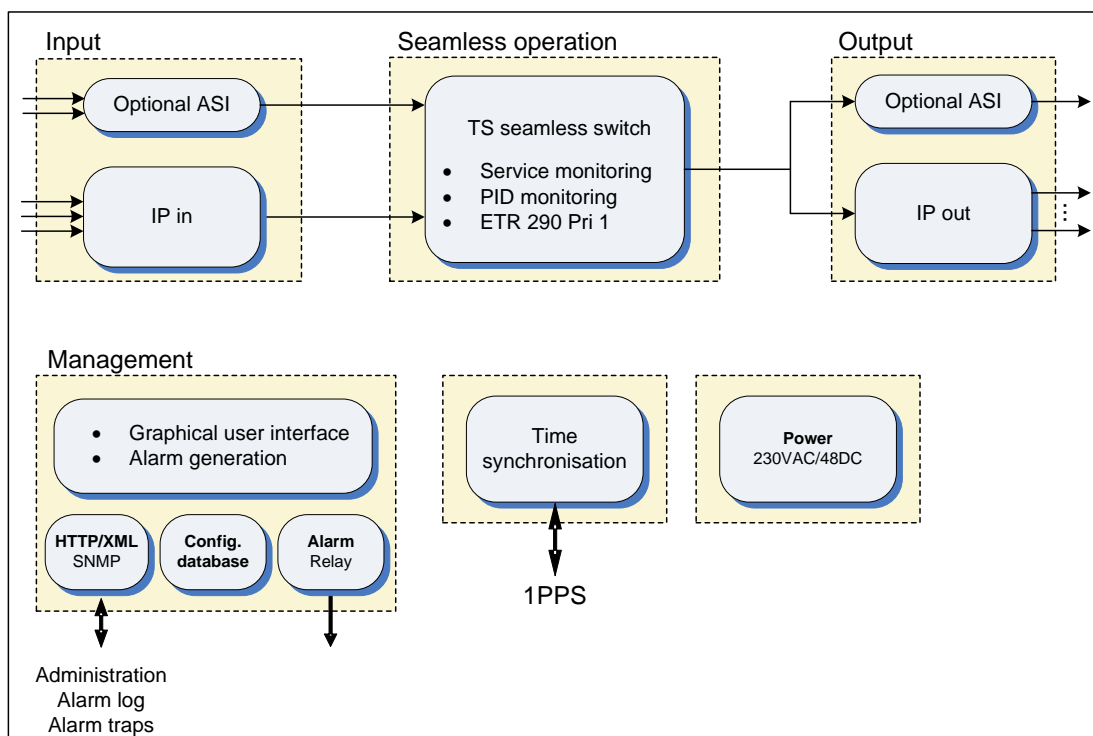


Figure 6.1 TNS544 block diagram

Each input is fed to a user specified seamless switch. The switch will match the streams and group them into matching groups. In case of sync loss on one of the input streams, the TNS544 will switch to one of the other inputs in a seamless way, causing no glitch or other errors at the output.

In case of higher level errors (content errors), a high level sophisticated switch logic takes care of the switching. Any kind of detectable alarm for an input may be used as switch criteria.

At any time, an operator may switch from the current selected IP stream on a switch to a different IP stream on the same switch. This on-demand switching will also be seamless.



Note: Seamless switching is only possible when the two incoming streams are identical. In case the streams are from different sources, switching will be done on a TS packet boundary to at least avoid sync loss at the output.

6.1 Input and output

The input interface includes two separate ethernet ports and one SFP socket that can be used to receive or transmit MPEG-2 Transport Streams over IP. However, only two of the three interfaces may be active at any one time. One of the Ethernet inputs may be substituted for a SFP module giving the option to provide input via e.g. optical fibre. Use of a SFP module is user configurable, provided this software option has been licensed.

Figure 6.2 gives a detailed overview of how the input and output interfaces are related and how they are connected to the seamless switches.

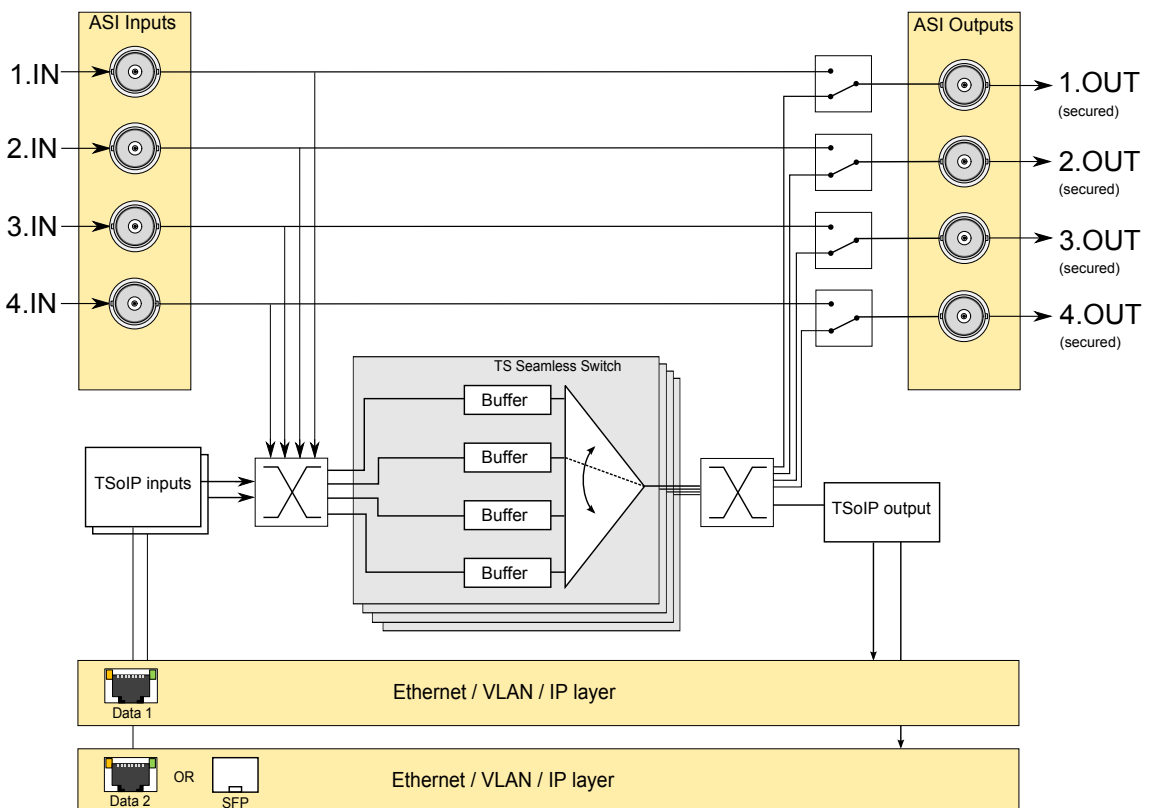


Figure 6.2 Inputs and outputs

If the unit is equipped with ASI connectors, there are 8 ASI connectors, which consists of 4 pairs with one input and one output. Each output has a controllable relay which lets the user select if the output TS should come from the corresponding input or from any of the switches. On power loss the ASI relay will fall back to its upper position, i.e. each output is wired to its corresponding input. On power loss there will be no IP output.

These are the following capabilities of the TNS544 TSoIP Switch:

- The TNS544 may have from 1 to 4 switches, where the number of switches is a licensed feature (SSWX).
- All inputs may be routed to any of the switches, but an input may not be routed to more than one switch simultaneously.
- A switch may have from 1 to 4 inputs, where each input may be ASI or IP or a combination of ASI and IP inputs.
- Each output may have up to 8 IP output copies, and up to 4 ASI output copies.
- All IP inputs and IP outputs may use any VLAN on any of the Ethernet/SFP interfaces.
- An ASI output may only be used as an output of the same switch as its corresponding input. If however the corresponding input is not used as a switch source, the output may be used as an output of any switch.

6.1.1 Protocol mapping

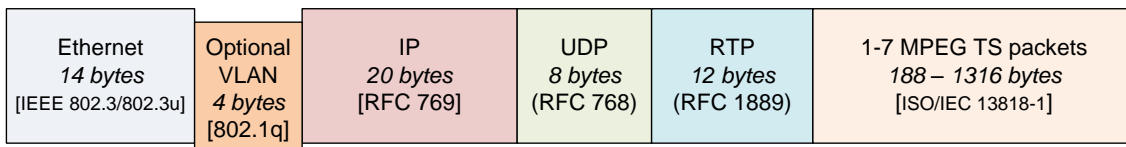


Figure 6.3 Protocol mapping

When transmitting TS streams over IP, the protocol mapping is according to figure 6.3. The VLAN framing and RTP encapsulation are optional.

The RTP layer is important for diagnosing network related problems, since it contains a sequence number that can be used for packet loss detection.

The maximum transfer unit (MTU) for Ethernet is usually 1500 bytes. This limits the number of transport stream packets to embed into the outgoing Ethernet/IP frames to be between 1 and 7.

6.2 Management subsystem

The management subsystem is a set of modules that handles all the interfaces to monitor and control the operation of the TNS544.

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.

6.2.1 Graphical user interface

Operators monitor and control the TNS544 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 TNS544 can be controlled from the web GUI.

6.2.2 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

6.2.3 Alarm manager

The TNS544 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.

Alarm relay 1 and alarm LED are controlled to signal whenever there is a **critical** alarm present. Alarm relay 2 is configurable.

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 TNS544 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.

6.3 Time synchronisation

The TNS544 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.

6.4 The SFP module

The SFP module (SFP = small form-factor pluggable) is a third-party product providing an extra, optional interface to the TNS544. Depending on the module type it may act as a direct bridge to E3 and T3 telecom network lines using coaxial cable, or provide a high-speed STM-1/OC-3 optical interface employing single or multi-mode optical fibre.



Figure 6.4 A typical SFP module

An SFP module may be configurable or non-configurable. Using a configurable SFP module the parameters relevant to its operation are controlled through the TNS544 WEB interface. Control information is passed to and from the SFP module using the I²C protocol.

A wider range of settings are available using the SFP module internal WEB server. To access the internal WEB server an SFP configuration adapter is required. For further information on this, and for detailed technical specifications, refer to the vendor's manual for the specific device.

The TNS544 provides a slot to accommodate an SFP module. Access to the SFP interface is possible if the SFP software is installed and the feature key has been licensed (see section [Section 9.4.7](#)).

The SFP interface must be expressly enabled from the TNS544 user interface (Device Info > Maintenance > General) by selecting SFP from the Electrical/SFP dropdown menu and hitting Apply

After rebooting, the user interface will reflect the presence of the SFP network interface. This is managed the same way as other network interfaces, but with an extra WEB page tab to support SFP specific functionality.

7 Physical Description

The TNS544 TSoIP Switch consists of a main board in a screened, self-ventilated cabinet. The unit is 1RU high and two units can be mounted side-by-side behind a common front panel in a 19 inch rack. All inputs and outputs are located on the rear panel and there are no front panel keypad or display.

The front panel provides four LEDs per TNS544. The meaning of each LED indicator is shown in table 7.1.

Table 7.1 Front panel LED descriptions

Indicator	Colour	Description
Power	Green	This LED is lit when power is on and initialisation is complete
Alarm	Red	This LED is lit when a failure is detected by the unit

These LEDs are replicated on the rear panel, as shown in figures 7.1 and 7.2 depending on the units ASI hardware configuration.

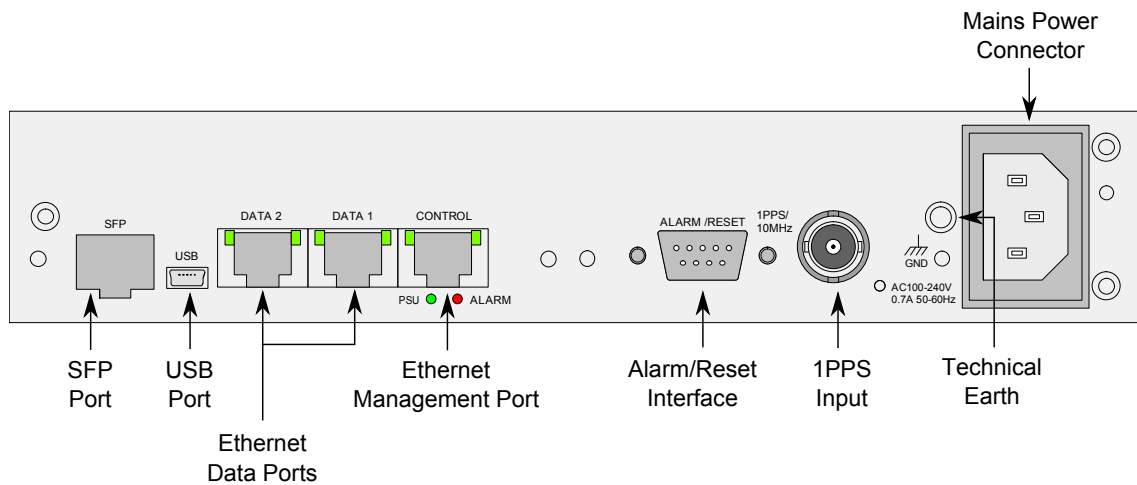


Figure 7.1 Rear panel no ASI connectors

Remove mains supply before moving or installing the equipment. Ensure ESD precautions are observed while interconnecting equipment.

7.1 ASI ports

The TNS544 may be shipped with or without ASI connectors. If equipped with an ASI board, there will be 8 ASI connectors on the rear panel, which are fixed as either input or output connectors. There are in total 4 ASI inputs and 4 ASI outputs, located in pairs of 1 input and 1 output as seen in figure 7.2. The input and output pairs are also connected through a passive relay, such that on power loss all input and output ASI pairs will be connected. See figure 6.2

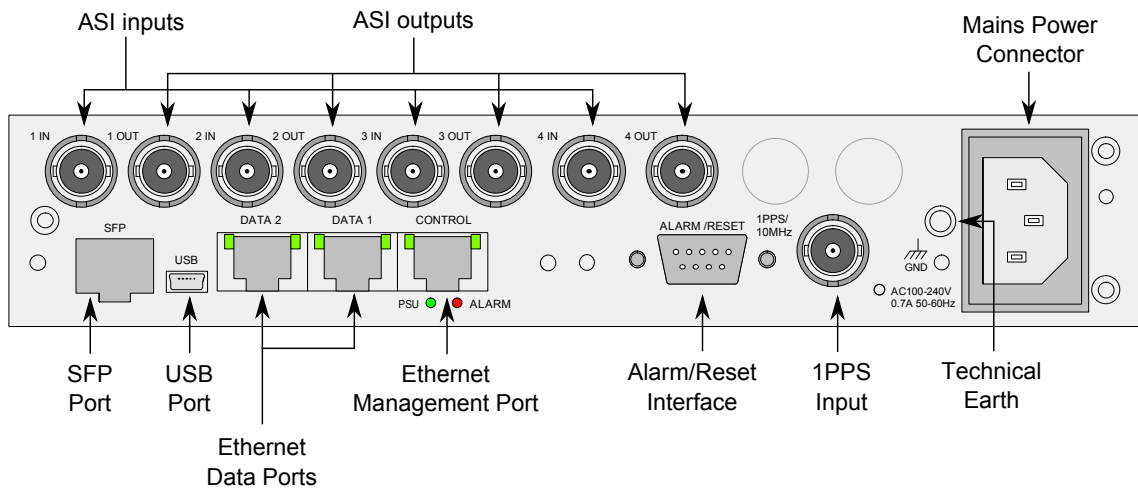


Figure 7.2 Rear panel with ASI connectors

for a circuit diagram. It is also possible to force a passive connection for each relay while power is connected, see chapter 9.6.2.1 for details on how to do this.

For physical specification of the ASI ports, please refer to [Appendix B: Technical Specification](#).

7.1.1 ASI input ports

Inputs signals connected to the ASI ports should be a DVB or ATSC compliant transport streams, depending on the selected setting (see chapter 9.4.7.1 and 9.5.2.1).

7.1.2 ASI output ports

The ASI port outputs a DVB compliant transport stream. When no stream can be supplied the output will be idle characters, only. If a stream is supplied the output will be a combination of MPEG-2 transport stream data bytes and idle characters.

7.2 1 PPS Input

An optional interface module provides an input connector for a 1 PPS synchronisation signal for the internal system clock. Connecting an 1 PPS signal will reduce potential output jitter.

The signal is:

- 1 PPS. 50 Ω TTL input for a 1 pulse-per-second signal.

For physical parameters of the 1 PPS port, see appendix [B.6.1](#).

7.3 Ethernet data ports


Two Ethernet ports are provided for data transmission. The default port setting is auto sense between 10, 100 and 1000 Mbit/s. The operator is able to force the interface speed to fixed 100 Mbit/s or fixed 1000 Mbit/s. This is useful to minimize the synchronisation time when reconnecting signal cables.


For flexibility, the TNS544 provides an optional SFP (Small Form-Factor Pluggable) slot to accommodate a copper or optical interface SFP, allowing customers to use different SFPs for special distance, cost, existing infrastructure and future expansion requirements. The TNS544 is prepared for electrical (1000Base-T) or optical 1000BASE-SX and 1000BASE-LX SFP transceivers. When the SFP module is in use Ethernet port Data2 is no longer available.

The LEDs for the electrical Ethernet data port are used as follows:

Table 7.2 Ethernet data port LEDs

LED indicator	Location	Description	Colour
Speed	Left	10 Mbit/s	Unlit
		100 Mbit/s	Green
		1000 Mbit/s	Yellow
Traffic and link	Right	Lit=Link, Blink=data tx or rx	Green

 **Note:** The TNS544 interface to the SFP slot is always Gigabit Ethernet. Other bitrates are not supported.

 **Note:** In case the SFP port is used, only the electrical Ethernet port “DATA1” will be available for use. The second data port will be deactivated when SFP is turned on using the settings in the user’s interface.

7.4 Ethernet management port

The TNS544 provides one Ethernet port for control and management. The default port setting is Auto sense, 10 or 100 Mbit/s. Connect the management port to the management network. The LEDs for the management port indicate as follows:

Table 7.3 Ethernet management port LEDs

LED indicator	Location	Description	Colour
Speed	Left	Unlit = 10 Mbit/s, Lit = 100 Mbit/s	Green
Traffic and link	Right	Lit=Link, Blink=data tx or rx	Green

7.5 Power supply

Section 5.5 provides details of the power supply, protective earth and security. Read all these instructions prior to connecting the units power cable.

7.6 Technical earth

Connect the Technical earth to a suitable earth point.

7.6.1 Alarm/Reset connector

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 7.4.

Table 7.4 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

When there is a *critical* (level 6) alarm in the unit, if the unit is not powered or if any other programmed condition for relay 1 is satisfied there will be a connection between pin 6 and pin 7. When the above conditions are not present 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 *not* to be activated for a *critical* (level 6) alarm.

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

For more details regarding the alarm relay please refer to Appendix on Technical Specifications **B**.

7.6.2 Serial USB interface

The TNS544 provides a USB interface intended for initial IP address setup. The interface conforms to the USB 1.1 specification through a Mini USB connector.

The USB interface requires a special COM port driver on the PC that shall communicate with the device. This driver is provided on the product CD shipped with the device.

8 Operating the Equipment

The TNS544 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 TNS544. 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 administrator 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 TNS544 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 TNS544 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 TNS544 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 privileges 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 TNS544 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 TNS544. Configure the PC to be on the same sub net as the TNS544. 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 TNS544 with factory default settings. The IP address/netmask

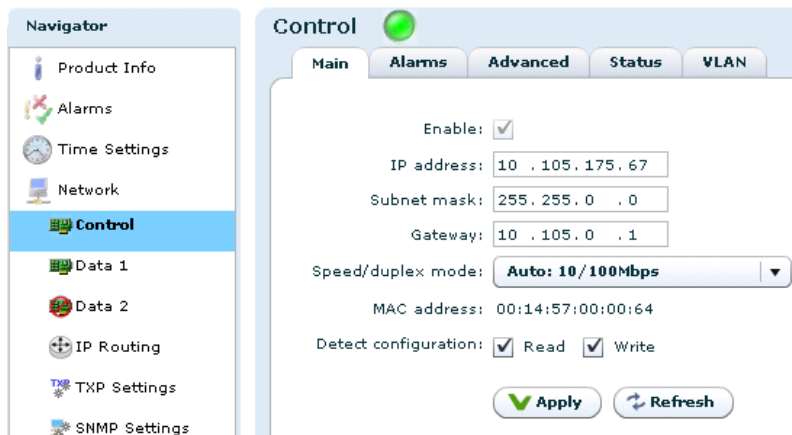


Figure 8.1 Configuring network settings via the Web GUI

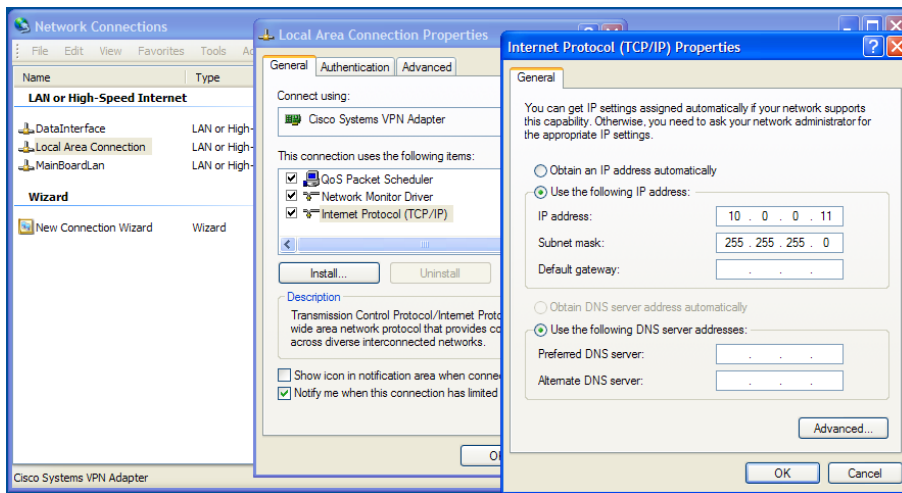



Figure 8.2 Setting static IP address 10.0.0.11 in Windows XP

is set to 10.0.0.11/255.255.255.0 which is on the same sub net as the TNS544, 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 TNS544 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. 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 TNS544 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.

9 WEB Interface

The TNS544 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 TNS544 and get status information.

9.1 Login

Access the TNS544 by entering its IP address in the address field of your favourite browser. When accessing the TNS544 the first time, the progress bar ([Figure 9.1](#)) should appear while the Flash application is loading from the device.

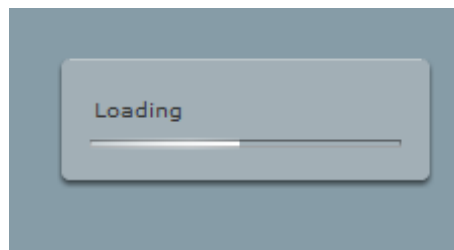


Figure 9.1 Flash application loading

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](#).

A screenshot of a login window titled "Login". It contains a "Username:" field with the text "admin" and a "Password:" field with "*****". Below these is a "Save password" checkbox which is checked. At the bottom are two buttons: "Login" and "Clear".

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.



Figure 9.3 The status header

In the status header the product name is shown on the left hand side, along with the T-VIPS logo.

The status bar displays an 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 E](#).

Several information are displayed in the right corner/section of the header. Starting from the left:

- The user defined device name, if entered.
- A button to log out from the GUI.
- A button to switch current user level.
- A text showing the current user name.
- The local device time.
- 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.
- 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 unit operational mode. Clicking a tab will open the corresponding page with a navigation pane to the left as shown in [Figure 9.4](#). This pane is used to navigate between sub-pages of the tab.

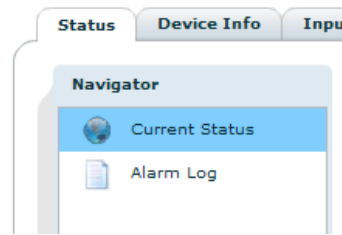


Figure 9.4 Status navigator



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 E](#).

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.

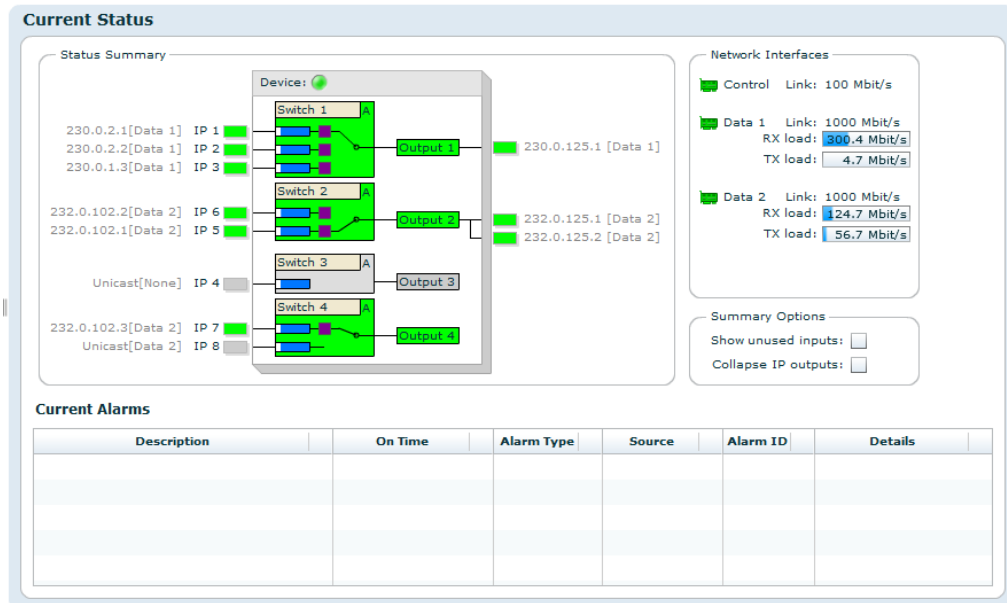


Figure 9.5 Current status

If an input switch is defined, it is shown in the status diagram as a box inside the device block in front of a MUX block. The block shows the ports that are members of the switching group, and the currently selected port. Clicking the switch block will take you to the configuration page for the switch.

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.

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 E](#).

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 TNS544.

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 E](#).

9.3.2 Alarm log

Severity	On Time	Off Time	Alarm type	Source	Description	Alarm id
Notification	1970-01-01 04:04:28	1970-01-01 04:04:28	System	System	Config changed	505
Notification	1970-01-01 04:02:44	1970-01-01 04:02:44	System	System	Config changed	505
Notification	1970-01-01 03:46:33	1970-01-01 03:46:33	System	System	User logged in	501
Critical	1970-01-01 02:51:54	1970-01-01 02:51:55	Ethernet ...	eth0	Ethernet link down	130
Critical	1970-01-01 00:15:00	1970-01-01 00:15:02	Ethernet ...	eth0	Ethernet link down	130
Notification	1970-01-01 00:00:41	1970-01-01 00:00:41	System	System	System started	503
Notification	1970-01-01 00:00:41	1970-01-01 00:00:41	System	System	Config changed	505
Critical	1970-01-01 00:00:34	1970-01-01 00:00:41	System	System	System is starting up	518

Alarms in log: 8 Enable updates

Figure 9.6 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 additional parameters 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 TNS544.

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 9.7](#).

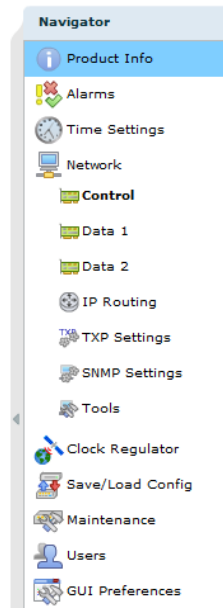


Figure 9.7 Device Info navigator

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

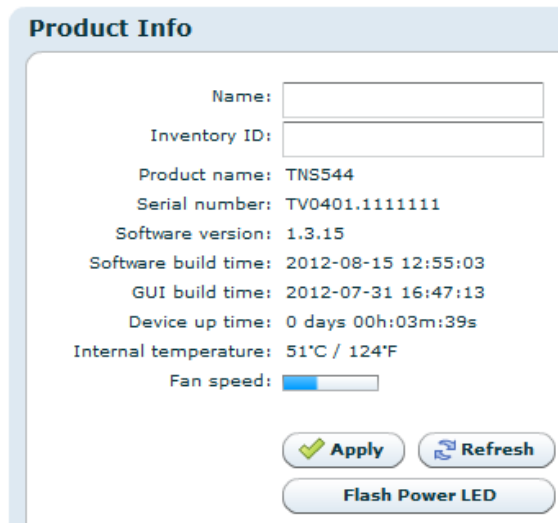
Configures the current user defined name of the unit. This parameter, together with the management network parameters are used as device identifiers and remain untouched if the unit configuration is changed by loading a different configuration file. See [Section 9.4.6](#). The device name is shown in the web GUI status header (see [Section 9.3.1](#)), and in the web browser title bar to facilitate identification of each device.

Product name

Displays the name of the product as designated by T-VIPS.

Serial number

The serial number of the device.



Product Info

Name:

Inventory ID:

Product name: TNS544

Serial number: TV0401.1111111

Software version: 1.3.15

Software build time: 2012-08-15 12:55:03

GUI build time: 2012-07-31 16:47:13

Device up time: 0 days 00h:03m:39s

Internal temperature: 51°C / 124°F

Fan speed:

Figure 9.8 Product Information

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 9.9](#):

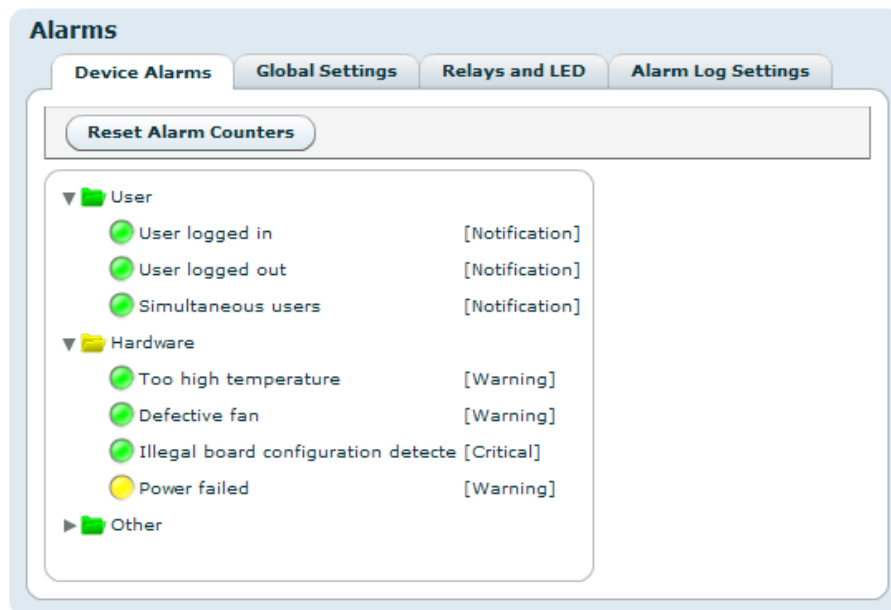


Figure 9.9 Alarm configuration

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 9.9](#) 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.

Description

Brief description 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

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.

Device Alarms

Alarms Global Settings Relays and LED Alarm Log Settings

Type ID	Type	Alarm ID	Description	Default Severity	New Severity	Send Trap	Log
24	IP Output	106	Unable to transmit	Critical	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Ethernet port	130	Ethernet link down	Critical	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Ethernet port	131	Ethernet output o...	Critical	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
20	Encoder	132	Total bitrate too l...	Critical	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
24	IP Output	140	IP address unres...	Warning	Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	IP Input	150	RTP sequence error	Warning	Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	IP Input	151	No data received	Warning	Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Port	152	FEC threshold ex...	Warning	Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
17	Ethernet port	153	Ethernet input ov...	Critical	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
23	IP Input	154	Data lost	Critical	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply Refresh

Figure 9.10 Global alarm configuration

9.4.2.3 Relays and LED

This page lets the user configure the alarm severity level that shall turn the relays and alarm LED on. The behaviour of Alarm relay 1 and Alarm relay 2, and the Alarm LED may be configured individually for each alarm severity level. Note that the Alarm relay 1 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 relays and LED is indicated inside the associated brackets.

Alarms

Device Alarms Global Configuration Relays and LED Alarm Log Settings

Relay and LED level triggers

	Alarm Relay 1 [yes]	Alarm Relay 2 [yes]	Alarm LED [yes]
Critical:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Major:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Minor:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Warning:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Notification:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

General Purpose Input
GPI status: Inactive
Enable GPI reset:

Virtual Relays

ID	Enable	Label	Expression	Count Thresh.	Count	Active
0	<input type="checkbox"/>			1	0	false
1	<input type="checkbox"/>			1	0	false
2	<input type="checkbox"/>			1	0	false
3	<input type="checkbox"/>			1	0	false
4	<input type="checkbox"/>			1	0	false
5	<input type="checkbox"/>			1	0	false
6	<input type="checkbox"/>			1	0	false
7	<input type="checkbox"/>			1	0	false
8	<input type="checkbox"/>			1	0	false
9	<input type="checkbox"/>			1	0	false

Apply Refresh

Figure 9.11 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 7.6.1](#). GPI status indicates if the input signal is active.

For further details on the physical relays refer to [Section B.5.1](#).

The Virtual Relays field shown in [Figure 9.11](#) 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 (\geq) 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 <i>subid1</i> value	Number	subid1 = 1
subid2	Alarm <i>subid2</i> value	Number	subid2 = 2
subid3	Alarm <i>subid3</i> value	Number	subid3 = 1190
port	Synonym for <i>subid2</i>	Number	port = 2
service	Synonym for <i>subid3</i>	Number	service = 102
pid	Synonym for <i>subid3</i>	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 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
<	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

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.

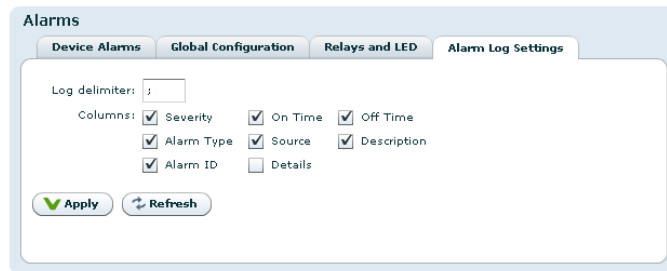


Figure 9.12 Configuring the alarm log

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

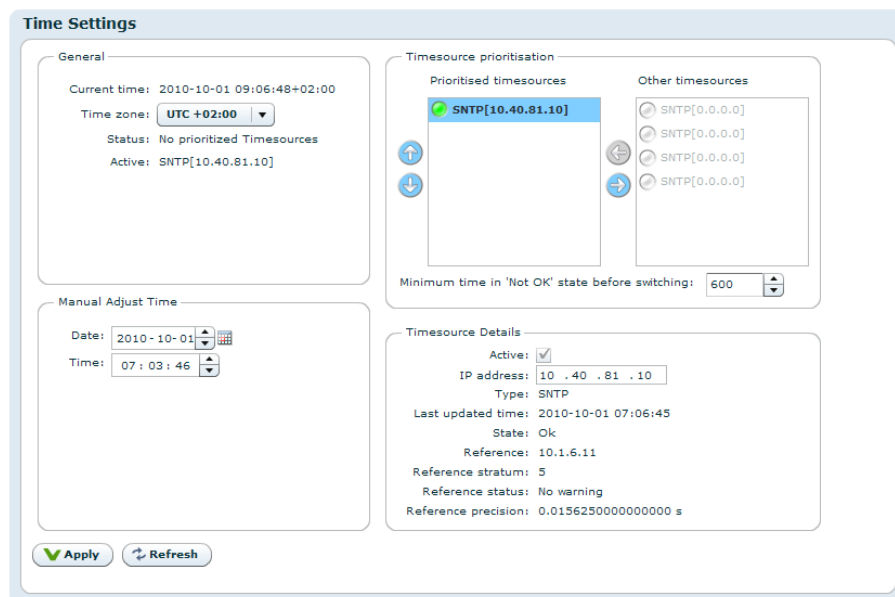


Figure 9.13 Time Settings

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 four main 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 all available 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 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).

Located below the lists is a field to define the maximum allowed time interval between updates from the currently used time source. Exceeding 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 9.14 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

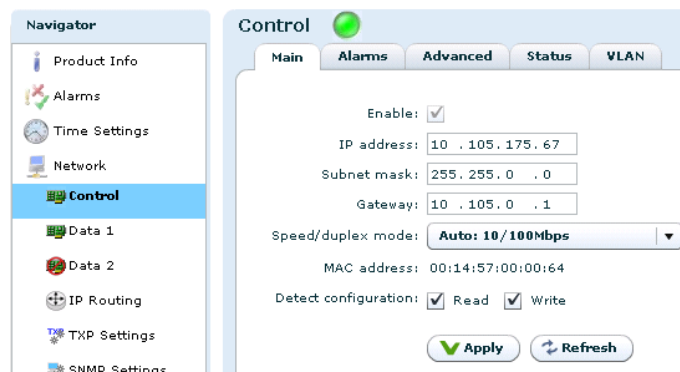


Figure 9.15 Main IP settings

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.

Enable

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

IP address

IP address of the interface.

Subnet mask

The subnet mask of the interface.

Gateway

The default gateway address for the 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 ((http://en.wikipedia.org/wiki/Duplex_mismatch,Wikipedia duplex mismatch article))(http://en.wikipedia.org/wiki/Duplex_mismatch).

MAC address

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

Detect configuration

Applies to the Control interface, only.

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

Enabling the Read option makes the TNS544 visible for the T-VIPS Detect on the LAN. If the Write option is enabled the IP address of the TNS544 may be configured using the T-VIPS Detect. These options do not affect the operation of the device from the management application T-VIPS Connect.

9.4.4.1.2 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.

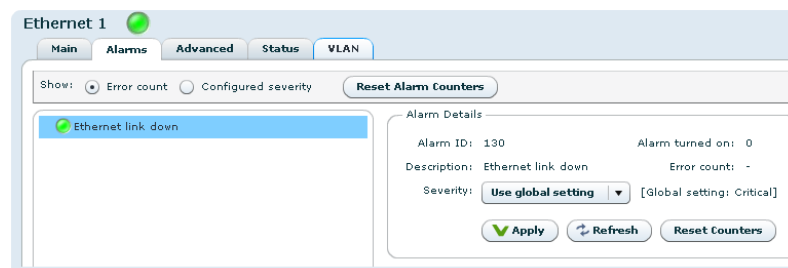


Figure 9.16 Network interface alarms

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.

9.4.4.1.3 Advanced

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

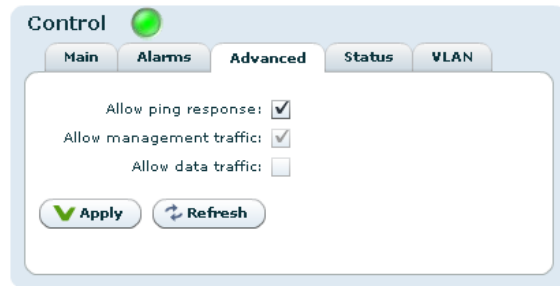


Figure 9.17 Advanced IP settings

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.*

Multicast router

This parameter is not shown in the management interface page.

The IP address of the multicast router. The address here is used in conjunction with the Use multicast router option in the "IP Output" page, [Section 9.6.3.1](#).

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.

9.4.4.1.4 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:

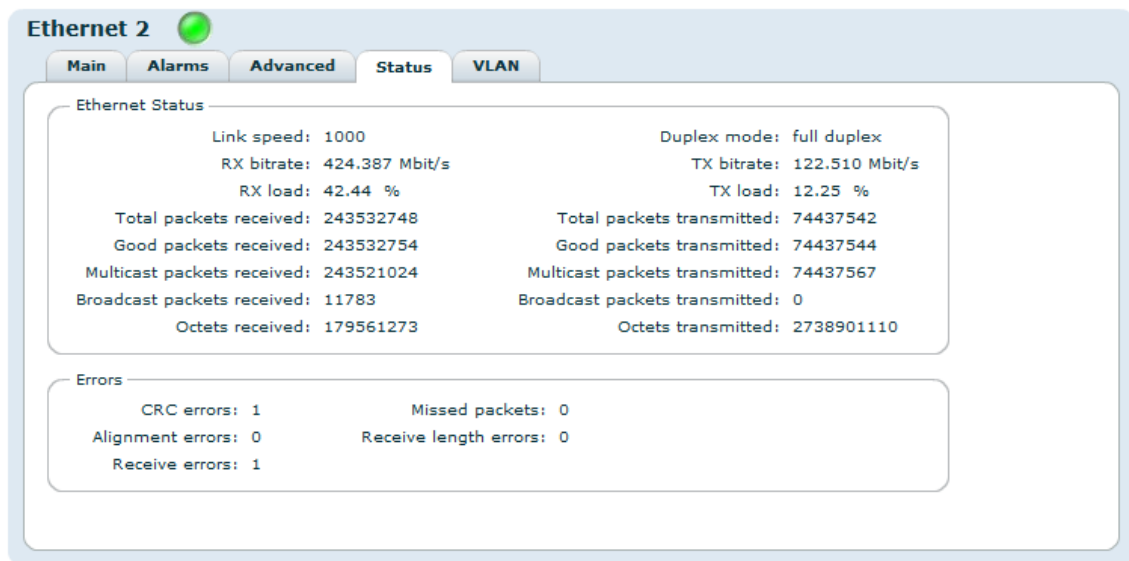


Figure 9.18 Interface Status

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.

9.4.4.1.5 VLAN

Enable	ID	Pri	IP Addr	Net Mask	GW Addr	Multicast Router	Data	Control	Ping	IGMP ver
<input checked="" type="checkbox"/>	1	0	10.0.0.10	255.255.255.0	10.0.0.1	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	v2
<input checked="" type="checkbox"/>	2	0	10.107.3.226	255.255.255.0	10.0.0.1	0.0.0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	v3
<input type="checkbox"/>	3	0	10.0.0.10	255.255.255.0	10.0.0.1	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	v2
<input type="checkbox"/>	4	0	10.0.0.10	255.255.255.0	10.0.0.1	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	v2

Figure 9.19 VLAN configuration

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. Editing is done directly in the table. Edited fields are shown as yellow. Pending deletions are shown in red.

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

Enable

Enable/disable the virtual interface.

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.

Pri

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

IP Addr

The IP address of the virtual interface.

Net Mask

The subnet mask of the virtual interface.

GW Addr

The gateway address to use for the virtual interface.

Multicast Router

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

Data

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

Control

Checked box enables the virtual interface to allow management traffic.

Ping

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

IGMP ver

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

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

9.4.4.1.6 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 9.4.7.1 , provided the appropriate licence has been installed .

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 TNS544 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 9.21](#), 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.

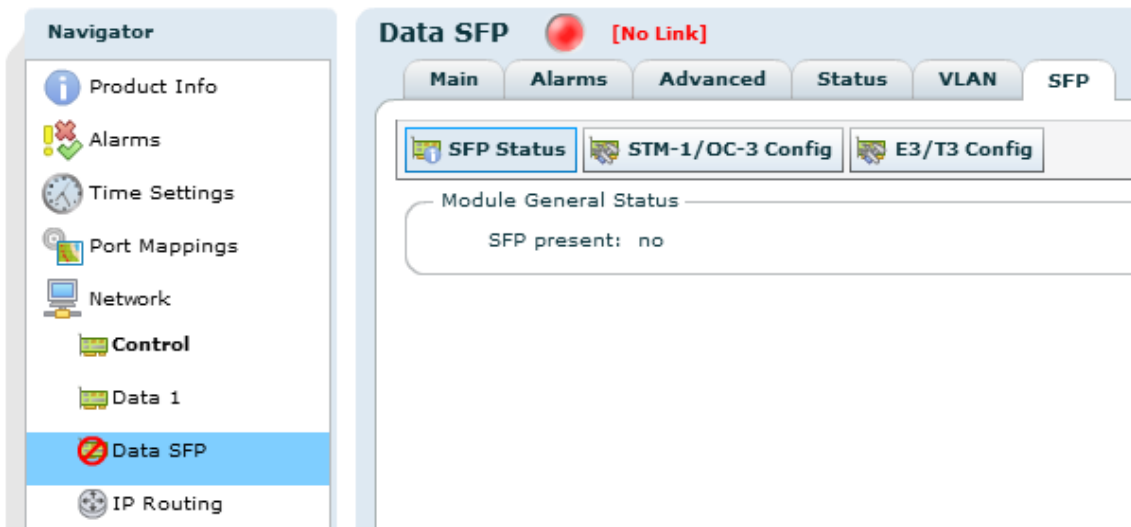


Figure 9.20 The Device Info > Network > SFP tab

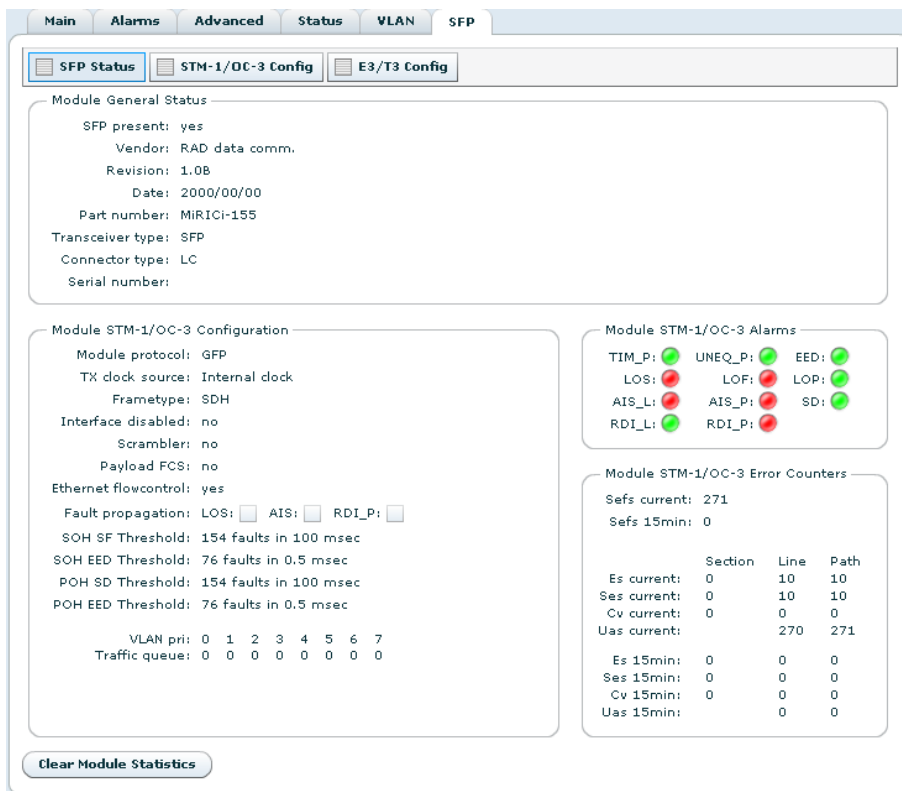


Figure 9.21 The SFP status page

The Module General Status field displays the status of the module as seen by the TNS544.

SFP Present

Indicates that the module has been detected by the TNS544.

Vendor

Shows the vendor name.

Revision

Indicates the module revision.

Date

Indicates the revision 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 TNS544.

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 9.22** 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 TNS544, only.

In the General field the main operational parameters are set.

STM-1/OC-3 present

Indicates if the module has been detected by the TNS544.

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.

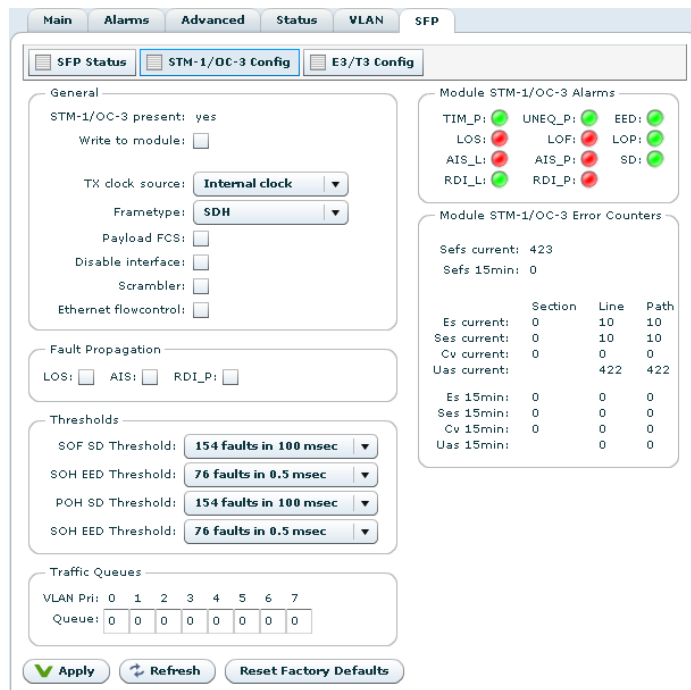


Figure 9.22 The configuration page for the STM-1/OC-3 SFP module

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 TNS544 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 shut-down 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 Traffic 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 9.23](#) the page contains four fields to set operational parameters. Editing the configuration settings will alter the SFP configuration file stored in the TNS544, only.

E3/T3 present

Indicates if the module has been detected by the TNS544.

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).

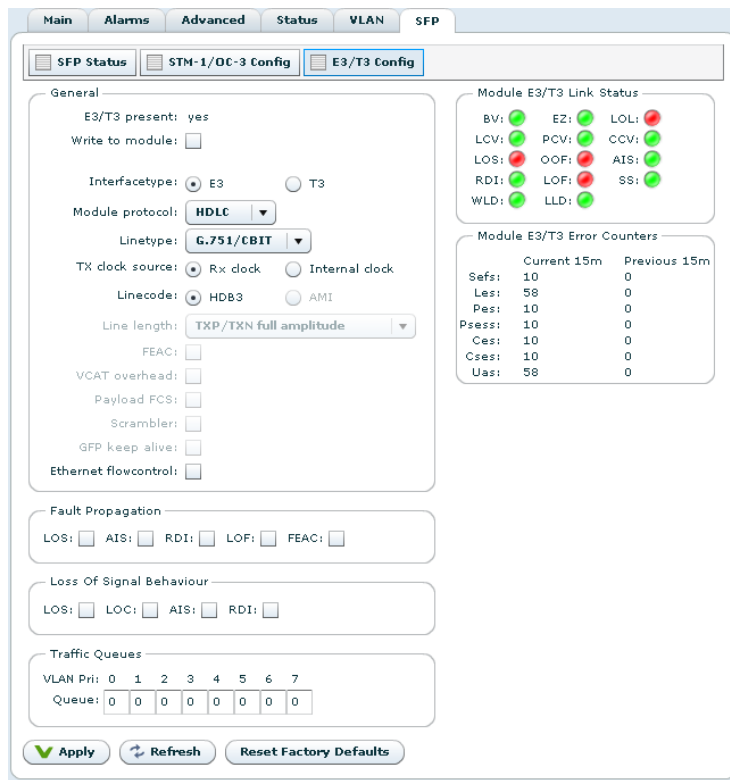


Figure 9.23 The configuration page for the E3/T3 SFP module

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 TNS544 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 Traffic 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 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 9.24 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.

9.4.4.3 TXP Settings

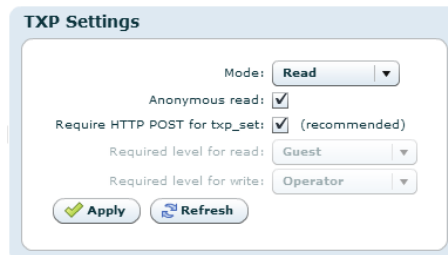


Figure 9.25 TXP Settings

TXP is a T-VIPS 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. A description of the TXP protocol can be found on the T-VIPS Product CD, or by contacting T-VIPS Support.

```

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>
    
```

9.4.4.4 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.

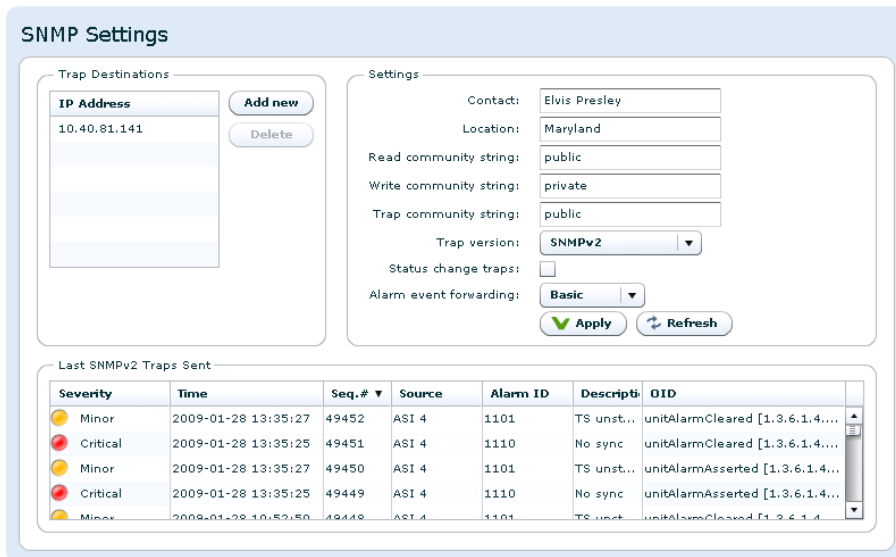


Figure 9.26 SNMP Settings

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](#).

9.4.4.5 Tools

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.

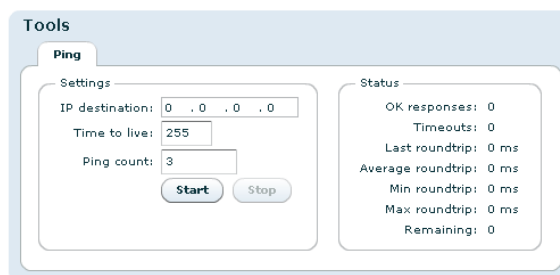


Figure 9.27 The Ping tool

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.

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.

9.4.5 Clock Regulator

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

9.4.5.1 Main

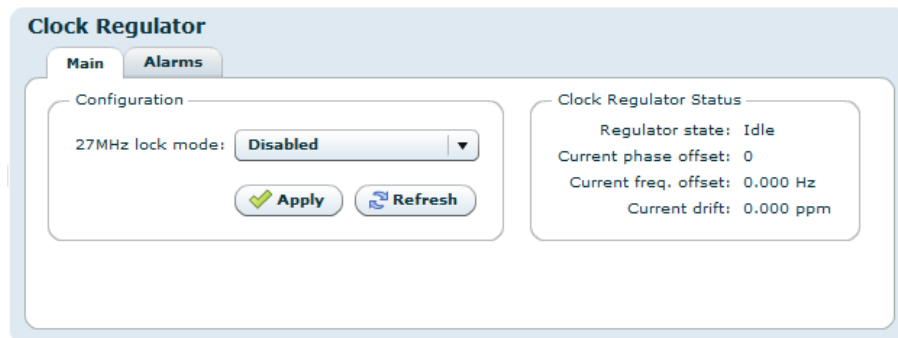


Figure 9.28 Clock regulator

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.

9.4.5.2 Alarms

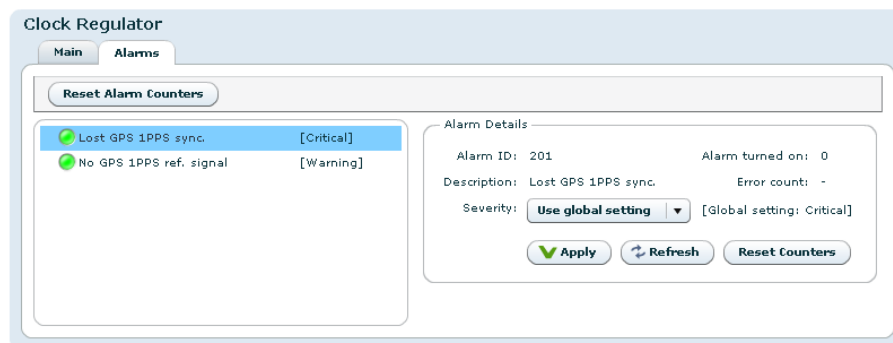


Figure 9.29 Clock regulator Alarms

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.

9.4.6 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.

9.4.6.1 Save/Load Configs

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.

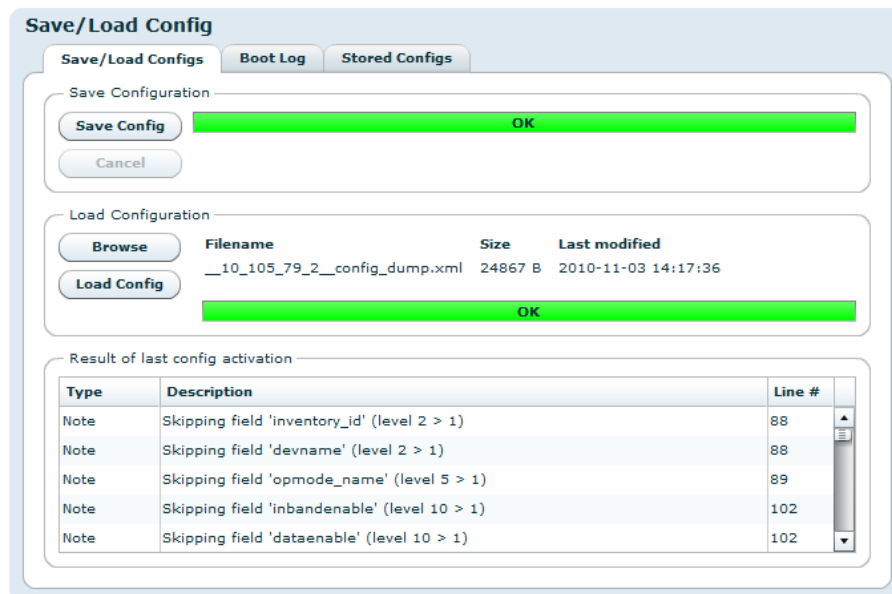


Figure 9.30 Saving and loading of configuration files

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.

Options specific to the device, including device name and management port network configuration, are intentionally 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.

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.

9.4.6.2 Boot Log

This page shows the configuration database status log from the configuration loading at last re-boot. 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.

9.4.6.3 Stored Configs

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

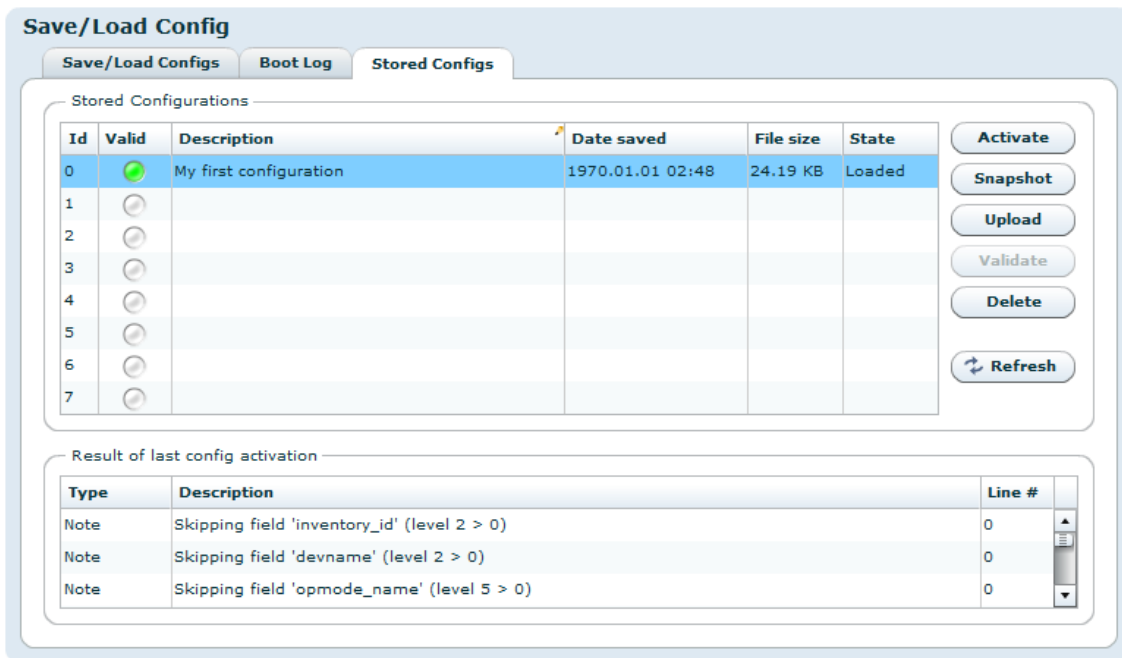


Figure 9.31 Locally stored configuration files

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 config has a valid XML syntax or not. Valid syntax is indicated by a green indicator and a invalid syntax 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**Full**

Indicates that the configuration is a snapshot that was taken using the Snapshot utility, storing a backup of the local system.

Loaded

Indicates that the snapshot was uploaded to the device from a PC.

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.

Validate

The validation process is done automatically during upload. The button is therefore disabled.

Delete

Delete the entry selected in the snapshot list.

Refresh

Reload the 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 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.

9.4.7.1 General

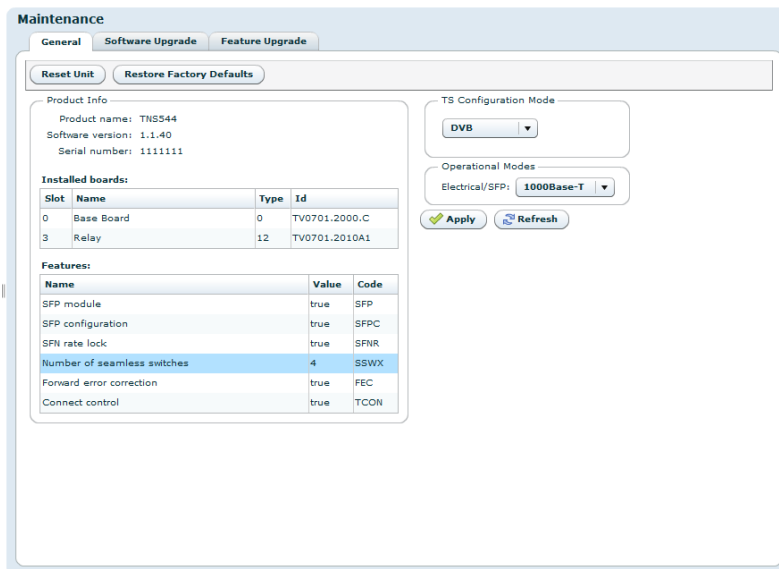


Figure 9.32 Maintenance

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.

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).

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

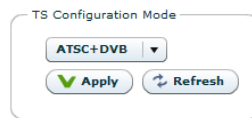


Figure 9.33 TS Configuration Mode

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.

The Operational Modes frame is visible if the SFP Module SW licence key is installed. This provides the option Electrical/SFP as shown in figure 9.34. This option is used to allocate the Data-2 IP input to operate through the Electrical Ethernet data interface, or through the SFP slot.



Figure 9.34 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.

9.4.7.2 Software Upgrade

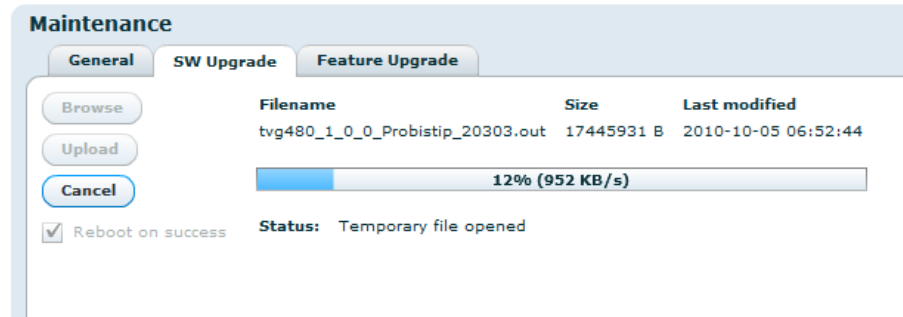


Figure 9.35 Software Upgrade

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 an 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.

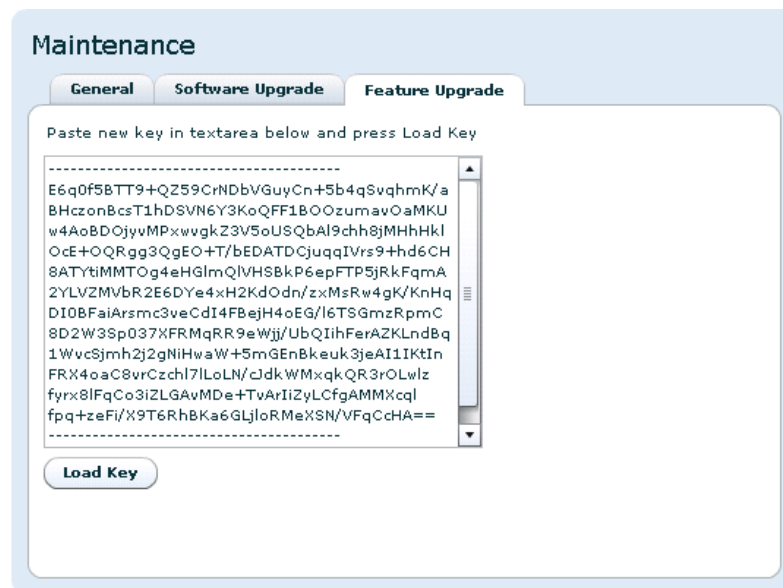
If the Reboot on success option is active the unit will automatically reboot when loading is complete, otherwise an alarm New SW pending is set to indicate that a new SW will be used on next manual reboot.

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.

9.4.7.3 Feature Upgrade



Maintenance

General Software Upgrade Feature Upgrade

Paste new key in textarea below and press Load Key

```

-----
E6q0f58TT9+QZ59CrNDbVGuyCn+5b4qSvqhmK/a
BHczonBcsT1hDSVN6Y3KoQFF1B0OzumavOaMKU
w4AoBD0jyvMPxwvgkZ3V5oUSQbAl9chh8jMHHkkl
OcE+OQRgg3QgEO+T/bEDATDCjuqqIVrs9+hd6CH
8ATYtiMMTOg4eHGlMqIVHSBkP6epFTP5jRkFqmA
2YLVZMVbR2E6DYe4xH2KdOdn/zxMsRw4gK/KnHq
DI0BFaiArsmc3veCdI4FBejH4oEG/l6TSGmzRpmC
8D2W3Sp037%FRMqRR9eWjj/UbQIihFerAZKLndBq
1WvcSjmh2j2gNIHwaW+5mGEnBkeuk3jeA11IKtIn
FRX4oaC8vrCzchI7lLoLn/cjdkWMxqkQR3rOLwLz
fyrx8lFqCo3iZLGAvmDe+TvArIiZyLCfgAMMXcql
fpq+zeFi/X9T6RhbKa6GLjloR.MeXSN/VFqCCHA==
-----

```

Load Key

Figure 9.36 Feature Upgrade

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. The device needs to be restarted to activate the new features.

Reset can be performed from the GUI as explained on the Maintenance > General tab in [Section 9.4.7.1](#).



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

9.4.8 Users

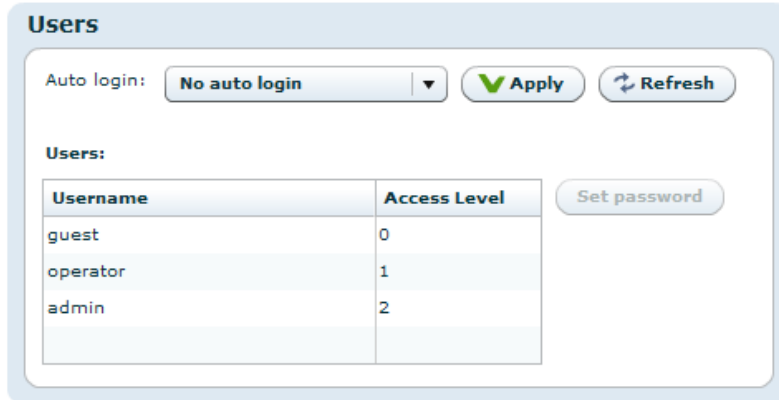


Figure 9.37 Users page

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 privileges 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.

9.4.9 GUI Preferences

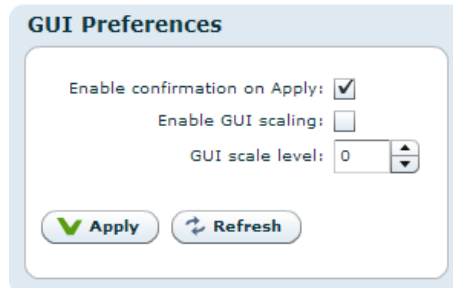


Figure 9.38 GUI Preferences page

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.

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. In addition the list also includes the input switchers and their corresponding inputs, if configured.

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

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.

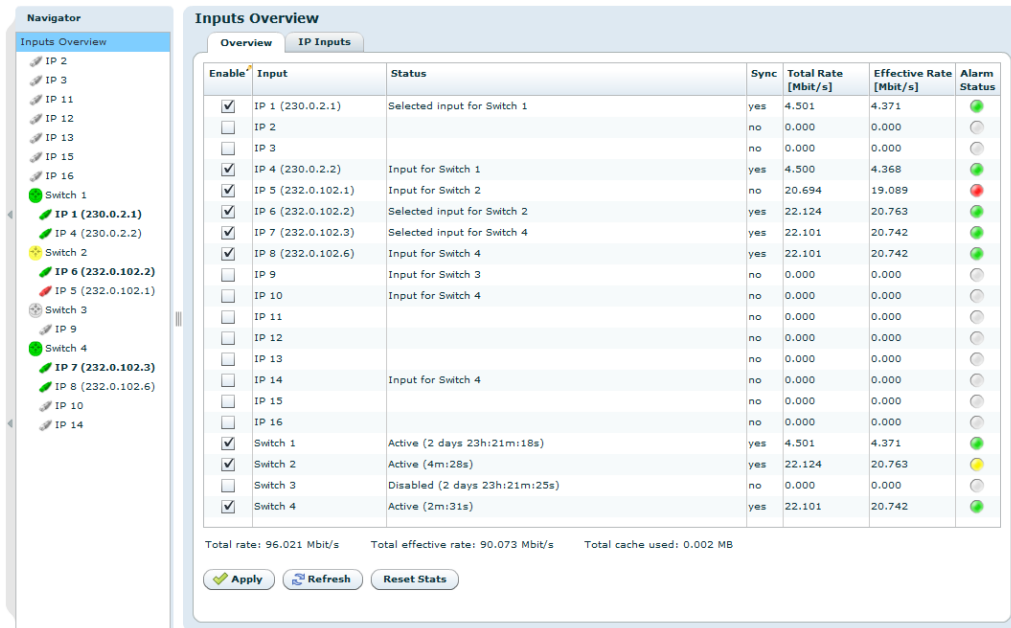


Figure 9.39 Inputs Overview

Input

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

Status

Describes status for the input signals and switches. For IP inputs, the status field indicates which switch they are sourcing as well as whether they are the active input. For the switches, this field indicates whether they are active or disabled.

Sync

Displays “yes” if the unit has synchronised to this transport stream input.

TS id

The transport id of the transport stream currently received on the input. This parameter depends on the PAT table of the PSI being present on the input and decoded successfully.

ON id

The Original Network id of the transport stream currently received on the input. The correctness of this parameter depends on the SDT-actual table of the SI being present on the input and decoded successfully.

Note that in ATSC mode the Original Network id is not applicable.

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 dialogue box that allows reset of channel statistics. [Figure 9.40](#) shows the dialogue box. Select the statistics items you want to reset and then press Apply.

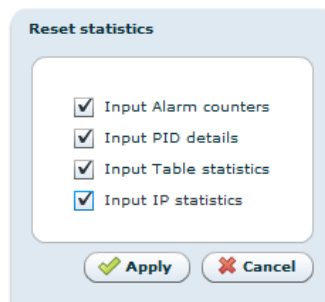


Figure 9.40 Reset statistics dialogue box

9.5.1.1 IP Inputs

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

Enable

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

IP Input

The name of the IP input, consisting of the factory defined label 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.

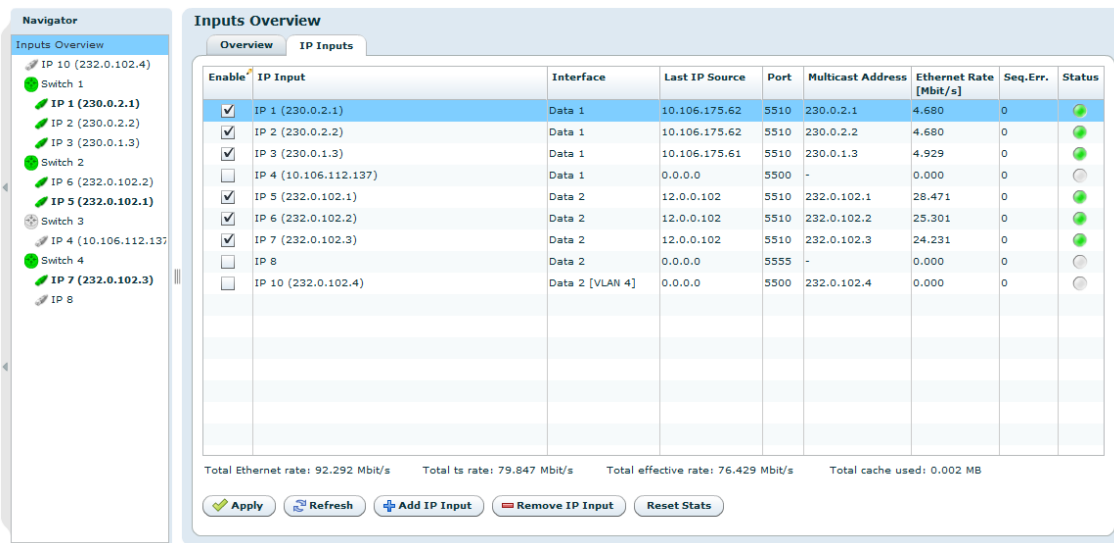


Figure 9.41 Inputs Overview - IP Inputs

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 top part of the page is common for all sub pages and shows the name and the current alarm status of the input.

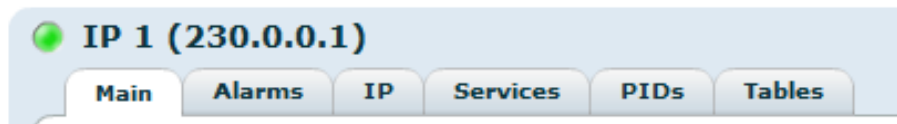


Figure 9.42 Input header

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.

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 [Section 9.3.1](#).

9.5.2.1 Main

The Main page is divided into three sections for ASI Inputs (figure [Figure 9.43](#)) 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 9.44](#).

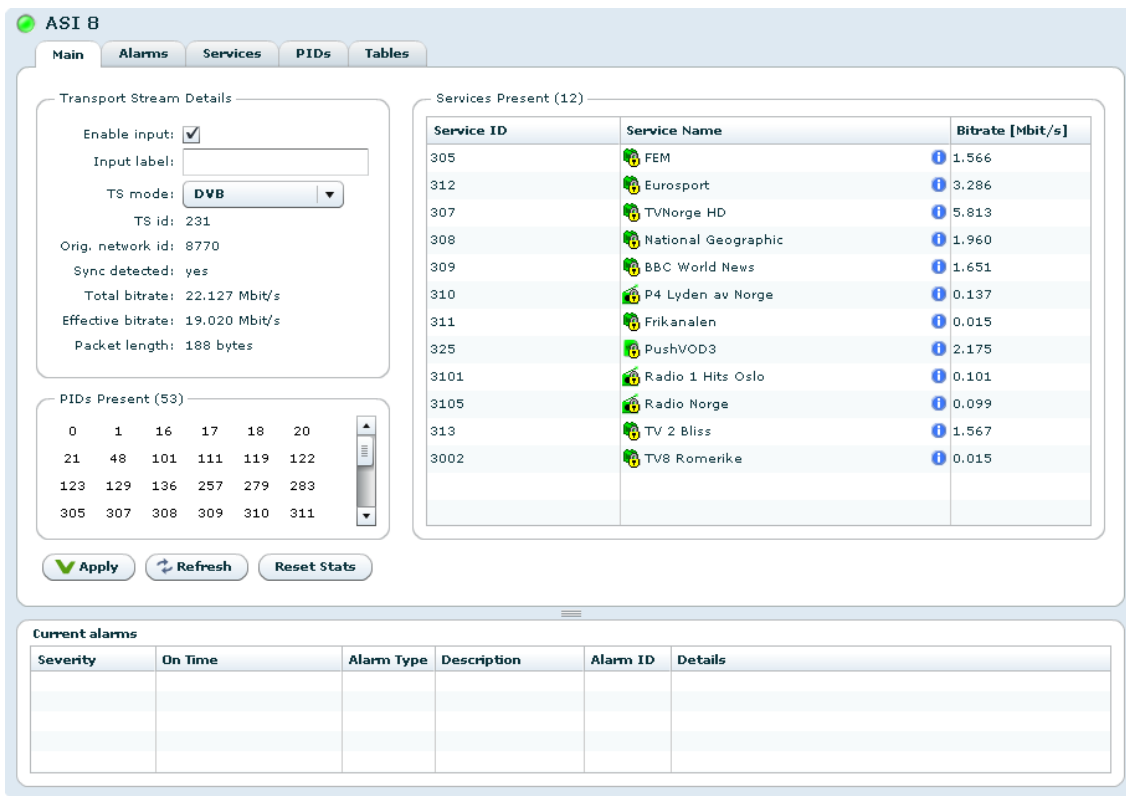


Figure 9.43 Main

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.

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.

IP 2 (230.0.238.1)

Main Alarms IP Services PIDs Tables

IP RX Configuration

Enable input:

Input label:

Receive port:

Presumed jitter: ms

Join multicast:

Source interface:

IP RX Status

Locked: yes

Last IP source: 10.106.250.238

Total bitrate: 28.936 Mbit/s

Latency: 130 ms

Min/Max latency: 8 ms / 131 ms

TS packets per frame: 1

RTP sequence errors: 0

Lost IP frames: 0

Transport Stream Details

TS mode:

TS id: 231

Orig. network id: 8770

TS bitrate: 22.136 Mbit/s

Effective bitrate: 21.042 Mbit/s

Packet length: 188 bytes

PIDs Present (56)

0	1	16	17	18	20	21	48
101	111	119	122	123	129	136	257
279	283	305	307	308	309	310	311
312	313	<i>559</i>	<i>561</i>	<i>562</i>	<i>563</i>	<i>564</i>	<i>565</i>
<i>566</i>	576	577	<i>748</i>	<i>756</i>	<i>760</i>	<i>764</i>	<i>768</i>
<i>772</i>	<i>776</i>	<i>800</i>	<i>804</i>	<i>805</i>	2800	2801	2803
2804	2805	<i>2849</i>	<i>2850</i>	2852	2864	2870	8191

Services Present (12)

Service ID	Service Name	Bitrate [Mbit/s]
305	FEM	2.630
312	Eurosport	1.193
307	TVNorge HD	5.348
308	National Geogra...	2.393
309	BBC World News	1.668
310	P4 Lyden av Norge	0.132
311	Frikanalen	2.041
325	PushVOD3	2.173
3101	Radio 1 Hits Oslo	0.096
3105	Radio Norge	0.098
313	TV 2 Bliss	2.591
3002	TV8 Romerike	0.014

Current alarms

Severity	On Time	Alarm Type	Description	Alarm ID	Details

Apply Refresh Reset Stats

Figure 9.44 IP Input Sections

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.

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.

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.

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.

In figure 9.45 the Alarm Config page is shown. Note that the alarms are organised hierarchically and that only the branches in focus need to be expanded.

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 9.46).

Error count

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



Figure 9.45 Input alarm configuration

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.

The input alarm tree is shown in figure 9.46. By clicking on the alarm nodes in the tree the details for the selected alarm is shown in the Alarm details section (figure 9.47).

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 9.47). The frame appears when a particular alarm is clicked. Its content may vary according to the alarm selected.

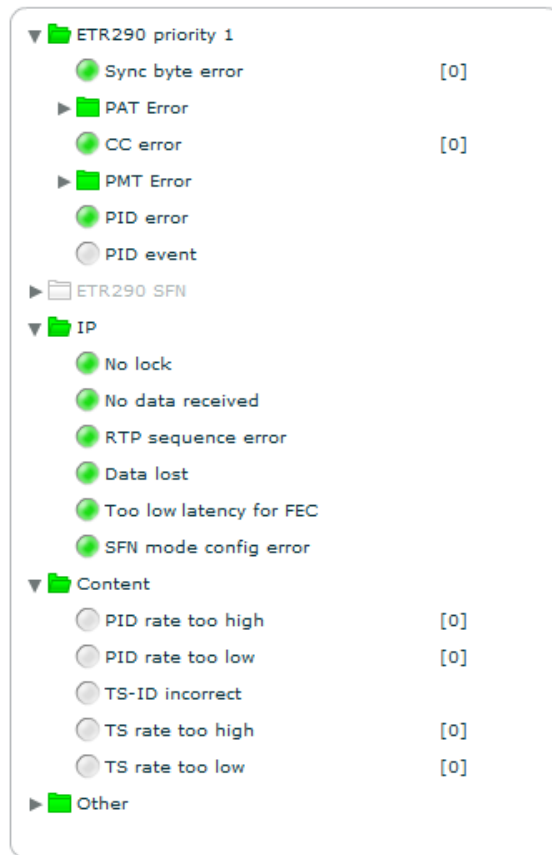


Figure 9.46 Input alarm tree

The 'Alarm Details' form contains the following information and controls:

- Alarm ID: 1151
- Alarm turned on: 0
- Description: PMT repetition interval
- Error count: 0
- Severity: Use global setting (dropdown menu) [Global setting: Warning]
- Off time: 15 s [Default: 15]
- Max interval: 500 ms [Default: 500]
- Buttons: Apply, Refresh, Reset Counters

Figure 9.47 Alarm details

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 E.3.

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.

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 9.48](#)) allow overriding of sub items. For such alarms two tables are shown below the alarm details.

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.

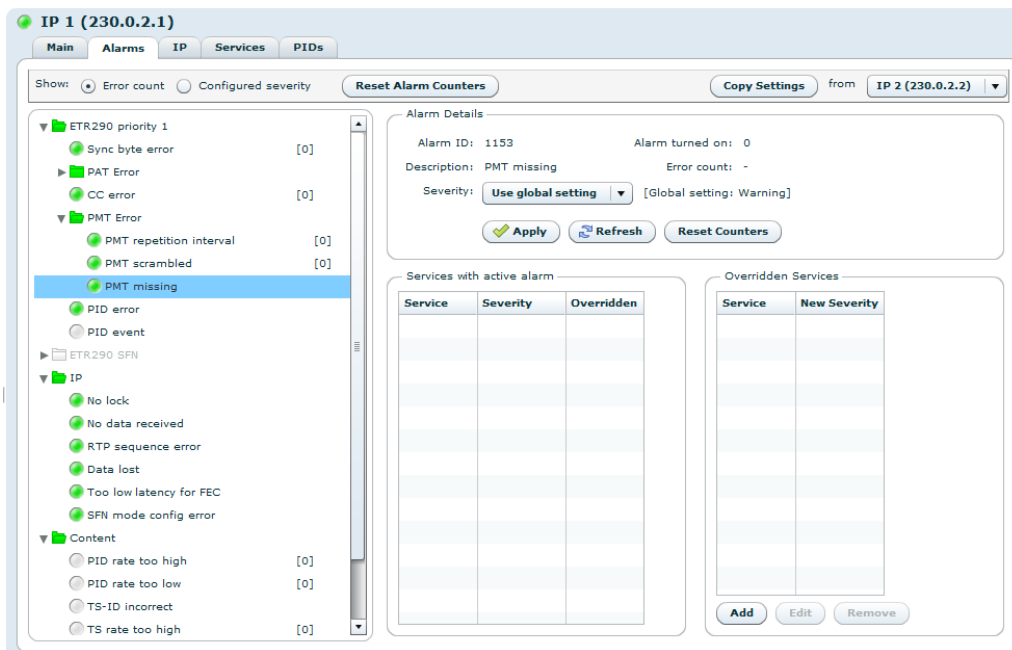


Figure 9.48 Alarm severity per sub-ID (typically Service or PID)

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.

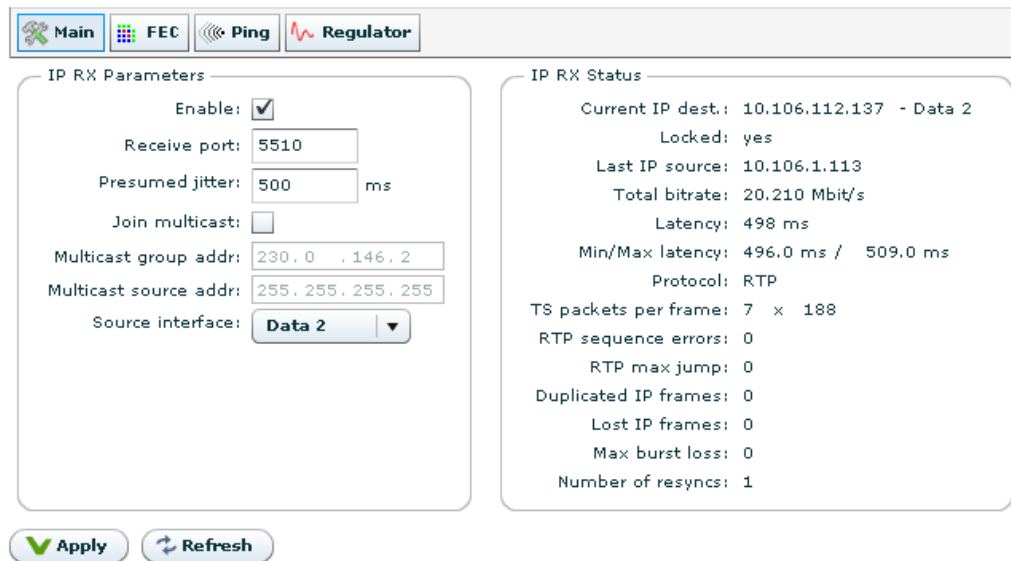
An override can be edited or removed by right-clicking on the entry in the list. Alternatively this can be done by hitting the Edit and Remove button, respectively. An override can also be added hitting the Add button and manually entering the ID and overridden values.

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.

The Main sub page is shown in figure 9.49.



The screenshot shows the IP Configuration web interface. At the top, there are four tabs: Main (selected), FEC, Ping, and Regulator. Below the tabs, there are two main sections: IP RX Parameters and IP RX Status.

IP RX Parameters:

- Enable:
- Receive port: 5510
- Presumed jitter: 500 ms
- Join multicast:
- Multicast group addr: 230.0.146.2
- Multicast source addr: 255.255.255.255
- Source interface: Data 2

IP RX Status:

- Current IP dest.: 10.106.112.137 - Data 2
- Locked: yes
- Last IP source: 10.106.1.113
- Total bitrate: 20.210 Mbit/s
- Latency: 498 ms
- Min/Max latency: 496.0 ms / 509.0 ms
- Protocol: RTP
- 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

At the bottom of the IP RX Parameters section, there are two buttons: Apply and Refresh.

Figure 9.49 IP Configuration

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.

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.

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

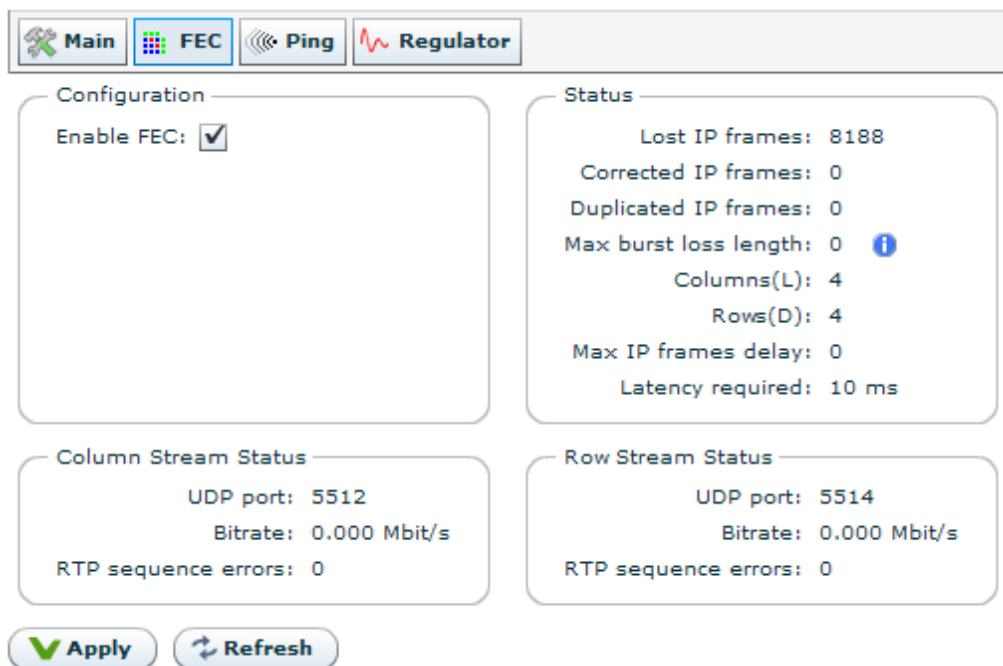
The maximum number of consecutive packets lost.

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.

9.5.2.3.1 FEC

The FEC sub page is shown in [Figure 9.50](#). This page displays the status of the forward error correction processing of the IP input.



The screenshot shows the following configuration and status information:

Section	Field	Value
Configuration	Enable FEC:	<input checked="" type="checkbox"/>
Status	Lost IP frames:	8188
	Corrected IP frames:	0
	Duplicated IP frames:	0
	Max burst loss length:	0 ⓘ
	Columns(L):	4
	Rows(D):	4
	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

Buttons: **Apply** (green checkmark), **Refresh** (circular arrow)

Figure 9.50 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 C](#).

9.5.2.3.2 Ping

The Ping sub page is shown in figure 9.51.



Figure 9.51 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.

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.

9.5.2.3.3 Regulator

The Regulator sub page is shown in figure 9.52.

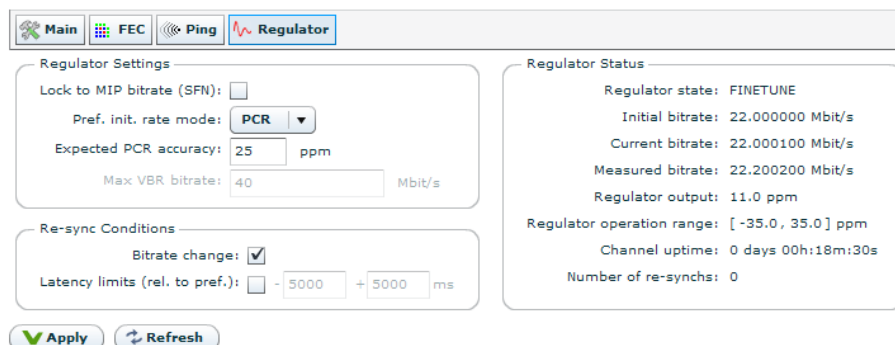


Figure 9.52 Regulator page

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

Lock to MIP bitrate (SFN)

Enable this to lock the ASI out rate to DVB-T MIP timestamp if a MIP is found in the stream.

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.

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 attempts to set up the regulator very fast on the expense of possible jitter on the output. For ASI output this may initially create jitter outside of the specification and should only be used when having IP -> IP transmission.

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 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](#)).

9.5.2.4 Services

The Services page 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 [9.53](#)).

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

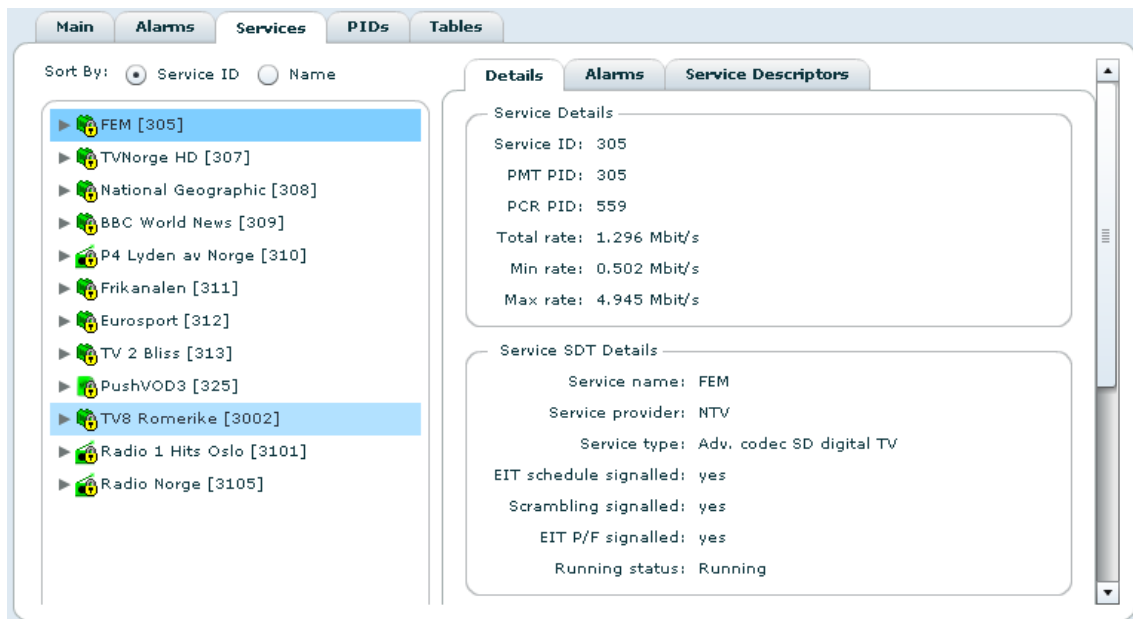


Figure 9.53 Service details overview when service list is not expanded.

Service ID

The service id of the selected service.

PMT PID

The program map table PID of the service.

PCR PID

The PCR PID of the service.

Total rate

The current bitrate of the service. The service bitrate is the sum of the bitrates of the PIDs pertaining to the service (PMT, PCR, ECMs and the component PIDs 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

The Alarms sub 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](#).

The Service Descriptors sub page is divided into two sections. The first section, Service Descriptors, shows a tree with all service descriptors (if present). The second section, SDT Descriptors, shows a tree containing all SDT descriptors (if present).

To list all components contained within a specific service click the arrow for the given service. The expanded view is shown in [Figure 9.54](#).

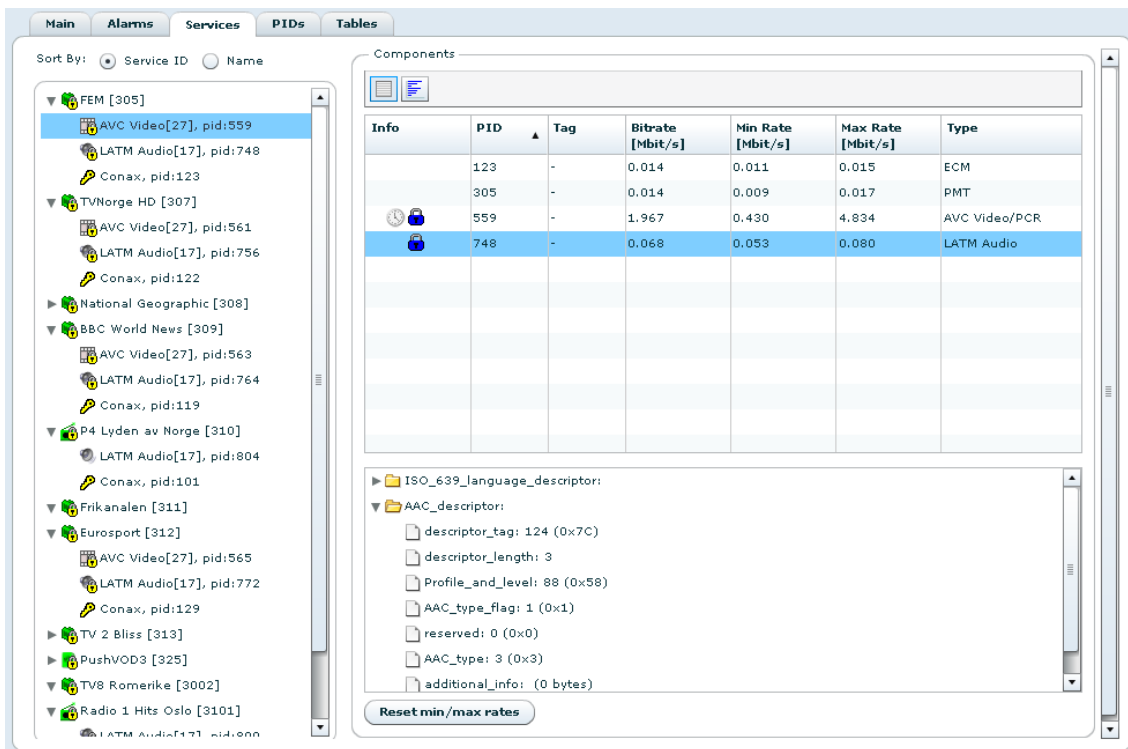


Figure 9.54 Service details full component overview

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 [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.

9.5.2.5 PIDs

This page gives detailed information about the PIDs present on the input. Two different PID views may be selected with buttons on the tool bar at the top of the page. 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	0.047	0.039	0.047	0	0		45643
	16	-	NIT	0.045	0.041	0.047	0	0		45643
	17	-	SDT/BAT	0.045	0.041	0.047	0	0		45643
	18	-	EIT	0.047	0.041	0.047	0	0		45643
	100	-	PMT	0.047	0.041	0.047	0	1		45643
	800	-	Video	3.975	3.595	4.016	0	1		3935668
	801	-	Audio/PCR	0.209	0.186	0.211	0	1		206370
	8191	-	Null Packets	0.083	0.059	0.164	0	0		75488

Figure 9.55 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 9.56 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 is a list of ECM packet streams containing descrambling information for this PID.

Count

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

Beneath the PID table are three buttons:

Reset CC error counts

This resets the CC error counters for all packet streams.

Reset min/max rates

This button resets the min and max bit rate measurements for all packet streams.

Reset packet counts

This button resets the packet counters for all packet streams.

The PID rate view is shown in figure 9.57. To the left is the bar chart showing the PIDs and 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 9.56 are shown if relevant.

Horizontally, 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.

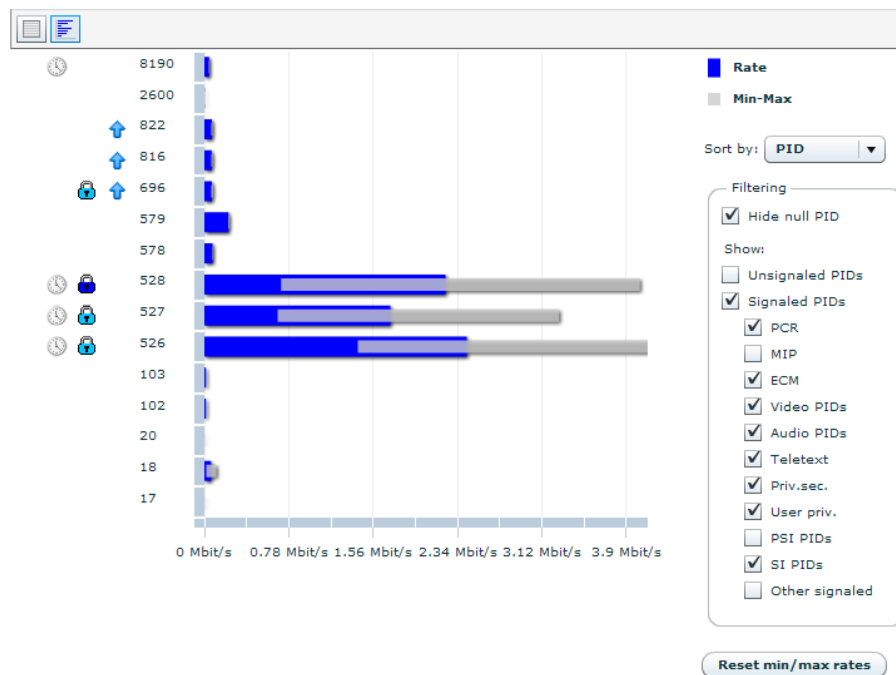


Figure 9.57 PID Details, rate view

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.

9.5.2.7 Tables

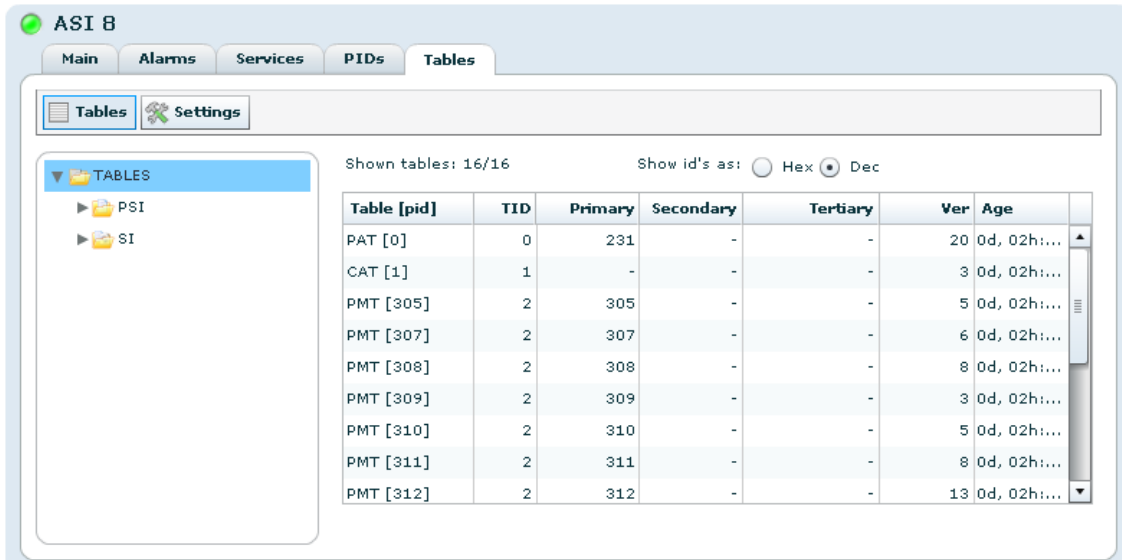


Figure 9.58 Table details, overview.

Figure 9.58 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.

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.

9.5.2.8 Settings

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 9.59 Table analysis configuration.

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 9.59 shows the page as displayed in DVB mode.

In ATSC mode the page looks different, as shown in figure **9.60**

Tables
Settings

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 CAT PMT TSDT

PSIP tables: MGT TVCT CVCT RRT STT

PIDs:	0	1	2-1	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

Apply
Refresh

Figure 9.60 Table analysis configuration in ATSC mode.

Note: Turning off analysis of certain tables may impact the output stream. Please make sure none of the tables you turn off analysis for are used by the output. See below for examples.

Examples:

- To be able to see the programs and do service filtering on an input port you must analyse at least PAT and PMT.
- To use the Playout Unchanged mode to play out a table on the output the table must be analysed on the selected input.
- To see the service name for the services you have to configure analysis of SDT_a (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 (EIT_{pfa}, EIT_{pfo}, EIT_{sa}, EIT_{so}). 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.

9.5.2.9 Sources

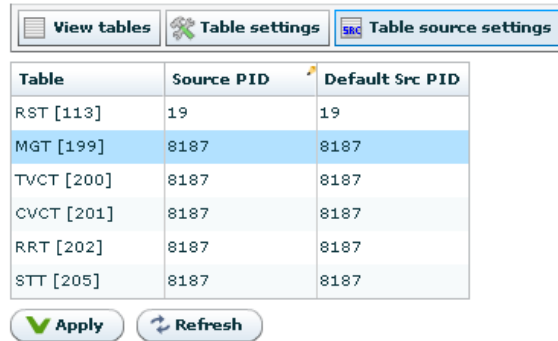


Table	Source PID	Default Src PID
RST [113]	19	19
MGT [199]	8187	8187
TVCT [200]	8187	8187
CVCT [201]	8187	8187
RRT [202]	8187	8187
STT [205]	8187	8187

Figure 9.61 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. This makes it possible to filter out “SDT other” on a PID of choice, while “SDT actual” is filtered on e.g. the default PID 17. “SDT other” can then be played out with the SI player and merged with “SDT actual” info on PID 17 on the output.

The page is shown in figure 9.61 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.

9.5.3 Switch

Information about the switches is displayed on a new page to the right by selection a switch. The top part of that page is common for all sub pages and shows the name and the current alarm status of the switch. Holding the mouse cursor over the alarm status indicator brings up a tool tip showing the current alarms on this switch.

Underneath the name of the switch is a tab navigator, which contains three sub pages, Main, Inputs and Alarms.

Main

This page shows a summary of the switch status, switch statistics and switch configuration.

Inputs

This page shows the switch input status and lets the user configure the switch inputs.

Alarms

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

In all sub-pages for a selected switch a list of current alarms for that switch is shown. The list is identical to the list displayed in the Current Status view, described in section **Section 9.3.1**.

9.5.3.1 Main

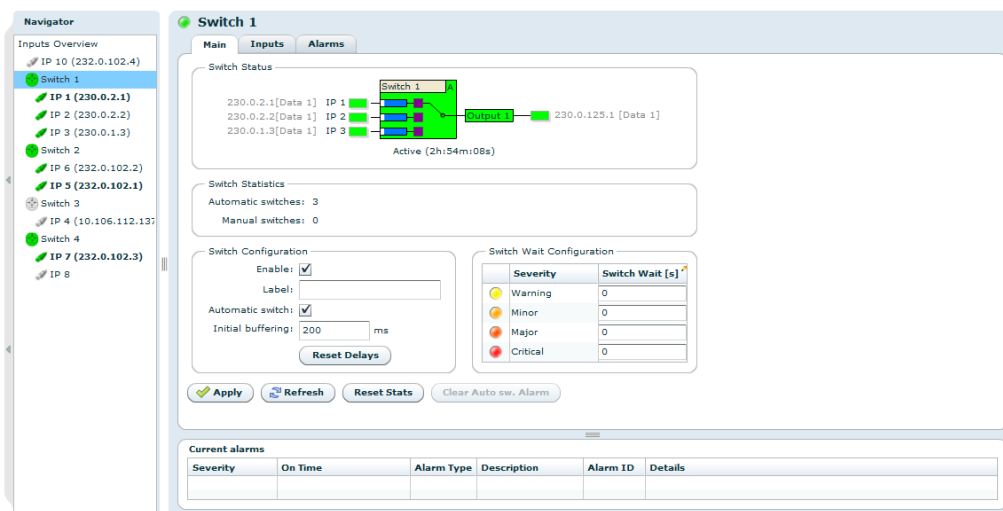


Figure 9.62 Switch - Main

Main tab provides the switch status, switch statistics, switch configuration as well as switch wait configuration.

Switch status field provides the status figure which shows the inputs/outputs of the switch, selected input and indicates the alarm level. Holding the mouse cursor over the status figure indicator brings up a tool tip displaying detailed information on the switch.

Switch statistics field indicates the number of automatic and manual switching that has been performed beginning from the boot up or the last reset statistics button has been pressed.

The switch configuration field has the following entries:

Enabled

Control enabling/disabling of the switch. When disabled the switch will have no output, and no matching will be performed.

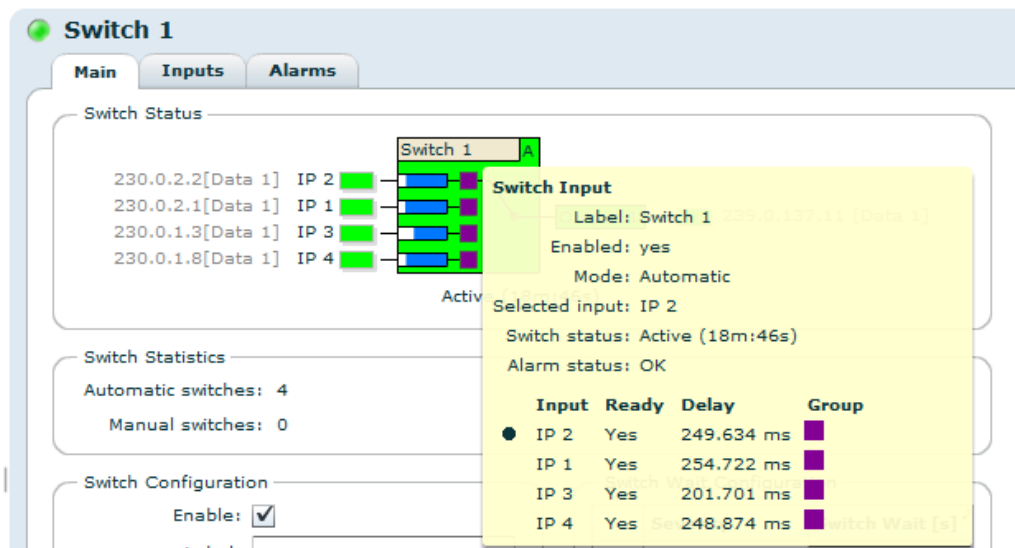


Figure 9.63 Switch Status

Label

This is the name of the switch. It is used as alarm source text, and shown in the web interface.

Automatic Switch

This sets the switching mode. When enabled, the unit will switch between inputs automatically based on alarm levels per input. Manual switching may be performed regardless of Automatic Switch enabled or not. Return switch (return to higher priority input automatically) can be configured at 'Switch Input Configuration' subpage. If disabled the unit will remember the selected input, even during power loss.

Initial Buffering

The purpose of initial buffering is to handle delay variations between the inputs during operation. In case the streams drift apart the buffers must be large enough to compensate for delay variations. For a new Initial Buffering value to be applied, Reset Delays (see below) must be initiated.

Reset Delays

Initiating Reset Delays should be initiated for the following reasons:

- Applying a new Initial Buffering value.
- Restoring initial input buffer values. This will typically be required if during operation either input has drifted and consumed all of its buffer. If this occurs an alarm will be triggered, and a larger Initial Buffering value should be applied to account for larger drifts.

By initiating Reset Delays, the switch will discard the currently measured delay between the input streams and find new delays. After a Reset Delays have been initiated the lagging input

will be buffered by the configured Initial Buffering value, while the other inputs will be buffered by the configured Initial Buffering value plus the delay difference compared to the lagging input.



Note: Resetting of the delay will cause a break in the output signal.

Switch Wait Configuration

The switch wait configuration is used to control the wait time from an alarm condition occurs until the switch is performed. The alarm settings applies to all inputs in a switch.

The only alarms considered for switching are the input alarms for the inputs of the switch. Generic device alarms and output alarms will not be considered.

It is possible to configure separate Switch Wait times per alarm level, such that for example an Critical alarm condition will trigger an immediate switch, while a Major alarm must be present for at least 20 seconds before a switch is performed.



Note: Many alarms have an off hysteresis to avoid rapid triggering of the same alarm. The “Off time” is a configurable parameter per alarm that defines how long an alarm will stay active after the last error condition have occurred. This must be taken into account when configuring the Switch Wait Configuration. See section [9.5.2.2](#) for further details.



Note: It is not possible to configure a shorter wait time for a less critical alarm. For example Switch Wait for Warning severity must be equal or higher than Switch Wait for Minor severity.

In order to commit the changes to the configuration, press Apply button at the bottom of the page. The Reset Stats button is used to clear statistics counters for the switches. The Clear Auto sw. Alarm button is used to clear the automatic switch alarms.

9.5.3.2 Inputs

Switch Input Status field shows an overview of the input streams currently attached to the specific stream. Figure [9.64](#) shows the graphical user interface of the switch input page. The following entries are listed:

Input

Lists the current inputs of the switch.

Alarm

Indicates the alarm state of each input.

Valid

This field indicates that the input stream is Valid. If Valid and not selected the input will

be considered the next time a switch is performed. If not Valid and selected the switch will try to switch to the highest prioritised input that is Valid. If the input is not valid, a reason will be stated.

Grp

The Match Group icon indicates which input streams that are equal. Streams that are equal contains the same TS packets in the same order, and the switch will be able to perform seamless switching between inputs belonging to the same Match Group. A seamless switch means that the output of the switch will be unaffected when the switch is performed. For a switch with 4 inputs, where 2 and 2 inputs are identical the switch will be able to create 2 match groups, with 2 inputs in each.



Note: If a switch will be seamless or not will not be considered when performing a switch. The first Valid input with the highest priority will always be selected when performing a switch. Instead make sure that identical inputs are next to each other in the prioritised list of inputs to get a seamless switch.

Delay

This field presents the applied delay in milliseconds to each input. For inputs belonging to the same Match Group (Grp) the delays will be set to compensate for the delay difference between the streams, while also applying the Initial Buffering value to the lagging input.



Note: The Delay of the selected input to the switch will always remain constant, while the delays of the other inputs will change if the input streams drifts relative to each other.

The screenshot shows the 'Switch 1' configuration page in the 'Inputs' tab. On the left, a 'Navigator' shows a tree of inputs including IP 10, Switch 1, Switch 2, Switch 3, Switch 4, and IP 8. The main area is divided into two sections:

- Switch Input Status:** A table showing the status of three inputs.

Input	Alarm	Valid	Grp	Delay [ms]
IP 1 (230.0.2.1)	●	Yes	■	200.000
IP 2 (230.0.2.2)	●	Yes	■	200.112
IP 3 (230.0.1.3)	●	Yes	■	201.400
- Switch Input Configuration (Prioritised Order):** A table for configuring the switch inputs.

Input	Return	Max severity	Return Wait
IP 1 (230.0.2.1)	<input checked="" type="checkbox"/>	Major [5]	0
IP 2 (230.0.2.2)	<input type="checkbox"/>	Major [5]	0
IP 3 (230.0.1.3)	<input type="checkbox"/>	Major [5]	0

At the bottom, there is a 'Current alarms' table with columns for Severity, On Time, Alarm Type, Description, Alarm ID, and Details.

Figure 9.64 Switch - Inputs

Switch Input Configuration shows a prioritised list of the switch inputs. This configuration reflects how the switch operates in Automatic switch mode. At the bottom of this field it is also

possible to add and remove inputs and also to perform manual switches. The following entries are present:

Input

Specifies the input streams to the switch. The top item in this list has the highest priority. On the right side there are two arrows to control the priority of the inputs of the switch.

Return

Specifies if the switch should try to return to the selected input if the input is considered valid. The switch will always try to choose the highest prioritised input that is ready and has the return field enabled.

Max severity

Max severity defines the maximum alarm severity an input can have to make it valid. The alarm severity in Alarms column under Switch Input Status will be compared against the Max severity parameter to decide if the input is Valid or not. If the alarm severity is lower than or equal to the specified severity, the input is considered Valid. For example if the Max severity is configured to Warning [3], any alarm severity worse (closer to Critical [6]) than Warning [3] will make this input **not** Valid as an input source of the switch.



Note: All alarms has a default alarm severity, but it may be reconfigured for each input. See section [9.5.2.2](#) for details.

Return wait

Specifies the minimum time to stay away from a previously used input before returning. For example if Return wait is configured to 20 seconds, and the switch switches away from the input, the input will not be considered valid again until 20 seconds have passed. This may be used to avoid rapid switches between inputs.



Note: Return wait does not apply if the switch was a Return switch.

9.5.3.3 Alarms

The Alarms sub page allows the user to configure the alarms for the input switch. It works identically to and is described under Device Alarms in section [9.4.2.1](#).

9.6 Outputs

The Outputs page contains all information and settings that apply to the output ports of the device. The navigation list to the left lets the user select which IP output or Switch output to view, or to select Outputs Overview to view a summary of all the outputs of the device.

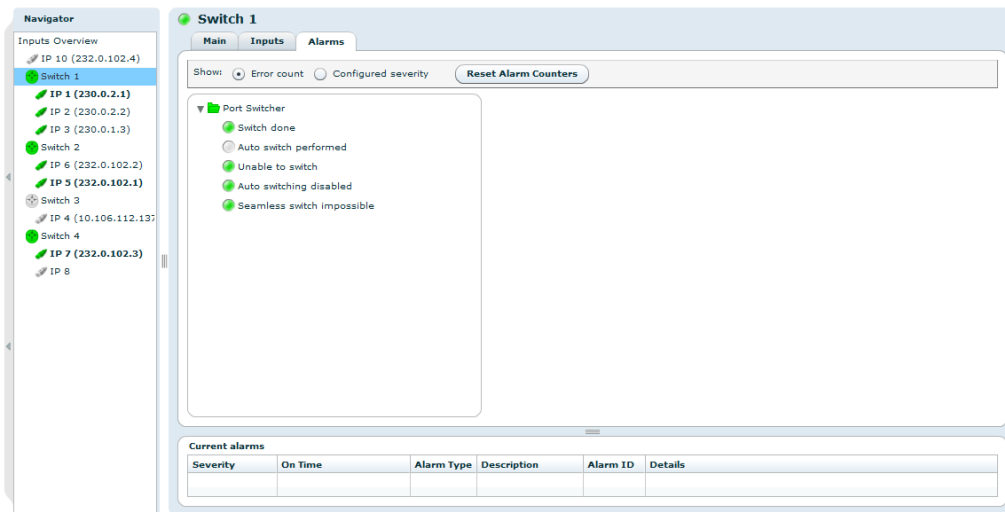


Figure 9.65 Switch - Alarms

9.6.1 Outputs overview

This page shows a short summary of all the IP Outputs allocated to each 'Switch'.

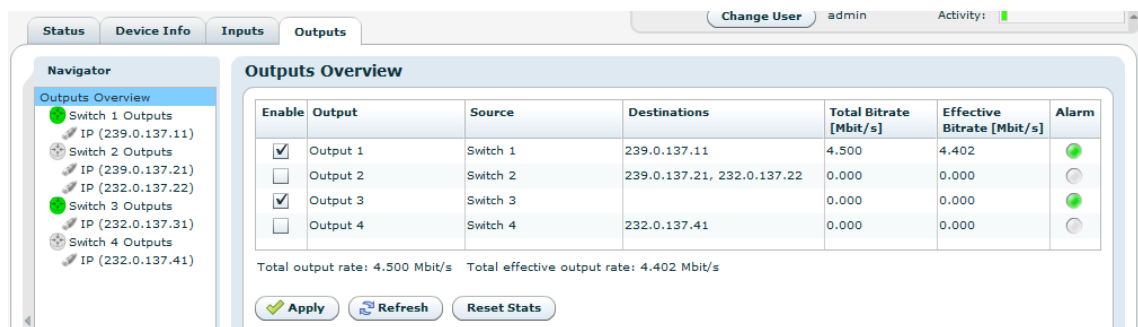


Figure 9.66 Outputs overview

The table has the following columns:

Enable

This shows whether the output is enabled or not. The output enabled or disabled for an output by clicking this check box and hitting apply.

Output

The name of the output.

Source

This indicates which switch is sourcing the output port.

Destination

The output destination: IP interface address.

Total Bitrate

The total bitrate of the transport stream currently transmitted on the output in Mbit/s.

Effective Bitrate

The effective bitrate (total minus null packets) of the transport stream currently transmitted on the output in Mbit/s.

Alarm

The current alarm status of the output is shown as a coloured circle.

9.6.2 (Switch) Output

When selecting an output a new page on the right hand side with information about the selected output is displayed. The top part shows the name and the current alarm status of the output. See figure [Figure 9.67](#). All current alarms related to the output are displayed in a tool tip by holding the mouse cursor over the alarm status indicator.

The tab navigator contains two sub-tabs:

Main

This page lets the user configure several parameters of to the chosen output.

Alarms

This page displays the status of all alarms on the output, and lets the user override the severity of these alarms.

9.6.2.1 Switch Main

The Switch Main page shows the switch status and lets the user configure the IP destinations for the switch.

The Switch Status field provides the graphical presentation of the inputs/outputs of the switch, selected input and the alarm level. Holding the mouse cursor over the status figure indicator brings up a tool tip displaying detailed information on the switch.

If the units is equipped with ASI connectors there will be a frame showing ASI configuration and a list of current ASI outputs from the current switch.

The ASI Outputs Configuration field:

ASI mode

Set transmission format for the ASI output, either Spread or Burst mode.

Packet length

Set TS packet length. 188 or 204 bytes. If using 204 bytes packets and having 188 bytes on the input, the unit will insert 0xff in the 16 last bytes.

The ASI Outputs field shown in [figure 9.68](#) lists the current ASI outputs of the selected switch.

Add ASI output

Add ASI output copies to this switch. In total there are 4 ASI outputs, and it is possible to assign all outputs to one switch. ASI outputs may however not be chosen entirely freely. An ASI output can not be the output of a switch if the corresponding ASI input is the source of another switch. 1.Out is the corresponding output to 1.In and so on. This limitation is present to ensure that the outputs have a logic output on power loss. If the

Navigator

Outputs Overview

- Switch 1 Outputs
 - 1.Out
 - 2.Out
 - IP (10.0.0.3)
 - IP (10.0.0.2)
- Switch 2 Outputs
- Switch 3 Outputs
- Switch 4 Outputs
 - 3.Out
 - 4.Out

Output 1

Switch Main | Alarms

Switch Status

230.0.0.1[Data 1] IP 1
230.0.0.2[Data 1] IP 3
2.In
1.In

Switch 1

Output 1

1.Out
2.Out
10.0.0.3 [None]
10.0.0.2 [None]

Active (2 days 11h:58m:31s)

ASI Outputs Configuration

ASI mode: Burst Spread
Packet length: 188 204

IP Outputs Configuration

TS packets per frame:

ASI Outputs

Port	Bitrate [Mbit/s]
1.Out	10.790
2.Out	10.790

+ Add ASI Output - Set to Passive

IP Destinations

Enable	Interface	Destination	Bitrate [Mbit/s]
<input checked="" type="checkbox"/>	None	10.0.0.3:5500	29.180
<input checked="" type="checkbox"/>	None	10.0.0.2:5500	23.500

+ Add Destination - Remove Destination

Apply Refresh

Figure 9.67 Output main page

ASI Outputs

Port	Bitrate [Mbit/s]
1.Out	11.056
2.Out	11.056

+ Add ASI Output - Set to Passive

Figure 9.68 Multiple ASI destinations

corresponding input is not used as a switch source, the corresponding output may be set freely as the output of any switch.

Set to Passive

Setting an ASI output to passive automatically removes the output from the switch, and sets the output to passive mode. The output will then be directly wired to its corresponding input. For example removing output 4.Out will wire it directly to 4.In. If there is a signal on 4.In, this signal will be transmitted on 4.Out. This will also be the case even if 4.In is used as a source for any other switch.

The IP Outputs Configuration field:

TS packets per frame

Sets the number of transport packets that will be included in an Ethernet frame. The maximum number is 7 to avoid fragmentation of the resulting IP packets.

Enable	Interface	Destination	Bitrate [Mbit/s]
<input checked="" type="checkbox"/>	Data 2	225.0.2.2:5500	23.027
<input type="checkbox"/>	Control	0.0.0.0:5500	0.000

Figure 9.69 Multiple IP destinations

The IP Destinations field has a table view ([Figure 9.69](#)) containing a tick box to enable or disable each output in addition to showing the status of each output. Each output is configured in the dedicated page, reached by double-clicking on the entry in the table.

Removing an IP destination is done by highlighting the output to delete, clicking Remove Destination and then clicking Yes in the pop-up box. This is exactly the same as selecting the appropriate IP destination in the navigator list.

9.6.2.2 Alarms

The Alarms page lets the user configure and view the status of all alarms belonging to the selected output. The page functions exactly like the input alarms page, except it is not possible to copy settings from a different output. (See [Section 9.5.2.2](#)).

9.6.3 Output to IP destination

If an IP destination has been allocated to a 'Switch' this is shown in the Outputs navigator list. Clicking the navigator entry opens the page to edit the IP destination settings.



Note: The IP output must be added before configuring it. Refer to [Section 9.6.2.1](#).

This page consists of the sub tabs Main and Ping. If Forward Error Correction has been enabled the FEC tab is also visible.

9.6.3.1 Main

This page is shown in [Figure 9.70](#).

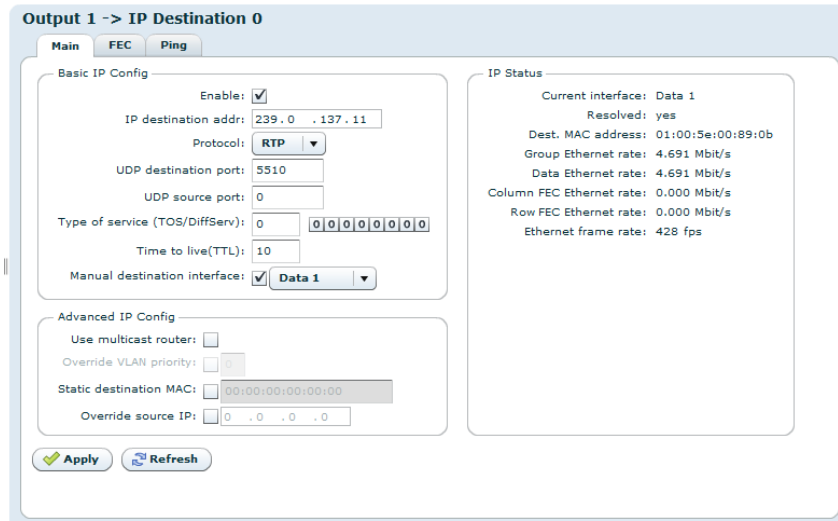


Figure 9.70 IP Configuration.

The Basic IP Config field:

Enable

If this box is checked, the generated transport stream will be played out over IP using the shown parameters.

IP destination addr

Enter the destination IP address to use when transmitting data over IP. The address may be either a unicast address or a multicast address.

Protocol

Select UDP or RTP transmission mode. See [Section 6.1.1](#) for more information on this.

UDP destination port

Enter the UDP destination port to use when transmitting data over IP. The UDP destination port is used by the receiver to separate one stream from another. UDP port numbers are in the range 1-65535.



Warning: Please ensure that there is no conflict in UDP ports in use. Pay special attention to the fact that FEC data are always sent on UDP ports two higher than the media port and four higher than the media port, e.g., if the UDP destination port is 5510, column FEC UDP port is 5512 and row FEC UDP port is 5514.

UDP source port

Enter the UDP source port to be used in the outgoing UDP frames. UDP port numbers

are in the range 1-65535. Note that the receiver unit may not check the source port when receiving streams. FEC frames are transmitted using the same UDP source port as the media frames.

Type of service (TOS)

Enter Type of Service parameter as a byte value to be set in the Type-of-Service (TOS) field in the IP header as specified in RFC-791. This parameter is used for Class-of-Service prioritisation. Its usefulness depends on routers honouring this field. Please refer to [Appendix D](#) "Quality of service – Setting Packet priority" for further details.

Time to Live (TTL)

Enter Time to Live parameter as a byte value to be set in the Time to Live (TTL) field in the IP header as specified in RFC-791.

Manual destination interface

If you want to manually set the interface you want the data to be transmitted through, check the box and select the wanted interface. If you wish to use the IP routing configuration leave the box unchecked.

The Advanced IP Config field:

Use multicast router

Click this box to enable use of multicast router. The address of the multicast router is the same for the entire unit and is configured in the Network sub-page of the Device Info page. When this option is enabled, the MAC address used when configuring a multicast destination IP address will be resolved to the IP address of the multicast router. If not using the multicast router option, multicast addresses automatically resolve to dedicated multicast MAC addresses.

Override VLAN priority

Priority is normally configured per VLAN interface. It is possible to override the VLAN priority field for the output stream by checking this box and entering a new priority value.

Static destination MAC

Static MAC destination address is used to specify a fixed MAC destination address in outgoing streams. This makes it possible to transmit to a destination host over a one-way link. The static MAC address setting then replaces the normal ARP lookup. To enable static MAC, check the box and enter a destination MAC address.

Override source IP

Option to use a different IP address than the one on the Ethernet interface when transmitting IP frames with transport stream data.

The IP Status field provides real time status information pertaining to the selected output.

Current interface

The interface the IP stream will be transmitted through. If Manual destination interface is enabled the configured interface will be shown. If not, the interface depends on the configured destination address and the configured IP routing entries.

Resolved

Yes when the MAC address of the configured IP destination address is resolved. The parameter is always Yes when multicast is used without a multicast router. No when the MAC address is not yet resolved by ARP lookup.

Dest. MAC address

Shows the destination MAC address used for the stream. This may be the MAC address of the receiving unit, or the gateway if the receiving unit is on another network. If using a multicast destination IP address without enabling multicast router, the field shows the multicast MAC address corresponding to the configured multicast group. In the case of multicast router, the MAC address resolved for the multicast router is shown. When the address is still not resolved this field displays the value 00:00:00:00:00:00.

Group Ethernet rate

The bitrate of the IP frames containing this MPEG-2 transport stream and any FEC data related to this stream.

Data Ethernet rate

The bitrate of the MPEG-2 transport stream contained in the IP stream.

Column FEC Ethernet rate

The bitrate of the column FEC contribution to the IP data.

Row FEC Ethernet rate

The bitrate of the row FEC contribution to the IP data.

9.6.3.2 FEC

This page allows configuring and applying forward error correction data to the output IP transport stream.

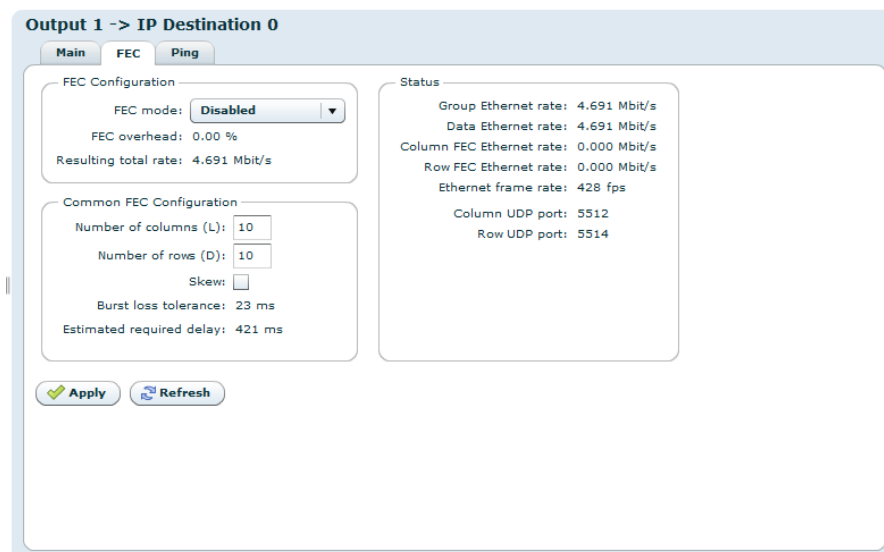


Figure 9.71 IP output FEC page

In the FEC Configuration field forward error correction is enabled and configured for each individual output:

FEC mode

From the pull-down list select Disabled to not apply FEC, Column only to apply one-dimensional FEC (i.e. add column FEC datagrams, only), or Column and Row to apply two-dimensional FEC (i.e. add column and row FEC datagrams).

FEC overhead

Gives an instant check of the overhead resulting from the applied FEC.

Resulting total rate

Shows the actual bit rate of the IP stream including FEC, if applied.

The Common FEC Configuration field allows setting of common parameters that will be applied to the FEC processor in general:

Number of columns (L)

The number of columns used in generating the Row FEC data.

Number of rows (D)

The number of rows used in generating the Column FEC data.

Skew

Check this box to enable a skewed FEC matrix.

For a detailed description of FEC usage, refer to [Appendix C](#).

The Status field shows the IP status resulting from adding FEC processing:

Group Ethernet rate

The bitrate of the IP frames containing this MPEG-2 transport stream and any FEC data related to this stream.

Data Ethernet rate

The bitrate of the MPEG-2 transport stream contained in the IP stream.

Column FEC Ethernet rate

The bitrate of the column FEC contribution to the IP data.

Row FEC Ethernet rate

The bitrate of the row FEC contribution to the IP data.

Column UDP port

The UDP port used for column FEC data.

Row UDP port

The UDP port used for row FEC data.

9.6.3.3 Ping

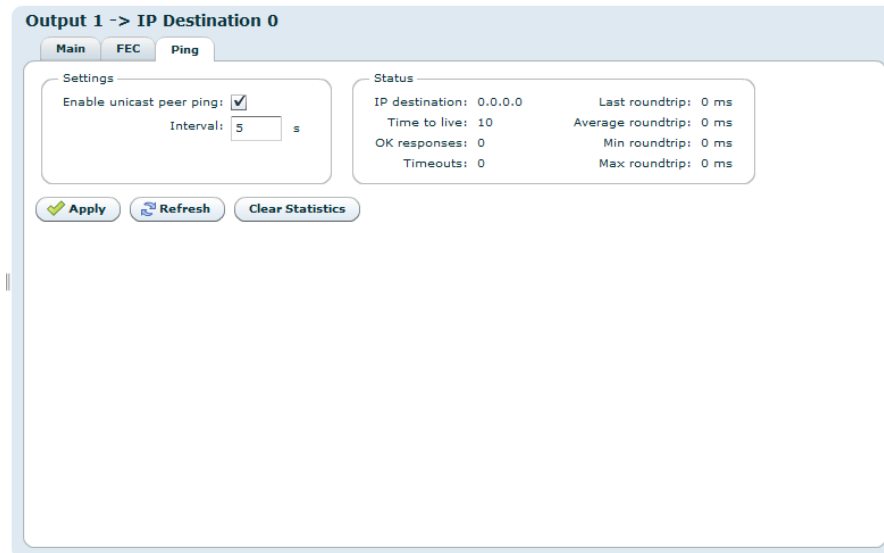


Figure 9.72 Ping page

Ping can be used to resolve network problems, avoid flooding and avoid time-out of MAC address lookup by the transmitter or a specific network component on the way to the receiver. Ping helps resolving such issues by sending a short message regularly. This feature also makes it possible for the receiver to monitor if an active sender is present.

The Settings field:

Enable Unicast Peer Ping

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

Interval

Set the interval in seconds between each Ping.

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.

Clicking the Clear Statistics button resets the counts in the Status field.

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 with the prefix VIGW-PROD.

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-SWITCH-MIB

This MIB contains parameters related to control of automatic redundancy switches. It is supported by products that have at least one type of redundancy switch controller, for example an automatic input switcher or an automatic service switcher. Parameters include:

- Control of currently selected input
- Control of switch controller mode

VIGW-PLAT-IPTRANSPORT-MIB

This MIB contains tables that relate to reception and transmission of streams over IP networks. The tables are independent of the payload format of the streams. The MIB is supported by products that support transmission and/or reception of streams over IP networks. Examples of information included are:

- Control of IP destination address for transmitted stream
- Control of UDP ports
- Status reporting of bit-rates and packet loss

VIGW-PLAT-VIDEO-MIB

This MIB contains tables and settings to configure video-specific processing. It is supported by products that relate to digital video streams, for example JPEG2000-based encoding/decoding products.

Examples of included information are:

- Control of video encoding parameters
- Control of video decoding parameters

VIGW-PLAT-RF-MON-MIB

This MIB contains tables and settings to configure RF-specific parameters. It is supported by products that relate to RF monitoring of DVB-T/T2 signals. Parameters include:

- Configuration of RF input signal and measurement settings
- RF status, DVB-T/T2 status and PLP status on individual RF channel inputs

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

<code>unitAlarmStatusChanged</code>	This trap is sent when the top level unit alarm status (indicated by the <code>unitAlarmStatus</code> variable) changes. The trap indicates both the old and new alarm level. Transmission of this trap type can be enabled/disabled through configuration.
<code>unitAlarmAsserted</code>	This trap is sent when an internal alarm is raised. No <code>subid3</code> information is included. A corresponding <code>unitAlarmCleared</code> trap is sent when the alarm cause is cleared.
<code>unitAlarmCleared</code>	This trap is sent when an alarm condition previously indicated with <code>unitAlarmAsserted</code> is cleared.
<code>unitAlarmEvent</code>	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".
<code>unitDetailedAlarmAsserted</code>	This trap is a more detailed version of <code>unitAlarmAsserted</code> . <code>subid3</code> information is included in addition to the basic parameters defined in <code>unitAlarmAsserted</code> .
<code>unitDetailedAlarmCleared</code>	This trap is sent when an alarm condition previously indicated with <code>unitDetailedAlarmAsserted</code> is cleared.
<code>unitDetailedAlarmEvent</code>	This is a more detailed version of <code>unitAlarmEvent</code> . <code>subid3</code> information is included in addition to the basic parameters defined in <code>unitAlarmEvent</code> .

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 Variables in SNMPv2 traps and their meanings

Field	Description
<code>unitEventSeverity</code>	This field indicates the severity of the alarm, 2-6. 1 will never be used, as this condition is indicated by transmitting a <code>unitAlarmCleared</code> message.
<code>unitEventAlarmType</code>	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 <code>subid1</code> and <code>subid2</code> values in the message.
<code>unitEventAlarmId</code>	A unique identifier for this alarm type. Refer to alarm documentation in the user manual for values.
<code>unitEventAlarmName</code>	A fixed name corresponding to the alarm id.
<code>unitEventRefNumber</code>	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.
<code>unitEventSubId1</code>	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.
<code>unitEventSubId2</code>	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.
<code>unitEventSubId3</code>	This field provide an even more detailed description of the alarm source. This field is only present in the "detailed" type of trap messages (<code>unitDetailedAlarmAsserted</code> , <code>unitDetailedAlarmEvent</code>). It's usage is dependent on the alarm ID. For example, in transport stream related alarms, <code>subid3</code> is used to indicate the PID value that caused the alarm.
<code>unitEventSourceText</code>	A textual description of the source of the alarm. This is typically a textual description of the <code>subid1</code> and <code>subid2</code> fields. For example, for transport stream related alarms, the text indicates the name (with label) of the port that generated the alarm.
<code>unitEventSubId3Label</code>	This field is fixed and indicates the label (meaning) of the <code>subid3</code> field, contained in the <code>unitEventSubId3</code> variable. It is intended to make it easy to log the alarm.
<code>unitEventDetails</code>	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.
<code>unitAlarmStatus</code>	This variable contains the new, top level alarm status of the unit <i>after</i> the condition leading to this trap message. It may be used to quickly update the top level status for the device after receiving the trap message.

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

<code>alarmCleared</code>	This trap is sent when an alarm goes off (i.e. is cleared) in the system. The binding <code>unitTrapHistoryRefNumber</code> matches the corresponding <code>unitTrapHistoryRefNumber</code> in the “raise” trap message.
<code>alarmIndeterminate</code>	This trap is sent when an alarm with severity level “notification” (level 2) is generated.
<code>alarmWarning</code>	This trap is sent when an alarm with severity level “warning” is generated.
<code>alarmMinor</code>	This trap is sent when an alarm with severity level “minor” is generated.
<code>alarmMajor</code>	This trap is sent when an alarm with severity level “major” is generated.
<code>alarmCritical</code>	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.

11 Preventive Maintenance and Fault-finding

This chapter provides the schedules and instructions, where applicable, for routine inspection, cleaning and maintenance of the TNS544, to be carried out by the operator of the unit.

11.1 Preventive maintenance

11.1.1 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.

11.1.2 Cleaning

- Remove power from the unit.
- Clean the external surfaces of the TNS544 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.

11.1.3 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 T-VIPS.

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

11.1.4 Warranty

The TNS544 is covered by standard T-VIPS 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 T-VIPS Customer Service Help Line

The warranty does not cover any engineering visit(s) to the customer premises.

11.2 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 T-VIPS 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 T-VIPS customer care.

11.2.1 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 T-VIPS Customer Support. Switch off the equipment if it becomes unusable, or to protect it from further damage.

11.2.2 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 TNS544 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 TNS544. Call a Service Engineer.
 - No
The problem lies with the cable. Replace the cable.

The PSU does not have any internal user changeable fuses.

11.2.3 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.

11.3 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.

11.4 Returning the unit

Before shipping the TNS544 to T-VIPS, contact your local T-VIPS reseller or T-VIPS directly for additional advice.

1. Write the following information on a tag and attach it to the TNS544.
 - Name and address of the owner
 - Model number
 - Serial number
 - Description of service required or failure indication.
2. Package the TNS544.
 - The original shipping containers or other adequate packing containers must be used.
3. Seal the shipping container securely, and mark it FRAGILE.

Appendix A Glossary

\$label ch_glossary1000Base-T

The term for the electrical Gigabit Ethernet interface. This is the most common interface for Gigabit Ethernet. Most Gigabit-enabled PCs and equipment support this interface.

3G-SDI

3Gbit High Definition - Serial Digital Interface. 3G-SDI, consisting of a single 2.970 Gbit/s serial link, is standardized in SMPTE 424M that can replace the dual link HD-SDI.

ARP

Address Resolution Protocol. A protocol used to “resolve” IP addresses into underlying Ethernet MAC addresses.

ATSC

Advanced Television Systems Committee. An American organisation working with standardisation of digital television broadcasts, primarily in the US but also in Asia and other parts of the world.

DiffServ

Differentiated Services. A mechanism used on layer 3 - e.g. the IP layer - to differentiate between traffic of various types. DiffServ is based on the ToS field and provides a mechanism for the network to give e.g. video traffic higher priority than other traffic (for example Internet traffic).

DVB

Digital Video Broadcasting. The European consortium defining standards for transmission of digital TV broadcasts, primarily in Europe.

DVB ASI

Digital Video Broadcasting Asynchronous Serial Interface. A common physical interface for transmission of MPEG2 Transport Streams (i.e. MPEG2-compressed video) over a serial interface, typically coaxial cables.

DWDM

Dense Wavelength Division Multiplexing. A mechanism to increase the bandwidth available in an optical fiber by adding extra signals using different optical wavelengths (colours).

Ethernet

Originally a 10 Mbit/s shared medium network type developed by Xerox. Later transformed into an official standard. Nowadays, most Ethernet networks are based on full duplex connections over twisted pair cables. Ethernet switches in the network take care of routing Ethernet frames between nodes. The speeds now supported are 10 Mbit/s, 100 Mbit/s and 1000 Mbit/s. 10Gigabit/s Ethernet networks are now emerging.

FEC

Forward Error Correction. A mechanism to protect data transmission by adding redundant

information. Increasing the amount of redundant data will enable the receiver to correct more errors (i.e. regenerate lost packets) in case of network data loss.

HD-SDI

High Definition - Serial Digital Interface. Also known as ANSI/SMPTE SMPTE 292M-1998. A specification describing how to digitize and transmit uncompressed high definition video signals. The typical bit rate of an HD-SDI signal is 1485 Mbit/s.

HDTV

High Definition Television. Television standard(s) that provide(s) improved picture resolution, horizontally and vertically, giving clearer and more detailed TV pictures.

HTTP

HyperText Transfer Protocol. The fundamental protocol used on the Internet for transmission of WEB pages and other data between servers and PCs.

ICMP

Internet Control Message Protocol. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation.

IGMP

Internet Group Management Protocol. IGMP is a protocol used to manage multicast on the Internet. For a host (receiver unit) to receive a multicast, it needs to transmit IGMP "join" messages in the right format. Three versions exist. IGMPv2 is commonly used today, but IGMPv3 is the next step.

JPEG2000

A wavelet-based image compression standard. It was created by the Joint Photographic Experts Group committee with the intention to supersede their original discrete cosine transform-based JPEG standard. JPEG2000 can operate at higher compression ratios without generating the characteristic 'blocky and blurry' artifacts of the original DCT-based JPEG standard.

Meta-data

Meta-data is descriptive data that is "tagged" to a movie or audio clip. Meta-data is essential for the broadcaster.

MPEG-2

Moving Picture Experts Group 2. The compression standard used today on most satellite and cable TV digital broadcasts. MPEG-2 also includes standardisation of data transport of video using other compression techniques, and other types of information.

MPLS

Multi-protocol Label Switching. A Quality of Service mechanism for IP networks that allows IP packets to flow along a predefined path in a network, improving the reliability and robustness of the transmission.

MPTS

Multi Program Transport Stream. MPEG2 transport stream that carry multiple TV/Radio services.

Multicast

An IP mechanism that allows transmission of data to multiple receivers. A multicast can also have several transmit sources simultaneously. In video applications, multicast is typically used to distribute a video signal from a central source to multiple destinations.

MXF

Material eXchange Format is a container format for professional digital video and audio media defined by a set of SMPTE standards.

NMS

Network Management System. A system used to supervise elements in an IP network. When a device reports an alarm, the alarm will be collected by the NMS and reported to the operator. NMS systems typically collect valuable statistics information about the network performance and can provide early warning to the operator of network issues.

PCR

Program Clock Reference. A sampled 27 MHz video clock used in MPEG2 Transport Streams. The primary purpose of the PCR is clock synchronisation of transmitter and receivers.

PID

Packet Identifier. An 11 bit field in an MPEG2 transport packet defining a logical channel. 8192 unique logical channels may coexist in one network.

PSI/SI/PSIP

Program Specific Information / Service Information. These are information tables (meta-data) carried in MPEG2 transport streams in addition to video and audio. The information carried is typically service/program IDs, program names and conditional access information.

QAM

Quadrature Amplitude Modulation. A digital modulation type that is used for transmission of digital TV signals over cable networks (e.g. DVB-C) or terrestrial networks (e.g. DVB-T).

QoS

Quality of Service. A common term for a set of parameters describing the quality of an IP network: Throughput, availability, delay, jitter and packet loss.

QPSK

Quadrature Phase-Shift Keying. A modulation type frequently used for transmission of digital TV signals.

RIP2

Routing Information Protocol v2. A protocol used between network routers to exchange routing tables and information.

RSVP

ReSerVation Protocol. A Quality-of-service oriented protocol used by network elements to reserve capacity in an IP network before a transmission session takes place.

RTP

Real-time Transfer Protocol. A protocol designed for transmission of real-time data like video and audio over IP networks.

SD-SDI

Standard Definition Serial Digital Interface. Also known as ANSI/SMPTE 259M-1997 or ITU-R BT.656. A specification describing how to digitize and transmit uncompressed standard definition video signals. The typical bit rate of an SD-SDI signal is 270Mbit/s.

SDI

Serial Digital Interface. Used to describe both HD-SDI and SD-SDI input and output ports.

SDP

Session Description Protocol. A protocol describing multimedia communication sessions for the purposes of session announcement, session invitation, and parameter negotiation. SDP is typically used to describe an ongoing multicast; for example the type of compression used, IP addresses etc.

SDTI

Serial Data Transport Interface. A mechanism that allows transmission of various types of data over an SDI signal. This may be one or more compressed video signals or other proprietary data types. The advantage of SDTI is that existing SDI transmission infrastructure can be used to transport other types of data.

SDTV

Standard Definition Television. The normal television standard/resolution in use today.

SFP

Small Form-factor Pluggable module. A standardized mechanism to allow usage of various electrical or optical interfaces to provide Gigabit Ethernet. Several types of SFP modules exist: Single mode fiber modules for long-distance transmission and multi mode fiber modules for shorter distances. SFP is also known as "mini-GBIC".

SIP

Session Initiation Protocol. The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, used for controlling multimedia communication sessions such as voice and video calls over IP. The protocol can be used to create, modify and terminate unicast or multicast sessions consisting of one or several media streams.

SNDU

Sub Network Data Unit. Protocol Data Units (PDUs), such as Ethernet Frames, IP datagrams, or other network-layer packets used for transmission over an MPEG-2 Transport Multiplex, are passed to an Encapsulator. This formats each PDU into an SNDU by adding an encapsulation header and an integrity check trailer. The SNDUs are fragmented into one or a series of MPEG-2 Transport Stream (TS) packets and sent over a single TS logical channel.

SNMP

Simple Network Management Protocol. A fundamental and simple protocol for management of network elements. Commonly used by Network Management Systems and other applications.

SNTP

Simple Network Time Protocol is an Internet protocol used to synchronize the system clocks of computers to a time reference. It is a simplified version of the protocol NTP protocol which is overcomplicated for many applications.

SPTS

Single Program Transport Stream. MPEG2 Transport Stream that contains a single program/service.

TCP

Transmission Control Protocol. A “reliable” protocol above the IP layer that provides automatic retransmission of datagrams in case of packet loss, making it very robust and tolerant against network errors. TCP is the fundamental protocol used in the Internet for WEB traffic (HTTP protocol). TCP is intended for point-to-point pcommunication; TCP cannot be used for communication from one node to many others.

TCP/IP

A common term used for the Internet protocol suite, i.e. the set of protocols needed for fundamental IP network access: TCP, IP, UDP, ARP etc.

ToS

Type of Service. This is a field in the header of IP datagrams to provide various service types. It has now been “taken over” and reused by DiffServ.

Transport Stream (TS)

The common name for an MPEG2 Transport Stream. A bit stream used to carry a multiplex of packets, each identified by a unique Packet Identifier (PID) defining a logical channel. A PID stream typically represents a video or an audio service.

UDP

User Datagram Protocol. An “unreliable” protocol above the IP layer that also provides port multiplexing. UDP allows transmission of IP data packets to several receiving processes in the same unit/device. UDP is used in multicast applications.

Unicast

Point-to-point connection. In this mode, a transmit node sends e.g. video data direct to a unique destination address.

VLAN

Virtual Local Area Network, a network of units that behave as if they are connected to the same wire even though they may be physically located on different segments of a LAN.

Watermarking

A mechanism to “stamp” video content with unique marks, making it possible to trace the origin of illegally distributed content. Watermarks are invisible to the viewer.

XML

eXtensible Markup Language. A common self-describing text-based data format. Used for many purposes: Meta-data, configuration files, documents, etc. The readability of the format has made it very popular and is now the basis of many types of WEB services.

Appendix B Technical Specification

B.1 Physical details

B.1.1 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

B.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

B.2 Environmental conditions

Table B.1 Environmental specification

Operating temperature	0 to +50 °C
Storage temperature	-20 to +70 °C
Relative humidity	5 % to 95 % (non-condensing)
Handling/movement	Designed for fixed use when in operation

B.3 Power

B.3.1 AC Mains supply

Table B.2 AC Power
Supply Specification

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

B.3.2 DC supply

Table B.3 DC Power
Supply Specification

Rated voltage	48 VDC
Voltage tolerance limits	36-72 VDC
Power consumption	< 60 W

Table B.4 Physical details

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

B.4 Input/output ports

B.4.1 DVB ASI port

Table B.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

B.4.2 Ethernet management port

Table B.6 Ethernet Management Port Specification

Type	10/100Base-T
Connector type	RJ45

B.4.3 Ethernet data port

Table B.7 Ethernet Data Port Specification

Type	10/100/1000Base-T
Connector type	RJ45

Table B.8 Optional SFP Ethernet Data Port Specification

Type	Gigabit Ethernet, 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).
-------------	---

B.4.4 Serial USB interface

Table B.9 USB port specification

USB 1.1
Compatible with USB 2.0
Mini USB Connector

B.5 Alarm ports

B.5.1 Alarm relay/reset port specification

Table B.10 Alarm Relay and Reset Port Specification

Connector type	9-pin DSUB Male
Relay rating	0.1 A max, 50 VDC max
Relay minimum load	10 μ A at 10 mVDC
Reset activation time	8 seconds

Table B.11 Alarm Relay and Reset Port Pin Out

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

B.6 External reference

B.6.1 10MHz/1 PPS input

Connector type BNC 50 Ω socket

B.7 Compliance

B.7.1 Safety

The equipment has been designed to meet the following safety requirements: [Table B.12](#).

Table B.12 Safety requirements met.

EN60950 (European)	Safety of information technology equipment including business equipment.
IEC 60950 (International)	Safety of information technology equipment including business equipment.
UL 1950 (USA)	Safety of information technology equipment including business equipment.

B.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.

B.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.

B.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 C Forward Error Correction in IP Networks

The normal operational mode of the public internet is that IP packets are forwarded using a “best effort” strategy implying that packets may occasionally be lost due to excessive load. To regulate the transport rate of an IP session a transmitting host will at session start ramp up the speed until the receiver starts to loose packets. The receiver will send acknowledgments as it receives packets. In the case of packet loss the source will re-transmit a packet and slow down transmission rate to a level where packets are no longer lost. This is inherent in the commonly used protocol TCP (Transmission Control Protocol).

In an IP network for broadcast signals however, this mode of operation becomes impractical since packet delay from source to receiver resulting from re-transmission amounts to three times the normal. It is also impractical for multicast as each individual receiver would need to request retransmissions, which in itself inflicts a bandwidth increase in a channel at the edge of overflow. Accordingly, all broadcast related IP traffic use UDP (User Datagram Protocol). Here no retransmission is included, which means that all data must be delivered in a safe manner at first attempt.

C.1 IP stream distortion

Distortions that influence the performance of an IP video transport system, in addition to packet loss, are packet delivery time variations (jitter), and packets arriving out of order. It should be noted that a single bit error occurring within an IP packet will result in the loss of the complete packet. As IP packets and Ethernet physical link layers normally go hand in hand, IP packets will be discarded if a single bit error occurs in transmission. The Ethernet link layer is secured with a cyclic redundancy check (CRC). An Ethernet frame with bit error(s) will be discarded by the first IP switch or router because the CRC check fails.

Furthermore, multiple packets may be lost during short periods due to congestion. As an IP packet contains close to 1500 bytes, or about 5% of a video frame for a video stream running at 5 Mbit/s, a lost IP packet will result in visible impairments.

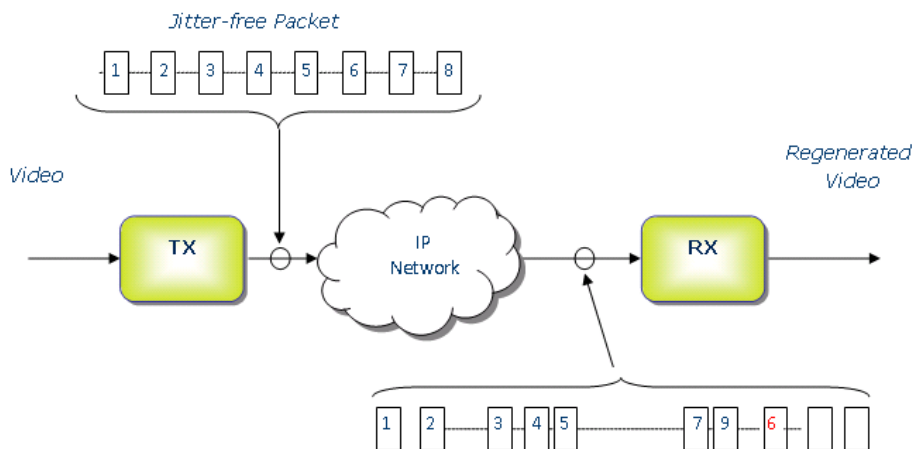


Figure C.1 Impairments of an IP packet stream

In **Figure C.1** distortions of an IP stream are visualised. The even stream of packets originating from the Tx node is modified in traversing the IP network. At the input of the Rx node the IP stream is distorted in the following ways:

- The packet spacing is no longer even
- The position of packet #6 has been shifted
- Packet #8 is missing

A properly designed IP node will handle the first two within certain limits; the input buffer size will determine the amount of jitter that can be tolerated and the time to wait for a delayed or out-of-order packet before it is deemed lost. Lost packets, however, are not recoverable unless special measures are taken.

C.2 Standardisation

All since streaming of broadcast services in IP networks began the insufficient reliability of IP links has been an issue, and methods to improve performance have been devised. Due to lack of standardisation many proprietary implementations and different solutions have been put into use by equipment manufacturers. The PRO-MPEG organisation has taken the initiative to achieve a common standard for transport of video over IP. These have been published as Code of Practice (COP) #3 and #4. COP#3 considers compressed video in the form of MPEG-2 Transport Stream, while COP#4 considers uncompressed video at 270Mbit/s and higher. The IP protocol stack proposed is RTP/UDP/IP. This work has been taken over by the Video Services Forum (VSF) (<http://www.videoservicesforum.org>). VSF has in cooperation with SMPTE successfully brought the COP#3 and COP#4 further and COP#3 is now finalised as SMPTE 2022-1 [9] and 2022-2 [8]. SMPTE 2022-1 focuses on improving IP packet loss ratio (PLR) performance using forward error correction techniques.

C.3 FEC matrix

SMPTE 2022-1 specifies a forward error scheme based on the insertion of additional data containing the result of an XOR-operation of packet content across a time window. By reversing the operation it is possible to reconstruct single lost packets or a burst of lost packets. The degree of protection may be selected to cover a wide range of link quality from low to heavy loss at the expense of increased overhead and delay.

SMPTE 2022-2 specifies use of RTP protocols and hence all packets have a sequence number. Thus, a receiver will be able to determine if a packet has been lost. There should be no cases of packets arriving containing bit errors as packets with checksum errors are discarded at the Ethernet layer. A FEC packet containing a simple XOR-sum carried out over a number of packets at the transmitter allows the receiver to compute one lost packet by redoing the XOR process over the same packets and comparing the results with the XOR FEC packet. This allows for the regeneration of one lost packet in an ensemble of N payload packets plus one FEC packet. If two or more packets in the ensemble are lost it is not possible to regenerate any of them. Packet loss in IP systems have a tendency to come in bursts (due to congestion). Therefore the FEC XOR calculation is not done on adjacent packets; rather packets at a fixed distance are used. This can be visualised by arranging the packets in a two dimensional array and inserting them in rows in the same order as they are transmitted.

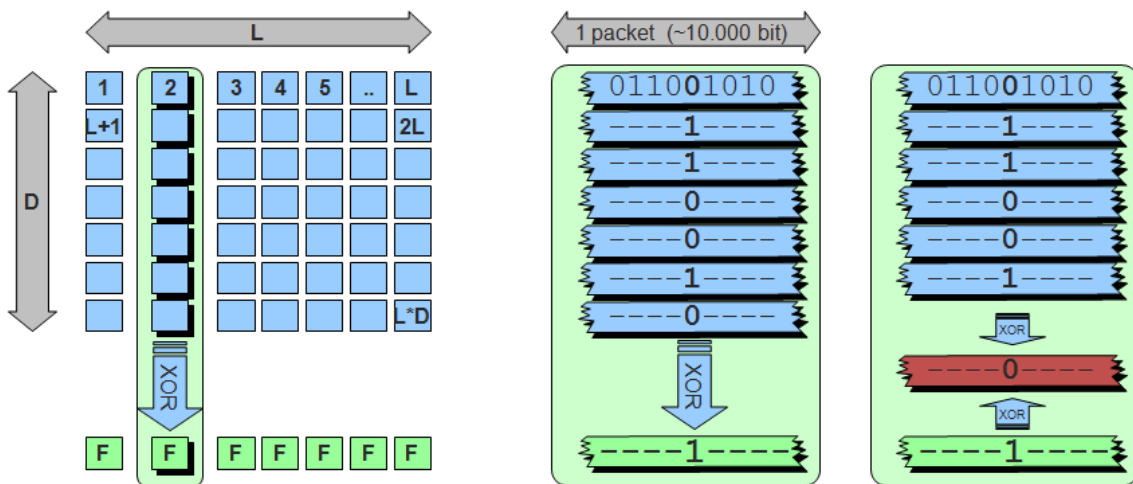


Figure C.2 IP packet FEC calculation matrix

Figure C.2 shows $L \times D$ consecutive IP packets arranged in a matrix. The FEC checksum is calculated over the columns, which means that the distance between two packets used in an XOR calculation is L . An XOR sum is calculated for each *bit position* of all the packets of a column. The checksums for all bit positions constitute the FEC checksum, and is inserted in a FEC packet which is sent in addition to the payload packets. There will be one FEC packet associated with each column, and it is therefore possible to regenerate as many packets as there are columns in the matrix.

In the right-most panel of Figure C.2 the case is shown where a packet in the last column position has been lost. The packet may then be regenerated (shown in red) by performing XOR addition over all remaining packets in that column, including the FEC packet. This is the default FEC mode of SMPTE 2022-1.

However, it is not possible to correct more than one error in a column. To increase the error correction capability the specification gives the option to also include FEC over the rows. By combining the two FEC calculations it is now possible to handle more complex packet loss distribution patterns and correct up to $L+D$ lost packets.

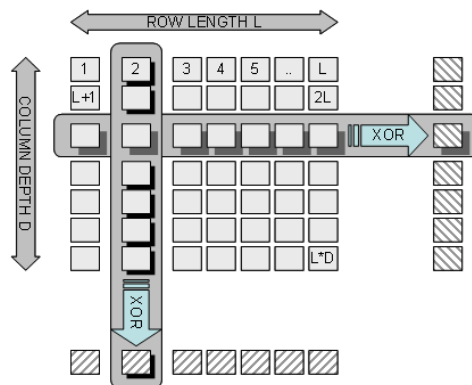


Figure C.3 Two-dimensional FEC calculation matrix

Figure C.3 shows this arrangement. Here, checksums are also calculated for the packets in each row. This gives rise to another D FEC packets, which again means increased overhead.

A drawback with a rectangular matrix arrangement is that all column-FEC packets need to be transmitted at nearly the same time as all column-FEC packets are generated when the last row of the matrix is being completed. Thus when transmitting the last row of payload packets the packet rate must be doubled in order to also send the FEC packets without generating extra payload packet delay. In itself this may cause temporary network overload with packet loss as a result. The specification [9] imposes some rules how FEC packets should be interleaved with payload packets to avoid excessive jitter and ensuring compatibility between equipment from different manufacturers. One method is to offset the FEC columns, one example is shown in **Figure C.4**, which also provides additional advantages.

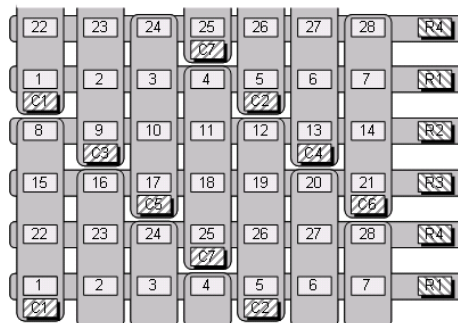


Figure C.4 FEC matrix with column offset

Column offset leads to column FEC packets being generated at a more regular rate and it is possible to transmit packets with a shorter delay than with a rectangular matrix. Offsetting the columns also increases the capability to regenerate longer bursts of lost packets; the length depending on the column and row length ratio.

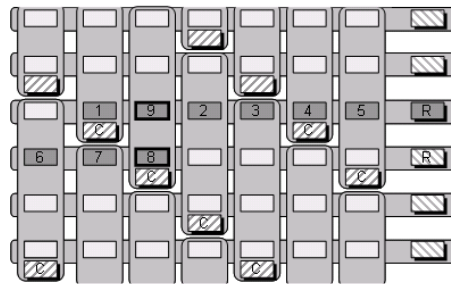


Figure C.5 Offset FEC matrix with missing packets

Figure C.5 shows an offset matrix with missing packets. The numbered items indicate packets lost. The figure shows that column offset may increase the capability to correct longer bursts of lost packets. In this example 9 consecutive packets are lost. Even if the row length is only 7 packets, all the 9 lost packets are reconstructed. The packets are numbered in the order they can be recovered. Packets marked 8 and 9 are protected by the same column FEC packet and are recovered by the row FEC packets after recovery of packets 1 through 7.

If more than one packet is lost in a row or a column of a matrix, the possibility to recover it depends on packet location. **Figure C.6** shows this.

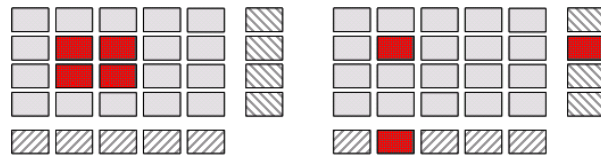


Figure C.6 Uncorrectable error patterns

The red-coloured packets are lost in transmission. The pattern to the left normally results in 4 unrecoverable payload packets. However, if two of the lost packets are FEC packets, then only 2 payload packets will be lost. The pattern to the right will result in one lost payload packet.

The specifications allow several parameter combinations for the FEC stream generation. The FEC matrix sizes can in principle be chosen at will to suit the operational conditions. Operators may easily be confused by the number of options, and it is not straightforward to choose the optimal FEC setting for a given scenario. For compatibility reasons SMPTE 2022-1 specifies that an MPEG-2 to IP network adapter should handle a minimum matrix size of 100 IP packets, and that row length or column depth should not exceed 20. Also the shortest column length allowed is 4.

C.4 Transmission aspects

The RTP protocol must be used if FEC shall be added to the IP payload. In order to provide compatibility between equipment handling application layer FEC and equipment without that capability FEC data is transmitted using UDP port numbers different from that of the payload. Column FEC is transmitted using port number (IP payload) + 2 and row FEC (if used) is transmitted using port number (IP payload) + 4.

Introducing FEC for the IP connection obviously leads to additional data overhead and consequently a higher demand on data capacity. The generated FEC packets need to be "squeezed" in between the payload packets, which will tend to increase the packet jitter experienced by the receiver. Notably, in a rectangular matrix all column-FEC packets are generated and inserted into the stream in succession. This leads to a short burst of packets in quick succession, or a considerable delay before the first packet of the next FEC frame can be transmitted (or indeed, some of each).

Figure C.7 illustrates the relative timing of FEC packets and payload packets. Applying an offset column structure results in a smoother packet stream. The overall packet rate will be the same in both schemes, since the same number of FEC packets are generated, but the packets will be more evenly spread in the IP stream. With larger matrix sizes the smoothing effect of an offset matrix will even more pronounced. The effect of added overhead and jitter should be considered when applying FEC to an IP video stream in a heavily loaded network. High instantaneous packet rates may cause temporary overload resulting in packet loss, defeating the object of introducing FEC in the first place.

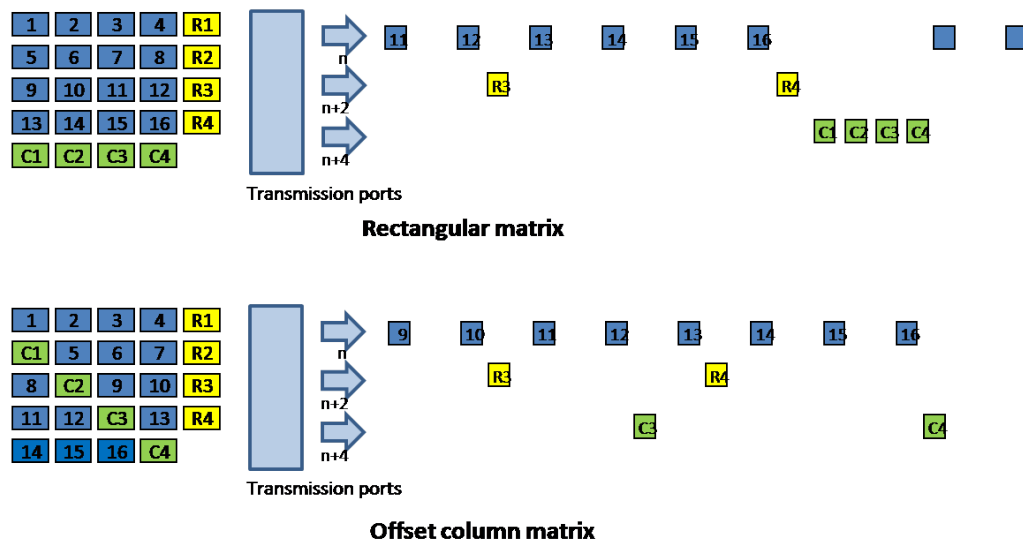


Figure C.7 FEC data transmission

C.5 Quality of service and packet loss in IP networks

One may ask how the FEC strategy relates to an operational IP network. Little information is available on packet loss patterns. Measurements show that up to 1% of the packets are duplicates and generated as a result of a retransmission request. Either because the packet has been lost or it has arrived too late. However, since these results are for TCP connections they merely serve to indicate an upper level for packet loss rate in an IP/MPLS network. Reported jitter measurements indicate that 0.01% of the packets were delayed more than 31ms and a fraction of those packets were delayed more than 100ms. This is also relevant for transmission of video as out-of-order packets arriving too late will be regarded as lost and must, if possible, be regenerated by FEC.

There are three main factors that cause packet loss:

- Occasional bit errors in the Ethernet frame caused by low noise margin or equipment fault
- Buffer overflow or packet delay caused by network congestion
- Packet re-routing, to circumvent a node breakdown or network bottlenecks

Some of the packets will arrive late. IP packet latency will vary as a result of variable traffic load on the network. Packets that do not arrive in time will be handled as lost packets. The FEC process will thus be able to handle occasional delay increase for a few packets and maintain a satisfactory Quality of Service. A video gateway should offer a setting for permissible packet delay, which should be optimised for the operation. If the receiver buffer latency is increased it is possible to reduce the FEC overhead and still get an error-free video link.

The Packet Loss Ratio (PLR) for an IP network is not a given number. Performance figures are normally in the order of 1×10^{-6} , but occasionally a link may become degraded showing PLR figures like 3×10^{-3} . The performance will vary over the day with the lowest performance

tending to occur at about the same time every weekday and lasting for one-half to one hour. The FEC setting should be set up to handle this peak hour with low residual loss.

The table of **Figure C.8** shows the IP network performance figures to meet the quality requirements of various grades of television services, as given by ITU recommendation Y.1541 [10]. Along these lines the DVB IPTV standard sets the performance requirement for a 4Mbit/s IPTV service at 1 visible error per hour, which means an IP packet loss ratio of 1×10^{-6} .

Profile (Typical bit rate)	One performance hit per 10 days	One performance hit per day	10 performance hits per day
Contribution (270 Mbit/s)	4×10^{-11}	4×10^{-10}	4×10^{-9}
Primary Distribution (40 Mbit/s)	3×10^{-10}	3×10^{-9}	3×10^{-8}
Access Distribution (3 Mbit/s)	4×10^{-9}	4×10^{-8}	4×10^{-7}

Figure C.8 Recommended error performance (as per ITU)

C.6 Error improvement

So, what does it take to make FEC improve the packet error rate of an IP network link to a level acceptable for the application? Assuming packet loss occurs at random **Figure C.9** shows how the depth of a one-dimensional FEC matrix affects the error correcting capability.

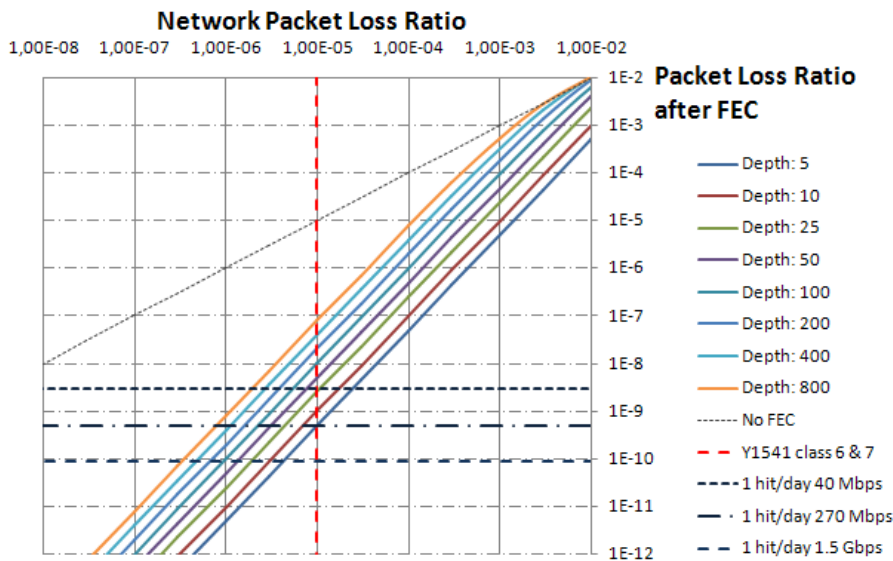


Figure C.9 Error improvement using column FEC only

It is evident that the smaller the column depth the better error correcting capability. At a network packet loss rate of 10^{-5} adding FEC will provide up to 4 magnitudes of improved error performance.

For ease of reference the diagram indicates packet loss rates resulting in one visible impairment (error hit) per day at transport stream bit rates of 40Mb/s, 270Mb/s and 1,5Gb/s, respectively.

It can be seen that in a network with worst hour packet loss rate of 3×10^{-3} it is not possible to provide distribution of a 3Mb/s transport stream with less than 10 hits per day (i.e. packet loss rate of 4×10^{-7} , as recommended in [Figure C.8](#)) using column-only FEC. In IP networks of ITU class 6 and 7 however, column-only FEC with reasonably small column depths will perform nicely for bit rates up to 270Mb/s.

Distributing video transport streams over high packet loss rate networks demand use of two-dimensional FEC. As explained earlier this increases the added overhead and thus the required network bandwidth.

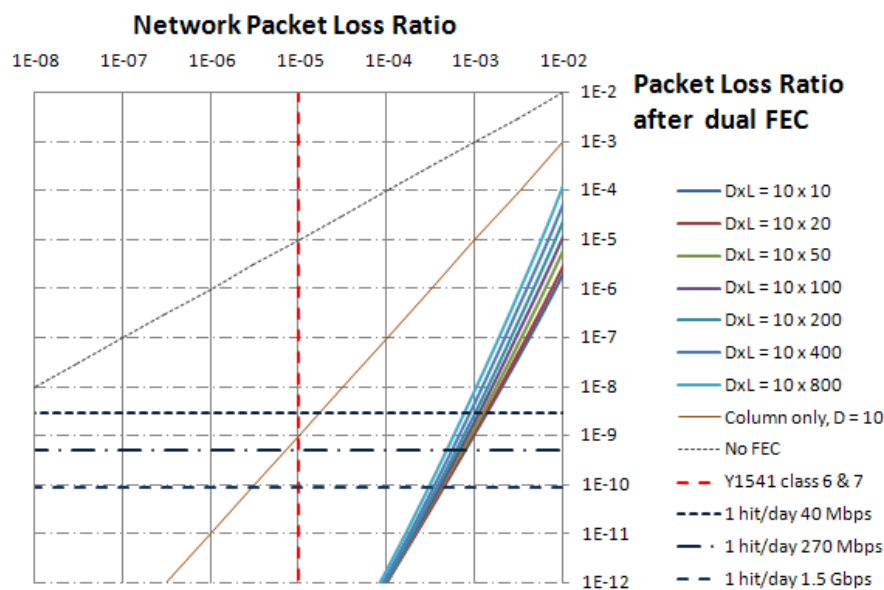


Figure C.10 Error improvement using two-dimensional FEC

[Figure C.10](#) shows how adding row FEC dramatically increases performance in high packet loss networks. Reverting to the previous case, a 3Mbit/s video transport stream in an IP network with worst hour PLR of 3×10^{-3} , a service with less than 10 error hits per day may be provided using any of the matrix sizes shown. In less error-prone networks however, using two-dimensional FEC schemes may be overkill and generate unnecessary FEC overhead.

C.7 Latency and overhead

Latency is increased when FEC is applied. The latency that can be accepted in a particular application may vary, and should be considered when setting FEC parameters.

FEC packet calculation in the transmitter is done on-the-fly and adds little to the latency. In a rectangular matrix, however, all FEC packets are generated nearly at the same time, as indicated in [Figure C.7](#). FEC packets should be spread in transmission to avoid introducing extra jitter. This also contributes to latency in error packet recovery. In the receiver all packets involved in the FEC calculation must be collected before a missing packet can be recovered. [Figure C.11](#) shows how different matrix sizes result in different latencies and required buffer sizes, using column-only FEC processing.

	Overhead	Latency			Recovery	Buffer size
		3Mbps	30 Mbps	100 Mbps		
XOR (5,10)	10%	175.5 ms	17.5 ms	5.3 ms	5 IP packets	66400 Bytes
XOR (10,10)	10%	350.9 ms	35.1 ms	10.5 ms	10 IP packets	132800 Bytes
XOR (20,5)	20%	350.9 ms	35.1 ms	10.5 ms	20 IP packets	132800 Bytes
XOR (8,8)	12.5%	224.6 ms	22.5 ms	6.7 ms	8 IP packets	84992 Bytes
XOR (10,5)	20%	175.5 ms	17.5 ms	5.3 ms	10 IP packets	66400 Bytes
XOR (8,5)	20%	140.4 ms	14.0 ms	4.2 ms	8 IP packets	53120 Bytes
XOR (5,5)	20%	87.7 ms	8.8 ms	2.7 ms	5 IP packets	33200 Bytes
XOR (4,6)	16.7%	84.2 ms	8.4 ms	2.5 ms	4 IP packets	31872 Bytes
XOR (6,4)	25%	84.2 ms	8.4 ms	2.5 ms	6 IP packets	31872 Bytes

Figure C.11 FEC latency and buffer size

Also shown is the resulting overhead and the number of packets that can be corrected. In column-only FEC there is one FEC packet per column, resulting in a 1/D increase in transmission overhead, D being the matrix column depth. I.e. in a 10 row matrix (D=10) the added overhead is 10%. The minimum allowable column depth of 4 will produce 25% overhead.

In two-dimensional FEC there will be D+L FEC packets in a DxL matrix (L being the row length). Thus the added overhead is D+L/DxL, which for a 10 by 10 matrix amounts to 20%.

Adding row-FEC will increase the error correcting capability without significantly increasing the latency or buffer size requirement. Applying row- and column-FEC also enables use of iterative FEC calculations to recover more missing packets. The equipment manufacturer is at liberty to determine the algorithm used in error recovery as long as the requirements and limitations of the specification are respected.

Appendix D Quality of Service, Setting Packet Priority

Normal IP routing is by best effort. This does not work well for broadcast television as the video and audio components need to be transported as a continuous flow of packets without interference from other traffic over the internet. There are different techniques to improve quality-of-service. The main ones are:

- MPLS (Multi Protocol Label Switching)
- Layer 3 routing priority
- Layer 2 routing priority

D.1 MPLS

In networks running MPLS, the packets are forwarded along a predefined path from an ingress router to an egress router. Packet switching is then done according to the label and packets will be switched expediently. The MPLS label is added to the IP packet by the ingress router and removed by the egress router. The labelling is done on the basis of packet classification.

D.2 Layer 3 routing

An alternative technique to improve QoS is to use layer 3 routing and give video content packets higher priority than other data. IP packets are put into queues according to their priority. Packets with high priority are forwarded expediently and have a lower probability of being discarded due to buffer overflow.

There are two ways to prioritise IP packets; using Differentiated services (Diff-serve) or precedence bits (TOS). Both these methods use the same bits in the IP header and both of them are in common use.

IP precedence values range from 0 to 7. Diff-serve code point (DSCP) values range from 0 to 63.

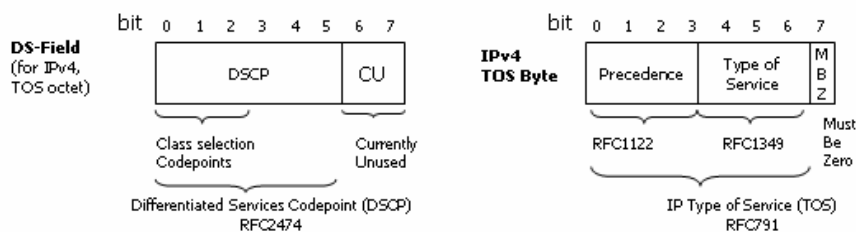


Figure D.1 Differentiated services (Diff-serve) and precedence bits (TOS)

Layer 3 prioritisation may also be combined with MPLS where layer 3 routing is used in the aggregation network and MPLS in the core network. The DSCP priority setting may be used for MPLS tagging.

D.2.1 TNS544 configuration

The number entered into the Type of service (TOS) field in TNS544 IP TX configuration menu defines all 8 bits. The value used should be in accordance with traffic engineering policy of the network and should be in the range from 0 to 255.

D.3 Layer 2 priority

Prioritisation can also be supported in layer 2 using VLAN tags. The 802.1q VLAN tag has 3 bits for setting the Class of Service (COS). The operation is further defined in [7]. The COS bits will be handled the same ways as Diff-serv or precedence bits regarding packet classification in the network.

D.3.1 TNS544 configuration

The COS priority is entered in the VLAN configuration page in the TNS544 IP TX configuration menu, in the field named VLAN Priority. A value in the range from 0 to 7 should be inserted. This value will be directly transferred to 3 user priority bits in the VLAN header.

More information on quality of service issues and configuration can be found in the literature, e.g. router configuration guides.

Appendix E Alarms

The TNS544 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 E.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 E.3 shows the possible alarms that can be signalled by the TNS544. For each alarm type, essential information is presented. The different fields are described in **Table E.2**.

Table E.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 <i>types</i> . This field contains a textual description of the type.
Type ID	Each alarm type has a corresponding number (ID).
Clear event	Set to <i>Yes</i> if an “off/cleared” alarm is expected after an “asserted” alarm. In most cases the value is <i>Yes</i> . 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 E.3.a Alarms

Alarm ID	Text	Def. severity	Details
106	Unable to transmit	Critical	<p><i>Description:</i> Channel not able to transmit any data, or only part of the data is transmitted.</p> <p><i>Type:</i> IP Output (<i>Type ID</i> = 24)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP output channel identifier</p> <p><i>Subid3:</i> Dest</p>
107	Output parameter conflict	Critical	<p><i>Description:</i></p> <p><i>Type:</i> IP Output (<i>Type ID</i> = 24)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP output channel identifier</p> <p><i>Subid3:</i> Dest</p>
130	Ethernet link down	Critical	<p><i>Description:</i> No link on Ethernet layer.</p> <p><i>Type:</i> Ethernet port (<i>Type ID</i> = 17)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>
131	Ethernet output overflow	Critical	<p><i>Description:</i> The total bitrate of the streams to transmit is too high compared to the available ethernet bitrate.</p> <p><i>Type:</i> Ethernet port (<i>Type ID</i> = 17)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>
140	IP address unresolved	Warning	<p><i>Description:</i> IP address is not resolved into physical MAC address.</p> <p><i>Type:</i> IP Output (<i>Type ID</i> = 24)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP output channel identifier</p> <p><i>Subid3:</i> Dest</p>
150	RTP sequence error	Warning	<p><i>Description:</i> 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.</p> <p><i>Type:</i> IP Input (<i>Type ID</i> = 23)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
151	No data received	Warning	<p><i>Description:</i> No data received on Ethernet input for stream.</p> <p><i>Type:</i> IP Input (<i>Type ID</i> = 23)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
153	Ethernet input overflow	Critical	<p><i>Description:</i> The total bitrate of the IP input streams is too high.</p> <p><i>Type:</i> Ethernet port (<i>Type ID</i> = 17)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>
154	Data lost	Critical	<p><i>Description:</i> The data stream received for a channel is incomplete, and if running FEC, the FEC engine is not able to recover all the lost frames.</p> <p><i>Type:</i> IP Input (<i>Type ID</i> = 23)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>

Table E.3.b Alarms

Alarm ID	Text	Def. severity	Details
155	No lock	Critical	<p><i>Description:</i> The incoming packet stream is absent or incompatible with the expected format.</p> <p><i>Type:</i> IP Input (<i>Type ID</i> = 23)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
157	Too low latency for FEC	Warning	<p><i>Description:</i> The preferred latency is set lower than the latency required to fully utilize the current FEC.</p> <p><i>Type:</i> IP Input (<i>Type ID</i> = 23)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
158	SFN mode config error	Warning	<p><i>Description:</i> Lock to MIP bitrate mode requires configuration and locking to an external 1PPS source (Device Info-Clock Regulator).</p> <p><i>Type:</i> IP Input (<i>Type ID</i> = 23)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
160	SNTP server unreachable	Warning	<p><i>Description:</i> The unit is not receiving answers from the SNTP server.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
161	Too high temperature	Warning	<p><i>Description:</i> Internal temperature of unit is too high.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
162	Defective fan	Warning	<p><i>Description:</i> One or more fans are not spinning.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
163	Time reference unreachable	Warning	<p><i>Description:</i> No selected timesources are OK.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
164	Illegal board configuration detected	Critical	<p><i>Description:</i> A board configuration that is incompatible with this product has been detected.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
165	Time source not OK	Notification	<p><i>Description:</i> One or more time sources are not OK.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
166	Time source switch	Notification	<p><i>Description:</i> Device started using a new time source.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>
167	Time adjusted	Notification	<p><i>Description:</i> The real time clock of the device was adjusted significantly.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>
168	Power failed	Warning	<p><i>Description:</i> One or more power supplies have failed, or are out of regulation.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Power supply ID</p>

Table E.3.c Alarms

Alarm ID	Text	Def. severity	Details
169	Virtual alarm relay activated	Notification	<p><i>Description:</i> A virtual alarm relay has been activated.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Relay ID</p>
210	Emergency switch active	Notification	<p><i>Description:</i> A user has activated the remote emergency switch.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
211	Emergency switch unreachable	Warning	<p><i>Description:</i> The device is not able to communicate with the remote emergency switch.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
212	Emergency switch rule config error	Warning	<p><i>Description:</i> An error has been detected in the configuration of the emergency switch.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> Yes</p>
501	User logged in	Notification	<p><i>Description:</i> This event is generated when a user logs on to the system.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>
502	User logged out	Notification	<p><i>Description:</i> This event is generated when a user logs out from the system.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>
503	System started	Notification	<p><i>Description:</i> The system has booted.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>
504	Switch done	Notification	<p><i>Description:</i> The input relay has switched position.</p> <p><i>Type:</i> Relay Switch (<i>Type ID</i> = 19)</p> <p><i>Clear event:</i> No</p> <p><i>Subid2:</i> Relay switch controller ID</p>
505	Config changed	Notification	<p><i>Description:</i> A modification has been made to the configuration of the device.</p> <p><i>Type:</i> System (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>
506	Unable to switch	Warning	<p><i>Description:</i> The relay controller is unable to switch because the spare input is not sufficiently good.</p> <p><i>Type:</i> Relay Switch (<i>Type ID</i> = 19)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Relay switch controller ID</p>
507	Auto switching disabled	Warning	<p><i>Description:</i> Enabled when auto switching is turned off.</p> <p><i>Type:</i> Relay Switch (<i>Type ID</i> = 19)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Relay switch controller ID</p>
508	Auto switch performed	Filtered	<p><i>Description:</i> Automatic switch is performed. This alarm will stay on until it is manually confirmed by the operator (see chapter on switch config).</p> <p><i>Type:</i> Relay Switch (<i>Type ID</i> = 19)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Relay switch controller ID</p>

Table E.3.d Alarms

Alarm ID	Text	Def. severity	Details
517	Alarm log cleared	Notification	<p><i>Description:</i> Alarm log was cleared, user in details</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> No</p>
518	System is starting up	Critical	<p><i>Description:</i> This alarm is set when the system is starting. Once booted correctly, the alarm is cleared.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> Yes</p>
519	Forced reset initiated	Notification	<p><i>Description:</i> A reset of the device was forced by the operator.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> No</p>
520	SW loading in progress	Notification	<p><i>Description:</i> Loading of an embedded SW image is in progress</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> Yes</p>
521	New SW pending	Notification	<p><i>Description:</i> A SW image has been successfully loaded, but manual reboot is needed for SW to be activated.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> Yes</p>
524	Simultaneous users	Notification	<p><i>Description:</i> Multiple users with administrator or operator access level are logged in.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> Yes</p>
526	Action performed	Notification	<p><i>Description:</i> Action performed by user. Used to log generic important events, see details field on each alarm event for additional information.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> No</p>
527	New SW license pending	Notification	<p><i>Description:</i> New SW licenses have been loaded but requires a re-boot to be activated.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> Yes</p>
528	New SW license installed	Notification	<p><i>Description:</i> New SW licenses have been loaded and installed without requiring reboot.</p> <p><i>Type:</i> System (Type ID = 13)</p> <p><i>Clear event:</i> No</p>
710	Seamless switch impossible	Warning	<p><i>Description:</i> Seamless switch to port not possible. This can be due to delay problems or mismatching streams.</p> <p><i>Type:</i> Relay Switch (Type ID = 19)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Relay switch controller ID</p>
1100	Sync unstable	Major	<p><i>Description:</i> Two separate sync-losses in 10s.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1101	TS unstable	Minor	<p><i>Description:</i> Lots of PIDs appearing/disappearing or CC errors.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>

Table E.3.e Alarms

Alarm ID	Text	Def. severity	Details
1110	No sync	Critical	<i>Description:</i> No valid ASI stream detected. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1120	Sync byte error	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1131	PAT repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1132	PAT invalid table ID	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1133	PAT scrambled	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1134	PAT missing	Warning	<i>Description:</i> PAT not found in transport stream. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1140	CC error	Warning	<i>Description:</i> Continuity counter error. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> PID
1151	PMT repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1152	PMT scrambled	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1153	PMT missing	Warning	<i>Description:</i> PMT not found in transport stream. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> Service

Table E.3.f Alarms

Alarm ID	Text	Def. severity	Details
1160	PID error	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1161	PID event	Filtered	<p><i>Description:</i> This alarm is currently used to configure the time before a PID is assumed to have disappeared.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> No</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1210	Transport error	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1220	CRC error	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1221	CRC error on update	Warning	<p><i>Description:</i> CRC error on table with new version number.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1230	PCR error	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1231	PCR discontinuity indicator error	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1240	PCR overall jitter	Filtered	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>

Table E.3.g Alarms

Alarm ID	Text	Def. severity	Details
1241	PCR accuracy error	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> PID
1250	PTS error	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> PID
1261	CAT missing	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1262	CAT invalid table ID	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1311	NIT invalid table ID	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1312	NITa repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1313	NITo repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1314	NITa section gap too small	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1315	NITo section gap too small	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1316	NITa missing	Warning	<i>Description:</i> NIT actual is not present. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier

Table E.3.h Alarms

Alarm ID	Text	Def. severity	Details
1317	NITo missing	Filtered	<p><i>Description:</i> No NIT other sections are present.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1320	SI repetition error	Warning	<p><i>Description:</i> See ETSI Technical Report 290. Note that this alarm fires together with the repetition interval and gap alarms for each specific table.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1340	Unreferenced PID	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1351	SDT invalid table id	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1352	SDTa repetition interval	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1353	SDTo repetition interval	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1354	SDTa section gap too small	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1355	SDTo section gap too small	Warning	<p><i>Description:</i> See ETSI Technical Report 290.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1356	SDTa missing	Warning	<p><i>Description:</i> SDT actual is not present.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1357	SDTo missing	Filtered	<p><i>Description:</i> No SDT other sections are present.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>

Table E.3.i Alarms

Alarm ID	Text	Def. severity	Details
1359	BAT missing	Warning	<i>Description:</i> <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1361	EIT invalid table id	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1362	EITpfa repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1363	EITpfo repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1364	EITpfa section gap too small	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1365	EITpfo section gap too small	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1366	EITpfa section missing	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1367	EITpfo section missing	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1368	EITpfa missing	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> Service
1369	EITpfo missing	Filtered	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier

Table E.3.j Alarms

Alarm ID	Text	Def. severity	Details
1371	RST invalid table id	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1372	RST section gap too small	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1381	TDT repetition interval	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1382	TDT/TOT invalid table id	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1383	TDT section gap too small	Warning	<i>Description:</i> See ETSI Technical Report 290. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1384	TDT missing	Warning	<i>Description:</i> <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1385	TOT missing	Warning	<i>Description:</i> <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1386	TOT repetition interval	Warning	<i>Description:</i> <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1523	Status Input connector	Warning	<i>Description:</i> Alarm representing external alarm relays, labeled Status Input <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1524	MIP PID not present	Warning	<i>Description:</i> The MIP PID is not present. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier

Table E.3.k Alarms

Alarm ID	Text	Def. severity	Details
1525	MIP CRC error	Critical	<p><i>Description:</i> A CRC error has been detected in the MIP.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1526	MIP new parameters	Notification	<p><i>Description:</i> An update has been detected in the parameters contained in MIP (TPS field or maximum delay field).</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1527	MIP CC error	Warning	<p><i>Description:</i> TS packet header CC error has been detected on the MIP PID.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1528	MIP STS range error	Warning	<p><i>Description:</i> The STS field indicates a value larger than a second.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1529	MIP pointer error	Warning	<p><i>Description:</i> The number of TS packets in the megafame does not match the parameters in MIP.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1530	MIP timing error	Warning	<p><i>Description:</i> STS values in consecutive MIPs have wrong timing values.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1531	Extra MIP	Warning	<p><i>Description:</i> An extra MIP has been detected within a megafame.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1532	Missing MIP	Warning	<p><i>Description:</i> No MIP is detected.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1533	MIP periodicity error	Warning	<p><i>Description:</i> The MIP periodicity is not correct.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1534	MIP ts rate error	Warning	<p><i>Description:</i> The rate of the transport stream does not match the rate signaled in the MIP.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>

Table E.3.1 Alarms

Alarm ID	Text	Def. severity	Details
1535	MIP network delay too high	Filtered	<p><i>Description:</i> 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.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1536	MIP network delay too low	Filtered	<p><i>Description:</i> 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.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1542	MIP size error	Warning	<p><i>Description:</i> There is not enough space in the MIP packet for all configured transmitter function loops.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1543	MIP Inserter time reference problem	Warning	<p><i>Description:</i> MIP Inserter time reference problem.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1801	TS-ID incorrect	Filtered	<p><i>Description:</i> 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.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1802	PID rate too high	Filtered	<p><i>Description:</i> PID bitrate is higher than set limit.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1803	PID rate too low	Filtered	<p><i>Description:</i> PID bitrate is lower than set limit.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1804	Static scrambling bits	Filtered	<p><i>Description:</i> Scrambling bits are static (not changing between odd and even) within the user defined interval.</p> <p><i>Type:</i> Port (Type ID = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>

Table E.3.m Alarms

Alarm ID	Text	Def. severity	Details
1805	Service missing	Filtered	<p><i>Description:</i> A service is missing from the stream (according to configured expected value)</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> Service</p>
1806	PID scrambled	Filtered	<p><i>Description:</i> Define list of PIDs which should NOT be scrambled. Alarm will be triggered if PID is scrambled</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1807	PID not scrambled	Filtered	<p><i>Description:</i> Define list of PIDs which should be scrambled. Alarm will be triggered if PID is NOT scrambled</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> PID</p>
1812	TS rate too high	Filtered	<p><i>Description:</i> TS bitrate is higher than set limit.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1813	TS rate too low	Filtered	<p><i>Description:</i> TS bitrate is lower than set limit.</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
1814	CA system ID missing	Filtered	<p><i>Description:</i> A specified CA system ID is missing in CAT</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> CAID</p>
1901	EITpf timing error	Warning	<p><i>Description:</i> The start/end time of the EITpf present event is not matching current time</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> TS-ID</p>
1902	EITpf following error	Warning	<p><i>Description:</i> The following event is not immediately following the present event</p> <p><i>Type:</i> Port (<i>Type ID</i> = 9)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p> <p><i>Subid3:</i> TS-ID</p>

Table E.3.n Alarms

Alarm ID	Text	Def. severity	Details
1903	EITs segmentation error	Warning	<i>Description:</i> Events found in wrong segment based on segmentation rules, or in wrong order <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> TS-ID
1904	EITs illegal event time	Warning	<i>Description:</i> Event start/end times outside valid range <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> TS-ID
1905	EITs gaps found	Warning	<i>Description:</i> Events are not describing all time span of EIT <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> TS-ID
2100	PSIP repetition error	Warning	<i>Description:</i> <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2101	MGT repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2102	MGT missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2103	MGT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2104	MGT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2106	TVCT repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2107	TVCT missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier

Table E.3.o Alarms

Alarm ID	Text	Def. severity	Details
2108	TVCT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2109	TVCT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2111	CVCT repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2112	CVCT missing	Filtered	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2113	CVCT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2114	CVCT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2116	RRT repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2117	RRT missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2118	RRT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2119	RRT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier

Table E.3.p Alarms

Alarm ID	Text	Def. severity	Details
2121	STT repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2122	STT missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2123	STT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2124	STT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2130	EIT-0 repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2131	EIT-0 missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> Source-ID
2132	EIT-1 repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2133	EIT-1 missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> Source-ID
2134	EIT-2/3 repetition interval	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2135	EIT-2/3 missing	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> Source-ID

Table E.3.q Alarms

Alarm ID	Text	Def. severity	Details
2136	EIT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2137	EIT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2138	ETT scrambled	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2139	ETT CRC error	Warning	<i>Description:</i> See ATSC Recommended Practice A/78. <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
13610	EITsa missing	Warning	<i>Description:</i> <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> Service
13611	EITso missing	Warning	<i>Description:</i> <i>Type:</i> Port (Type ID = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier <i>Subid3:</i> TS-ID

Appendix F References

- [1] ISO13818-1, 2 and 3; MPEG-2 Video and Audio and Systems
- [2] ETSI EN 300 468: Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB Systems.
- [3] ETSI TR 101 211: Digital Video Broadcasting (DVB); Guidelines on Implementation and Usage of Service Information.
- [4] ETSI EN 300 744. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television.
- [5] ETSI TS 101 191. Digital Video Broadcasting (DVB); DVB mega-frame for Single Frequency Network (SFN) synchronisation.
- [6] ETR 154 Digital Video Broadcasting (DVB); Implementation Guidelines for the Use of MPEG-2 Systems, Video and Audio in Satellite and Cable Broadcasting Applications. ETSI Technical Report ETR 154, European Telecommunications Standards Institute ETSI.
- [7] IEEE 802.1Q-2005 802.1QTM, Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks
- [8] SMPTE 2022-2-2007: Unidirectional Transport of Constant Bit-Rate MPEG-2 Transport Streams on IP Networks
- [9] SMPTE 2022-1-2007: Forward Error Correction for Real-time Video/Audio Transport over IP Networks
- [10] ITU-T Y.1541 (02/2006) Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Internet protocol aspects; Quality of service and network performance. Network performance objectives for IP-based Services
- [11] Pro-MPEG Forum: Pro-MPEG Code of Practice #3 release 2, July 2004: Transmission of Professional MPEG-2 Transport Streams over IP Networks

- [12] Pro-MPEG Forum: Pro-MPEG Code of Practice #4 release 1, July 2004: Transmission of High Bit Rate Studio Streams over IP Networks
- [13] J. Rosenberg, H. Schulzrinne, IETF RFC2733, December 1999: An RTP Payload Format for Generic Forward Error Correction