

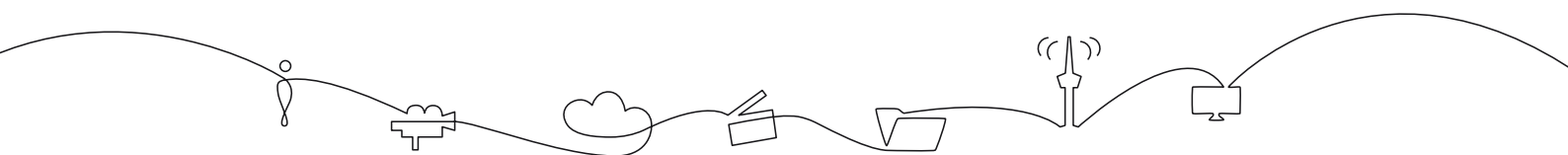
CP524 TS Adapter User's Manual

Revision: 1.0.38 (3712)

2012-09-11



Valid for SW version 1.0.38 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	Software options	14
4	Installing the Equipment	17
4.1	Inspect the package content	17
4.2	Installation Environment	17
4.3	Equipment installation	18
4.4	Ventilation	18
4.5	Power supply	19
4.5.1	AC power supply	19
4.5.2	Dual AC power supplies	19
4.5.2.1	AC power cable	19
4.5.2.2	Protective Earth/technical Earth	20
4.5.2.3	Connecting to the AC power supply	20
4.5.3	DC power supply	21
4.5.3.1	DC power cable	21
4.5.4	Powering up/down	21
5	Functional Description	23
5.1	Introduction	23
5.2	TS inputs	23
5.3	TS output	24
5.4	Input switching	24
5.5	Video over IP	24
5.5.1	Input and output	24
5.5.2	Protocol mapping	24
5.6	Management sub-system	25
5.6.1	Graphical user interface	25
5.6.2	Configuration database	26
5.6.3	Alarm manager	26
5.7	Time synchronisation	27

5.8	TSP Module	27
5.8.1	PID Router	28
5.8.2	PSI/SI/PSIP section filter	29
5.8.3	PSI/SI/PSIP playout module	29
5.8.4	Output Priority Queue	30
5.8.5	Bitrate shaping algorithm	33
5.8.6	TS Builder - Service and PID routing	33
5.9	PSI/SI/PSIP playout	35
5.9.1	Main configuration	36
5.9.2	Carousel priorities	36
5.9.3	Carousel bitrate	36
5.9.4	Bitrate saturation handling	37
5.9.5	Configurable back-log time	38
5.10	Service fallback	39
5.10.1	General	39
5.10.2	Details on confirm timeout handling	41
5.10.3	Manual switching on GPI	42
5.11	Hitless switching	43
5.12	Redundancy controller	44
5.12.1	Operation	44
6	Physical Description	47
6.1	Connecting the CP524	47
6.1.1	Physical description overview	47
6.1.2	ASI ports	47
6.1.3	ASI input ports	48
6.1.4	ASI output ports	48
6.1.5	1 PPS Input	48
6.1.6	Alarm/Reset	48
6.1.7	Electrical Ethernet data ports	49
6.1.8	Ethernet management port	49
6.1.9	The SFP module	49
6.1.10	Serial USB interface	50
6.1.11	Power Supply	50
6.1.12	Technical Earth	50
7	Operating the Equipment	51
7.1	Accessing the graphical user interface	51
7.2	Password protection	51
7.2.1	Resetting the password list	52
7.3	Changing the IP address of the unit	52
7.3.1	Changing IP address via the Web GUI	52
7.3.2	Changing the management port IP address via terminal interface	53
8	WEB Interface	55
8.1	Login	55

8.2	Status header	56
8.3	Status	57
8.3.1	Current Status	57
8.3.2	Alarm log	59
8.4	Device Info	61
8.4.1	Product info	61
8.4.2	Alarms	63
8.4.2.1	Device alarms	63
8.4.2.2	Global configuration	64
8.4.2.3	Relays and LED	65
8.4.2.4	Alarm log settings	67
8.4.3	Port Mappings	68
8.4.4	Time Settings	69
8.4.5	Network	71
8.4.5.1	Interfaces	72
8.4.5.1.1	Main	72
8.4.5.1.2	Alarms	73
8.4.5.1.3	Advanced	74
8.4.5.1.4	Status	74
8.4.5.1.5	VLAN	76
8.4.5.1.6	SFP	77
8.4.5.2	IP Routing	86
8.4.5.3	TXP Settings	87
8.4.5.4	SNMP Settings	88
8.4.5.5	Tools	89
8.4.6	Clock Regulator	91
8.4.6.1	Main	91
8.4.6.2	Alarms	92
8.4.7	Save/Load Config	92
8.4.7.1	Save/Load Configs	92
8.4.7.2	Boot Log	94
8.4.7.3	Stored Configs	94
8.4.8	Maintenance	96
8.4.8.1	General	96
8.4.8.2	Software Upgrade	98
8.4.8.3	Feature Upgrade	99
8.4.9	Users	99
8.4.10	GUI Preferences	100
8.5	Inputs	101
8.5.1	Inputs Overview	101
8.5.1.1	IP Inputs	102
8.5.1.2	Switch Inputs	104
8.5.2	Input	105
8.5.2.1	Main	106
8.5.2.2	Alarms	108
8.5.2.3	IP	113
8.5.2.3.1	RTP/IP Diversity Reception	115

8.5.2.3.2	FEC	118
8.5.2.3.3	Ping	119
8.5.2.3.4	Regulator	120
8.5.2.4	Services	122
8.5.2.5	PIDs	125
8.5.2.6	Tables	128
8.5.2.7	Tables	128
8.5.2.8	Settings	130
8.5.2.9	Sources	131
8.5.3	Switch	132
8.5.3.1	Main	133
8.5.3.2	Alarms	135
8.6	Outputs	135
8.6.1	Outputs Overview	135
8.6.2	Output	136
8.6.2.1	Main	137
8.6.2.2	Alarms	139
8.6.2.3	IP	140
8.6.2.4	Services	140
8.6.2.5	Service edit dialogue	143
8.6.2.5.1	Service Edit – General	143
8.6.2.5.2	Service Edit - Service Descriptors	147
8.6.2.5.3	Service Edit - Components	149
8.6.2.5.4	Service Edit – Fallback	156
8.6.2.6	PIDs	158
8.6.2.7	Tables	161
8.6.2.7.1	Main	162
8.6.2.7.2	EIT Sch	164
8.6.2.7.3	EIT/ETT Sch	166
8.6.2.7.4	EIT sources	167
8.6.2.7.5	Static SI	167
8.6.2.7.6	PSI/SI/PSIP editor	168
8.6.2.7.7	PSI/SI Editor	170
8.6.2.7.8	PSIP Editor	176
8.6.2.8	Pri Queue	180
8.6.2.9	Outgoing	182
8.6.2.9.1	Services	182
8.6.2.9.2	Service Routing	183
8.6.2.9.3	PIDs	183
8.6.2.9.4	Tables	185
8.6.3	Output copies	185
8.6.4	TS-OUT -> IP Destination	186
8.6.4.1	Main	186
8.6.4.2	FEC	188
8.6.4.3	Ping	190
8.7	Redundancy	191
8.7.1	Redundancy Controller	191

8.7.1.1	Global redundancy controller switching	192
8.7.1.2	Poll settings	192
8.7.1.3	Remote device IP addresses	194
8.7.1.4	SNMP switch actions	194
8.7.2	Service switchers	195
9	SNMP	197
9.1	SNMP agent characteristics	197
9.2	MIB naming conventions	197
9.3	MIB overview	197
9.3.1	Supported standard MIBs	197
9.3.2	Custom MIBs	197
9.4	SNMP related configuration settings	199
9.4.1	Community strings	199
9.4.2	Trap destination table	200
9.4.3	Trap configuration	200
9.5	Alarm/status related SNMP TRAPs	201
9.5.1	The main trap messages	201
9.5.2	Severity indications	201
9.5.3	Alarm event fields	202
9.5.4	Matching of on/off traps	203
9.5.5	Legacy trap messages	203
10	Examples of Use	205
10.1	Intro	205
10.2	Installation in a system	205
10.3	Raw PID multiplexing	205
10.4	Simple local insertion of a program	206
10.5	Sharing of service component	206
10.6	Adding an unsignalled component (Ghost PID)	207
11	Preventive Maintenance and Fault-finding	209
11.1	Preventive maintenance	209
11.1.1	Routine inspection	209
11.1.2	Cleaning	209
11.1.3	Servicing	209
11.1.4	Warranty	210
11.2	Fault-finding	210
11.2.1	Preliminary checks	210
11.2.2	PSU LED not lit / power supply problem	211
11.2.3	Fan(s) not working / unit overheating	212
11.3	Disposing of this equipment	212
11.4	Returning the unit	212
A	Glossary	213

B	Technical Specification	219
B.1	Physical details	219
B.1.1	Half-width version	219
B.1.2	Full-width (dual power) version	219
B.2	Environmental conditions	219
B.3	Power	220
B.3.1	AC Mains supply	220
B.3.2	DC supply	220
B.4	Input/output ports	221
B.4.1	DVB ASI port	221
B.4.2	SMPTE 310M port	221
B.4.3	Ethernet management port	221
B.4.4	Ethernet data port	221
B.4.5	Serial USB interface	222
B.5	Alarm ports	222
B.5.1	Alarm relay/reset port specification	222
B.6	External reference	223
B.6.1	10MHz/1 PPS input	223
B.7	Compliance	223
B.7.1	Safety	223
B.7.2	Electromagnetic compatibility - EMC	223
B.7.3	CE marking	224
B.7.4	Interface to “public telecommunication system”	224
C	Forward Error Correction in IP Networks	225
C.1	IP stream distortion	225
C.2	Standardisation	226
C.3	FEC matrix	226
C.4	Transmission aspects	229
C.5	Quality of service and packet loss in IP networks	230
C.6	Error improvement	231
C.7	Latency and overhead	232
D	Quality of Service, Setting Packet Priority	235
D.1	MPLS	235
D.2	Layer 3 routing	235
D.2.1	CP524 configuration	236
D.3	Layer 2 priority	236
D.3.1	CP524 configuration	236
E	Alarms	237
F	References	249

1 History

Revision	Date	Comments
1.0.38	2012-09-11	– Added section about Hitless switching and RTP/IP diversity reception. – Updated sections about Embedded redundancy.
1.0	2012-06-20	– First version of manual

2 Introduction

2.1 Scope

This manual is written for operators and users of the CP524 TS Adapter and provides necessary information for installation, operation and day-to-day maintenance of the unit. The manual covers the functionality of the software version 1.0.38 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 CP524 is part of the T-VIPS cProcessor product family for processing and handling of MPEG transport streams. The cProcessor family represents a line of compact and powerful, yet cost-effective, products designed for advanced modification of MPEG Transport Streams.

The CP524 is a Transport Stream Re-multiplexer for regional multiplexing of MPEG transport streams.

The CP524 supports insertion of unsigned PIDs on the input (Ghost PIDs) into outgoing services.

3.1 Summary of Features

Features of the CP524 include:

- Flexible transport stream processing
 - PID and program filtering
 - Service component filtering by PID value or by component tag
 - Program re-multiplexing (option)
 - TS rate adaptation
 - Minimum null-packet rate feature
- Powerful PSI/SI/PSIP handling
 - PSI/SI regeneration
 - Flexible EIT handling
 - Zero or configurable minimum null-packet rate by filling up with EIT
- PSI/SI/PSIP editor
 - Generate and create custom static PSI/SI/PSIP signalling.
- Transport stream monitoring
 - TR 101 290 Priority 1 monitoring: Sync loss, CC error
 - Monitoring of min/max bitrate for individual PIDs
 - Output PID monitoring (CC errors)
- Flexible alarm configuration options
 - Alarm levels freely configurable individually for each channel
 - Individual setting of alarm levels based on PID values

- Multiple unique multiplexer TS outputs
 - Up to four unique simultaneous TS outputs.
- Compact, cost-effective solution
- User-friendly configuration and control
 - WEB/XML based remote control
 - Easy access to unit from any WEB browser
 - Easy integration to NMS systems with SNMP Trap support
 - SNMPv2c agent
 - Equipment monitoring from T-VIPS Connect
- Embedded redundancy controller (Option)
- RTP/IP diversity reception (option)
 - Seamless switching between two IP streams from the same source.
- Transmission of transport stream over Gigabit Ethernet
 - Forward Error Correction (Option)
- Reception of transport stream over Gigabit Ethernet
 - Forward Error Correction (Option)

3.2 Software options

The CP524 functionality depends on the software licences installed. The following table describes the features available as software options. Please refer to [Section 8.4.8.3](#) for more information how to obtain and enable feature upgrades.

Table 3.1.a 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.
Number of input ports activated	24	Controls the number of simultaneously activated transport stream inputs.
Input switching	-	Enables creation of input switching groups.
Forward Error Correction	-	Controls availability of the FEC feature for IP outputs and IP inputs.

Table 3.1.b Functionality enabled through software licences

RTP/IP diversity reception	-	Enables configuration of IP diversity reception input pairs.
Service fallback	-	The feature makes it possible to configure pairs of services where one is back-up for the other. Switching decision is made based on alarm levels on each service.
PSI/SI/PSIP editor	-	Controls availability of built-in PSI/SI/PSIP Editor function in GUI, to edit tables for static playout.
Output Streams	4	Controls the number of Transport Stream outputs that can be active at the same time.
TS MUX	-	Enables Transport Stream multiplexing with data from more than one input.
Connect control	-	Enables supervision of the unit through the Connect Software.
Embedded redundancy controller	-	Availability of on-unit redundancy controller service.

4 Installing the Equipment



Caution: The CP524 must be handled carefully to prevent safety hazards and equipment damage. Ensure that the personnel designated to install the unit have the required skill and knowledge. Follow the instructions for installation and use only installation accessories recommended by the manufacturers.

4.1 Inspect the package content

- Inspect the shipping container for damage. Keep the shipping container and cushioning material until you have inspected the contents of the shipment for completeness and have checked that the CP524 is mechanically and electrically in order.
- Verify that you received the following items:
 - CP524 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.

4.2 Installation Environment

As with any electronic device, the CP524 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 CP524.

- 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 CP524 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.

4.3 Equipment installation

The CP524 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 CP524 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 CP524.

4.4 Ventilation

Openings in the cabinet are provided for ventilation to protect it from overheating and ensure reliable operation. The openings must not be blocked or covered. Allow at least 50 mm free 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 4.1](#).
- The CP524 may be vertically stacked in 19" racks without intermediate ventilation panels. In systems with stacked units forced-air cooling may be required to reduce the operating ambient temperature.

[Figure 4.1](#) shows the air path through the unit, where cool air is taken from the left hand side, seen from the front.

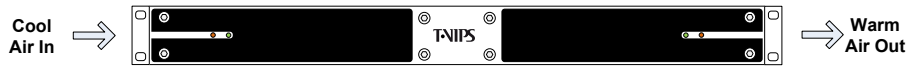



Figure 4.1 Air path through the unit

4.5 Power supply

The CP524 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.

4.5.1 AC power supply

The CP524 has a wide-range power supply accepting the voltage range 100-240 VAC, 50/60 Hz. Please refer to [Appendix B](#) for a detailed specification of the AC power supply.

4.5.2 Dual AC power supplies


Alternatively, the CP524 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.

4.5.2.1 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 4.1](#).

Table 4.1 Supply cable wiring colours

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

4.5.2.2 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.

4.5.2.3 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 CP524 mains input connector(s) and then to the local mains supply.

4.5.3 DC power supply

The CP524 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.

4.5.3.1 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 4.2](#). The power cable itself is not supplied.

Table 4.2 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 CP524 power input connector.

4.5.4 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.

5 Functional Description

5.1 Introduction

The CP524 is an MPEG Transport Stream Adapter, designed for easy and flexible manipulation of Transport Streams for carriage over ASI, SMPTE 310M or Ethernet connections. The SFP connector can also be used for data carriage. Use of SFP is enabled with a SW licence key.

The product offers an easy-to use WEB based user interface, a flexible and powerful MPEG Transport Stream re-generation module and integration with network management systems via the SNMP interface.

This chapter gives a brief description of the inner guts of the CP524, to give a better understanding of how the product works, how you use it and what you can use it for.

Figure 5.1 shows a functional block diagram of the main components inside CP524. The different blocks are described more in detail in the following sections.

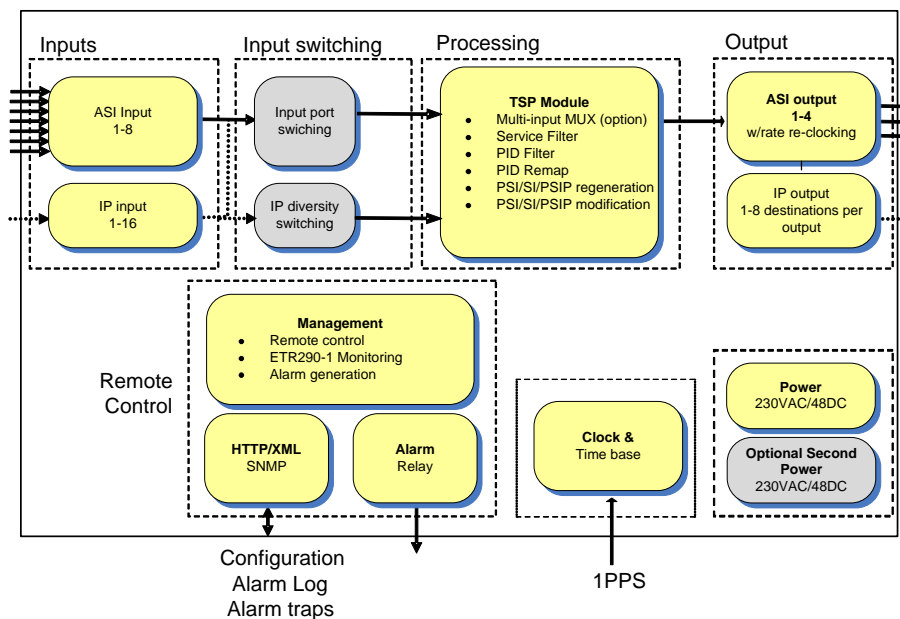


Figure 5.1 Product block diagram

5.2 TS inputs

The CP524 can be fitted with up to 8 ASI ports. Each of the ASI ports can be used as either input or output port. When only using IP output, all 8 ASI ports can be used as inputs. In ATSC+DVB configuration mode, SMPTE 310M input format is also supported.

In addition to 8 Transport streams inputs on ASI, a number of Transport streams can be received on either of the Ethernet data interfaces.

The number of TS inputs that can be enabled simultaneously is limited with a SW licence key, making it possible to start with few inputs and then enable more ports when needed. The licence key also covers the transport streams received on Ethernet/IP.

5.3 TS output

The CP524 can generate up to 4 MPEG output Transport Streams. The outputs can be programmed to be presented as ASI on one or more of the physical BNC I/O connectors as described in chapter 6.1.2. In ATSC+DVB configuration mode, SMPTE 310M output is also supported.

The output is always re-clocked, configuring a wanted bitrate for each output multiplex.

The output transport stream can also be transmitted on either of the Ethernet data interfaces.

5.4 Input switching

The CP524 supports combination of several inputs into a prioritized order switching group, where the highest priority source that has sync and no critical alarms, is automatically selected as the source of program data and PSI/SI/PSIP data.

The input switch is itself modelled as an input, so once defined, it can be referred to as the source of programs and PSI/SI/PSIP data when building up the output multiplex. A sync loss on the currently selected source will cause immediate switching to an alternative input in the switching group.

The signals on each of the inputs in a switching group, can be identical or different. Fastest switching times are achieved when the signals are identical with respect to PIDs and services.

The input switching function can be used on both ASI sources and IP sources, or any combinations of these. Signal loss detection on IP sources is slower than for ASI sources.

Sources that are members of a switching group cannot be referred to directly.

The input switching feature is protected by a SW licence key.

5.5 Video over IP

5.5.1 Input and output

The CP524 supports MPEG transport streams over IP, input and output.

IP inputs are defined dynamically on need, up to a maximum number that is 16 at the time of writing. Once the IP inputs are defined, they are modelled to have the same functionality as the ASI input ports, and content received will be available to the multiplexer generating the output. The input streams can be either SPTS or MPTS and streams with or without RTP layer are accepted.

The multiplexer can generate 4 output multiplexes and the operator chooses whether to transmit these streams over IP or not. Each transport stream can be transmitted to up to 8 IP destinations.

Two Ethernet interfaces can be used simultaneously for video carriage, the interfaces are bi-directional. When using the SFP slot, one of the Electrical interfaces will be disabled.

5.5.2 Protocol mapping

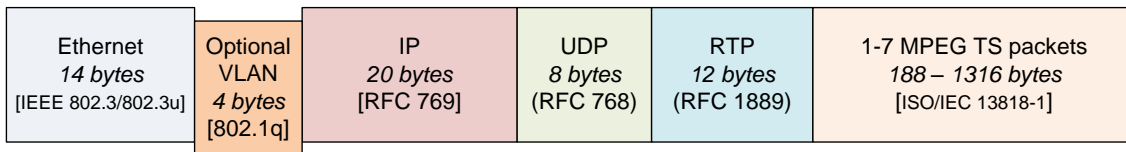


Figure 5.2 Protocol mapping

When transmitting and receiving MPEG transport streams over IP, the protocol mapping is according to figure 5.2. 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.

5.6 Management sub-system

The management subsystem is a set of modules that handles all the interfaces to monitor and control the operation of the CP524.

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.

5.6.1 Graphical user interface

Operators monitor and control the CP524 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 CP524 can be controlled from the web GUI.

5.6.2 Configuration database

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

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

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

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

- Device Name and Inventory ID
- IP network parameters
- ASI Port mappings
- On-device stored configurations

5.6.3 Alarm manager

The CP524 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 CP524 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.

5.7 Time synchronisation

The CP524 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 one of the ASI/SMPTE 310M ports (using TDT/TOT or STT)
- 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.

The internal clock can be used for generation of TDT/TOT on the output.

5.8 TSP Module

The TS Processor (TSP) module is the heart of the unit. Its job is to create a new MPEG Transport Stream based on configuration and current input signals. Figure 5.3 shows the different components in the TSP subsystem.

The lower left hand corner represents the interface between the management subsystem and the TSP subsystem.

The central process in the TSP module is the TS Builder, which handles the logic creating PID routing and regenerate PSI/SI/PSIP based on configuration and current PSI/SI/PSIP tables. See Section 5.8.6 for more details on service and PID routing.

The following chapters covers more on the different modules shown in the figure.



Note: The overall architecture of the TSP module, and the description in this chapter, is shared between several products in the cProcessor product family, but not all modules are available on every product.

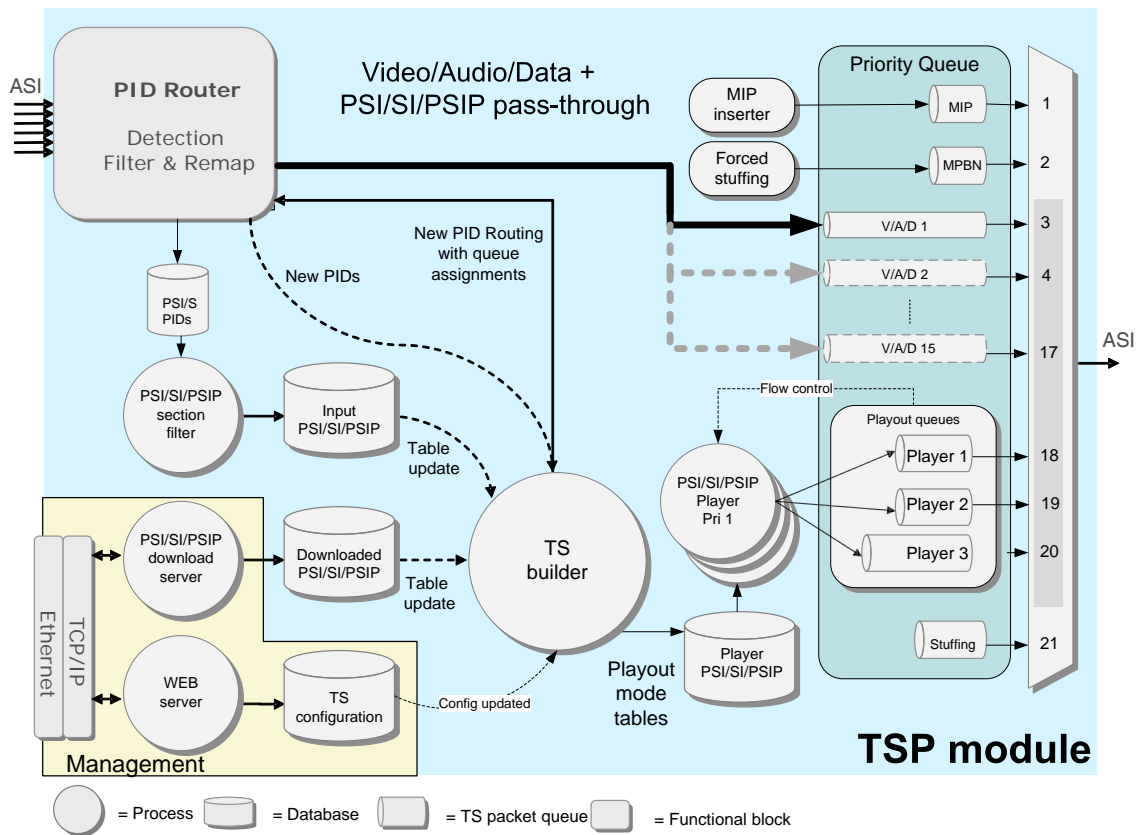


Figure 5.3 TSP module

5.8.1 PID Router

A PID router module tells the TS Builder which PIDs are present.

The router is used by the TS Builder to pass on the correct elementary streams from the input to the output. New PID values can be assigned to any elementary stream. One elementary stream can only be transmitted on an output once, so one input PID can only have one output PID value. This is reflected in the GUI and configuration structure.

TS packets that have a route to the output are travelling on the “main highway” through the unit. This is where video, audio and other service components are passed. Packets that are filtered do not have a route.

The output TS packets carrying PSI/SI/PSIP may either be routed through on the highway, or they are played out through the PSI/SI/PSIP playout module. This is one of the most important details to learn from figure 5.3, since the applied configuration determines the data flow direction.

The PSI/SI/PSIP TS packets on the input can, in addition to being routed on the highway to the output, be routed to the PSI/SI/PSIP section filter module, which is briefly described in section 5.8.2.

Read more about the prioritisation of data in chapter 5.8.4.

5.8.2 PSI/SI/PSIP section filter

The PSI/SI/PSIP section filter is a real-time process in the system. It receives continuous streams of TS packets on the different PSI/SI/PSIP PIDs and checks the content for version number updates. One PSI/SI/PSIP table section can span a number of TS packets. The filter keeps state information for every PSI/SI/PSIP PID and re-builds the section blocks whenever a version number update is detected.

The output of the section filter module is re-created table sections (sub-tables). These are posted to the input PSI/SI/PSIP database, which in turn triggers an event to the TS Builder.

5.8.3 PSI/SI/PSIP playout module

The PSI/SI/PSIP playout module is the reverse of the PSI/SI/PSIP section filter, and generates a continuous streams of TS packets from PSI/SI/PSIP sections. PSI/SI/PSIP tables that are configured in any “Playout” mode (see section 8.6.2.7), are posted through this module. Tables are played out via the PSI/SI/PSIP playout module according to the user configured repetition interval.

An important detail in figure 5.3 is the arrow tagged with “Flow Control” pointing from the player output queues to the PSI/SI/PSIP player. This means that data played out here is under flow control making loss of TS packets unlikely. The flow control mechanism also makes it possible to configure a SI/PSIP playout that fills up spare capacity with EIT packets, since a buffer can be kept full with packets to insert when there is spare capacity.

The playout module prioritises data in 2 levels; first by dividing the different table types into 3 groups that are handled by system processes of different priority, then by assigning each PID stream to one of 3 packet posting queues with different priority level. All packets on one PSI/SI/PSIP PID must be transmitted on the same queue to assure the the packets are transmitted in sequence.

Table 5.1 shows the table_ID-to-process assignement in the first level of prioritisation.

Table 5.1 PSI/SI/PSIP playout table ID process priorities

Process Table IDs	
Priority	
1	PAT, CAT, PMT
2	NIT actual, SDT actual, EIT p/f actual, TDT, TOT, STT, RTT, MGT, VCT.
3	NIT other, SDT other, BAT, ETT, EIT p/f other, EIT schedule actual and other



Note: The priorities in table 5.1 are the priorities referred to by the output alarm “Pri X tables delayed” where x is the priority level.

Table 5.2 shows the table PID to queue number assignment in the second level of prioritisation. The actual priority of each of these queues can be configured, but the normal case would be to use falling priority for these queues.

Table 5.2 PSI/SI playout table PID to queue assignment.

Table 5.3 shows the table PID to queue number assignment in the second level of prioritisation

Player Queue Tables	Corresponding PID Values
Player 1	PAT,CAT,PMT,TDT 0, 1, PMT*N, 20
Player 2	NIT, SDT
Player 3	EIT

in ATSC mode.

Table 5.3 PSI/PSIP playout table PID to queue assignment.

Player Queue Tables	Corresponding PID Values
Player 1	PAT,CAT,PMT
Player 2	MGT/TVCT/CVCT/SST/RRT 8187
Player 3	EIT/ETT

See [Section 5.9](#) for a more details on PSI/SI/PSIP playout.

5.8.4 Output Priority Queue

The right hand part of figure 5.3 represents the TS packet output priority queue of the TSP. It indicates that all data is prioritised before being output.

The CP524 generates a constant (configurable) output bitrate translating to a fixed number of available packet slots per time unit. Data from different sources are mapped to the priority queue on the output to compete for the available bandwidth according to the configured priority rules. Some data sources have fixed priorities to assure proper behaviour; other data source priorities are configurable. The ones that are configurable are framed with a darker grey rectangle within the MUX symbol in [Figure 5.3](#).

PID sources fall into the following different categories:

Table 5.4.a Priority queue categories.

Cat.	Sub-group	Name	Description
A	1	MIP inserter packets	If the CP524 is set to operate as an SFN adapter and MIP packet transmission is configured, the MIP packets are transmitted at fixed packet positions. To assure exact positioning, these are transmitted with highest priority.

Table 5.4.b Priority queue categories.

Cat.	Sub-group	Name	Description
B	1	Forced stuffing	Downstream equipment may require a certain amount of stuffing packets to operate properly. This may be guaranteed by activating the forced stuffing function, specifying the maximum number of TS packets between each stuffing packet. This packet transmission operates at fixed priority just below the MIP inserter, therefore the max distance between each null packet may deviate with 1 from the configured value if used in combination with MIP insertion.
C	1	Components routed from input (video/audio/data)	This is typically audio or video components belonging to an input service that are to be inserted into the outgoing stream. CP524 will be able to buffer these packets for a significant time, but the delay through the unit shall generally be as short as possible.
	2	Transparent input PSI/SI/PSIP	Dependent on the configuration for PSI/SI/PSIP table handling, the input PAT and PMT tables may be transmitted transparently as components through the unit. No caching of these tables will be done; they are let through on a packet-by-packet basis.
	3	Unreferenced PIDs	Unreferenced PIDs are components that are not signalled in any services.
D	1	Table data from internal carousels (PSI/SI/PSIP player)	When PSI/SI/PSIP tables are configured for playout via the PSI/SI/PSIP player, the tables are cached internally and are played out at the configured intervals according to algorithms described in this document. PID streams generated by the PSI/SI/PSIP player are divided into 3 sub-groups on which the priority can be controlled individually. The 3 queues are shown in table 5.2
E	1	Null packets	These packets are stuffing packets that are transmitted when no other source requests transmission of packets, i.e always at the lowest priority.

MIP insertion, and hence Group A, is not available on the CP524.

Groups A, B and E have fixed priority, while the priority of the queues within the C and D group may be freely configured. Group C and D queues can also be assigned a maximum bandwidth.

Queues in group C are handled without flow control, meaning that packets will be discarded if there is not enough packet positions on the output to empty the packets filled into these queues. This will also happen if the bandwidth for each queue exceeds the configured shaping threshold.

Group D queues used by the PSI/SI/PSIP player **have** flow control, allowing the player to suspend waiting for available space. This means that if the D groups are configured with lower priority than the C groups, and the available bandwidth after passing video/audio is less than the bandwidth required to play out PSI/SI/PSIP at configured rate, the PSI/SI/PSIP player will stagger on the queues, trying to fill up remaining capacity on the output. If the pass-through data is not varying too much in bitrate, it will actually be able to fill up the stream, with the effect of not having any stuffing packets inserted.

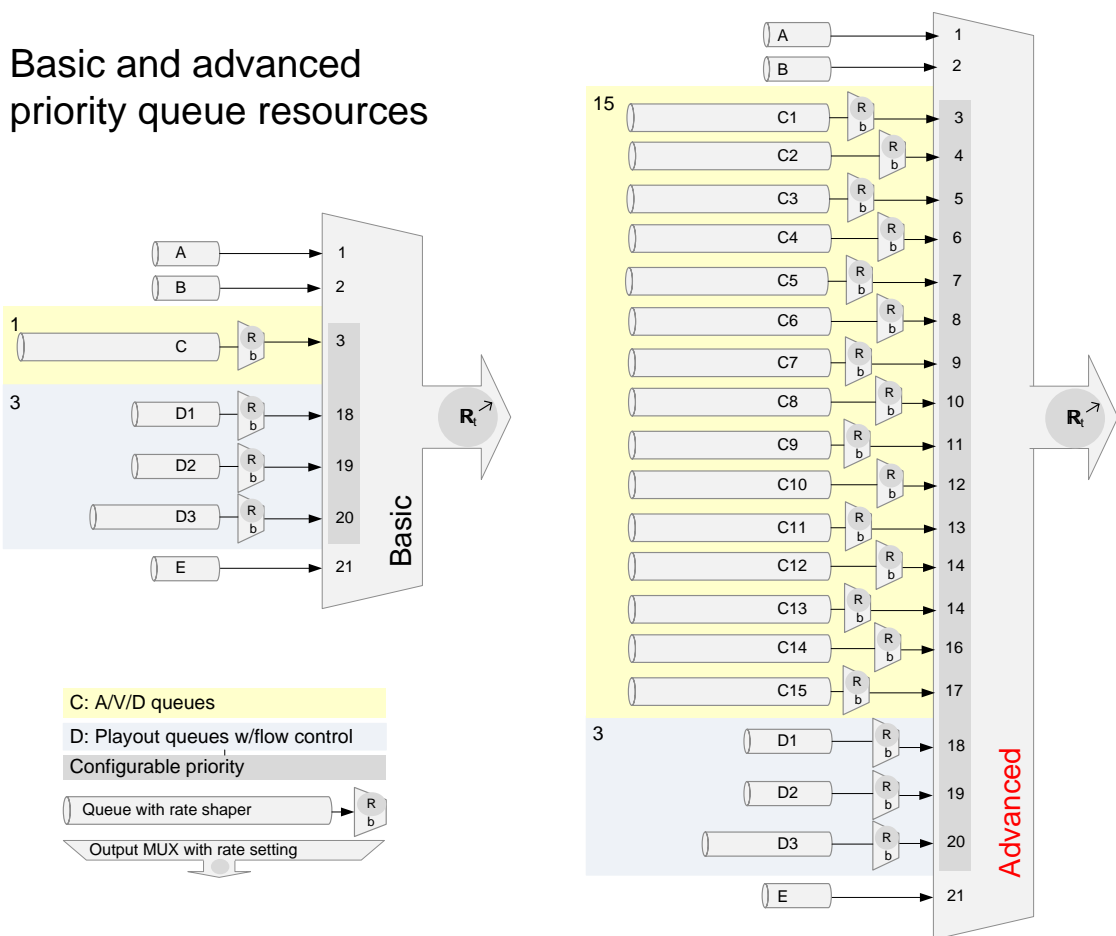


Figure 5.4 Basic and Advanced Priority queues

There are two main variants of the priority queue as presented in figure 5.4.

The basic variant to the left, offers 1 queue for category C data and the 3 shown queues for group D data. Priorities can be freely configured between the category C and D queues.

The advanced queue configuration is only available on some products. Different flavours of queue structures may exist.

5.8.5 Bitrate shaping algorithm

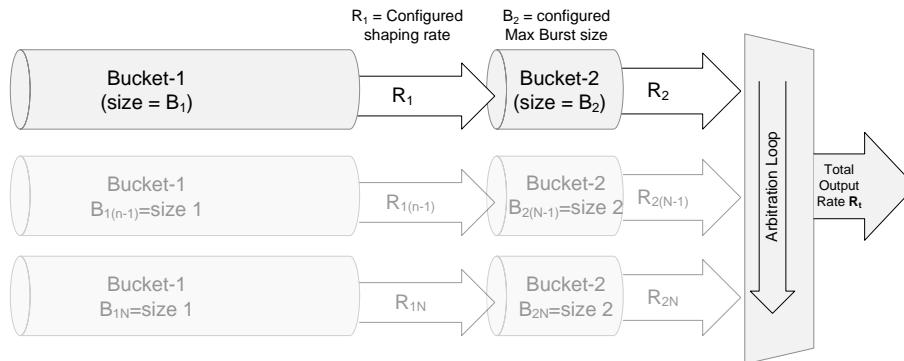


Figure 5.5 Dual leaky bucket algorithm for bitrate shaping

Category C and category D queues (section 5.8.4) support configuration of bitrate shaping to assure data is discarded if exceeding a configured threshold.

The method used for shaping is a “dual leaky bucket” algorithm illustrated in figure 5.5.

The configurable parameters are R_1 (Shaping) and B_2 (Max Burst). $B_1 + B_2 \leq B_t$, where B_t is 128 on the current implementation.

TS packets are dumped into bucket-1 when they arrive, and are extracted into bucket-2 at the configured shaping bitrate R_1 . Only queues that have TS packets in bucket-2 participate in the competition for a packet slot on the output. The highest priority queue that has a packet in bucket-2 wins.

The maximum extraction rate R_2 from a queue is R_t , i.e the configured total output bitrate. The B_2 parameter is referred to as “Max Burst” since, even with an R_1 that is much lower than R_t , B_2 packets can be transmitted back-to-back at R_t if bucket-2 has been able to build up for some time due to higher priority queues having data to send.

5.8.6 TS Builder - Service and PID routing

The TS Builder reacts to the following events:

- Configuration changes that affect the output Transport Stream.
- New PSI/SI/PSIP table arrived on any input, or a table has timed out on the input.
- Table update in the downloaded PSI/SI/PSIP database.
- Changes to the list of present PIDs on any input.

When activated, the builder retrieves information from the different databases and from the PID lists, to create new PID routing.

If PSI/SI/PSIP tables are configured for playout, they are generated and posted to the PSI/SI/PSIP playout module for continuous packetisation and repetition.

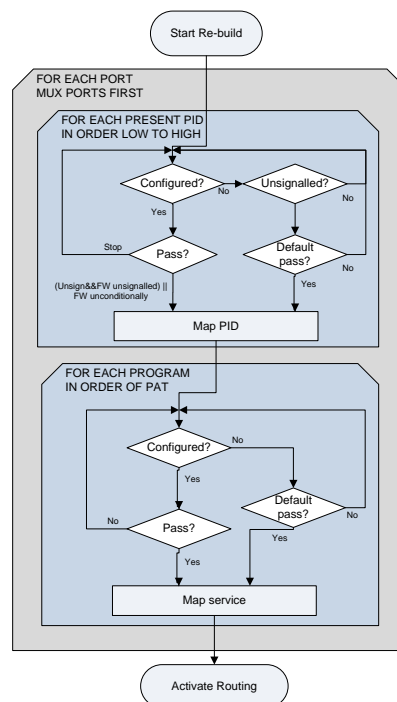


Figure 5.6 Service routing

Services and PIDs are passed or stopped based on configuration choices made by the user or by the system. Both services and components may be passed or stopped implicitly with a default rule, or explicitly with an include or exclude rule.

Re-mapping of service ID and PID values requires an explicit routing rule.

The process of selecting services and unsignalled PIDs to pass can be illustrated by the flow chart in figure 5.6.

First, each present PID is checked for a PID configuration rule. If there is no explicit configuration entry, unsignalled PIDs may be routed or stopped by a default rule. Signalled PIDs can only be routed here if they are tagged with a pass-unconditionally rule.

Then the incoming PAT is traversed and the programs are routed in the order of which they appear in the incoming PAT. If a program has an explicit rule, that rule is used either to stop or forward the program. If no explicit rule is found the default rule for services on that port is used either to stop or pass the service.

The 'Map Service' block in the service routing diagram involves forwarding the wanted service components for that service. This process is illustrated in figure 5.7.

As can be seen from the figure, service components are traversed in the order they appear in the incoming PMT for the program. Then the same logic is applied to components merged from other programs, and then the PCR PID before the known ECM PIDs. The order of traversal determines which PIDs are dropped in the event of a PID conflict.

At the top of the loop we can see that the global PID table is checked for stop commands and global re-map entries first.

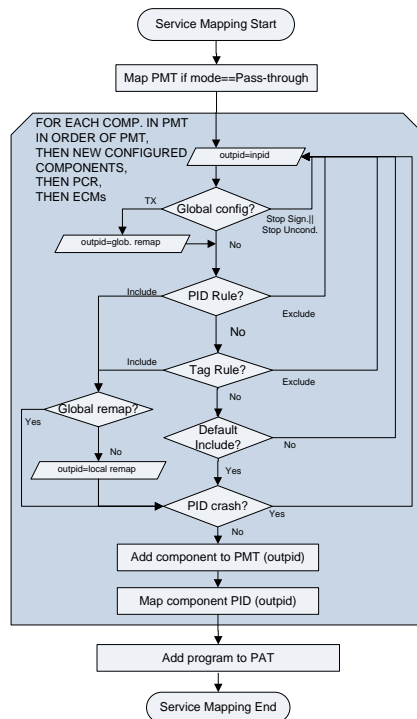


Figure 5.7 Service component routing

PID rules are looked for before tag rules, and local re-mappings stored on either a PID rule or a Tag rule are only used if no global remapping was found.

If no rule exists for the component, the default behaviour is retrieved from the service configuration for the given service. If this service is routed by default rule, the default component behaviour is to pass the component.

If a PID conflict is detected with a PID previously routed in the routing process, the new PID is filtered and an alarm is activated.

5.9 PSI/SI/PSIP payout

The CP524 contains a payout module for PSI/SI/PSIP tables as shown earlier in section 5.8.3. This module is designed to repeatedly transmit any legal PSI/SI/PSIP table to the CP524 output transport stream.

The PSI/SI/PSIP played out is managed on a table to table basis, and may be sub-sets or complete sets of tables retrieved from the inputs, or complete sets downloaded from an external SI/PSIP system.

The alternative to playing out PSI/SI/PSIP via the SI/PSIP player is to pass through PID elementary streams in the same way as for audio and video.

5.9.1 Main configuration

The fundamental configuration parameter for the playout module is to specify a wanted *repetition interval* for a given table ID. Each table (identified by `table_id` and a number of sub-id's) is played out regularly at the given interval. The repetition interval indicates the maximum time a receiver must wait before the table is received and is therefore an indication of the perceived quality of the service (wait time before receiver has fetched all information).

The dependency between repetition interval and resulting bitrate is dependent on several factors:

- The number of tables that should be played out
- The size of each table; larger tables yields higher rate

For a given table ID and corresponding sub-ID's, the playout module will aim to keep the configured repetition interval. It will also play out the tables such that the requirement for minimum distance between sections (25ms) will not be violated.

5.9.2 Carousel priorities

Within the PSI/SI/PSIP player, there are 3 priority levels for tables as shown in table 5.2 in chapter 5.8.3. The priority levels become significant when there is not enough bandwidth available in the output stream.

The PSI table queue is typically placed at a high priority level, above data routed from the input to assure PAT and PMT is transmitted even in an overload situation.

The EIT queue is typically configured at lowest priority with a high bandwidth limitations if one want to fill up rest capacity with EIT. Another option is to configure the EIT queue at high priority but with a limited bandwidth to create an EIT stream with sub-table repetition intervals that are not influenced by other content on the output, but with a controlled bandwidth consumption.

5.9.3 Carousel bitrate

In a typical scenario, the available Null packet rate available for PSI/SI/PSIP playout will be variable, as shown in figure 5.8.

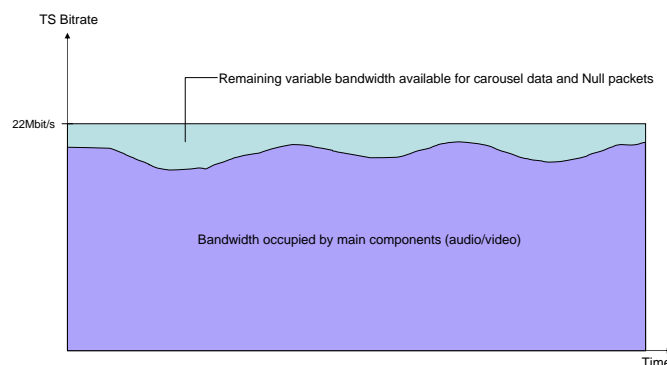


Figure 5.8 Illustration of remaining variable bandwidth in transport stream

It will be possible to configure at least 3 scenarios with the CP524 product.

1. There are plenty of available bandwidth in the transport stream, and the resulting bandwidth due to repetition rate configuration fits well within the available bandwidth.
2. The configured repetition rate results in a bandwidth that is too high compared to the available bandwidth. The playout carousel will utilise all available bandwidth.
3. Carousel max. bitrate is set to a certain value to guarantee a certain amount of Null packets in the outgoing transport stream. If the repetition intervals are set sufficiently low, the carousel playout will utilise all the bandwidth within the configured limits.

The 3 scenarios are shown in figure 5.9.

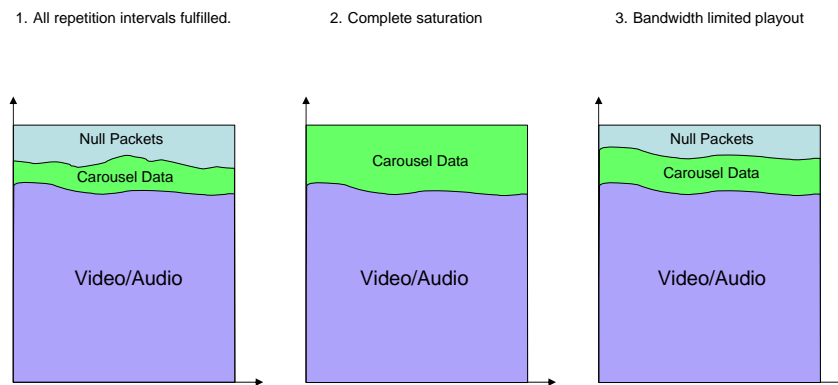


Figure 5.9 Three different playout scenarios

For case 2 and 3, we have a *saturation* scenario, e.g. the carousel will completely fill up the configured bandwidth. In this scenario, the configured repetition intervals will *not* be fulfilled. All configured tables will “suffer” a certain amount. The expected behaviour for this scenario is described in the next section.

5.9.4 Bitrate saturation handling

This chapter does not apply in ATSC mode.

In the descriptions below, we assume that the different tables are played out on *the same carousel priority level*, for example priority level 3.

Scenario: The configured repetition intervals lead to a bandwidth that is higher than the configured bandwidth. The playout carousel will continuously try to transmit tables to the output, leaving no room for null packets at all.

In this case, the playout module will try to “spread” the resulting delay equally across all tables, independently of configured interval.

An example may illustrate this:

- Assume that one EIT table group is configured with 9 seconds repetition interval while later groups are configured with 27 seconds interval and this leads to a saturation scenario.
- A resulting scenario in this case may be that *all* tables will suffer 3 seconds higher repetition intervals
- The interval for the first group will increase from 9 to 12 seconds while the interval for the second group will increase from 27 to 30 seconds.

Note that the scenario above is just intended for illustration. In practise, the suffered delay will vary dependent on the available bitrate in the stream. There will also be a small random variation in the delays due to variable section lengths etc.

5.9.5 Configurable back-log time

This chapter does not apply in ATSC mode.

Refer to chapter 5.9.4 regarding bitrate saturation handling. In case the output bitrate is configured too low to keep up with the configured repetition intervals, each output table will “suffer” a certain time for each repetition cycle. Compared to the “ideal” playout time, each section will be more and more delayed.

When the output bitrate capacity becomes high enough again to keep up with the configured repetition intervals, there are basically two ways to go:

1. Accept the resulting introduced delay and just continue using the normal repetition interval. The wanted repetition interval has then not been achieved for the time period that passed.
2. Try to utilise the extra capacity available and “speed up” transmission by using a lower repetition interval. In this way, it is possible that the *average* target repetition interval will be fulfilled.

CP524 allows for both strategies, using a configurable “back-log” time. Figure 5.10 illustrates the concept.

The dark green graph illustrates the “ideal” transmission time for each section. It is a long line with “even” spacing between each table section.

The purple graph illustrates a table that does not allow for “back-log”. In period B, the distance between each section again becomes the normal, configured interval.

The red graph illustrates the case when a back-log is configured larger than zero. In this case, the CP524 will actually reduce the transmission interval until the “ideal” line again is reached. This means that the average repetition interval will be fulfilled.

The back log time is controlled by a configuration parameter “Backlog time”, which is specified as a fraction of the repetition interval. The default value is 1.0, which indicates that a table is allowed to be delayed by time for one, complete repetition interval.

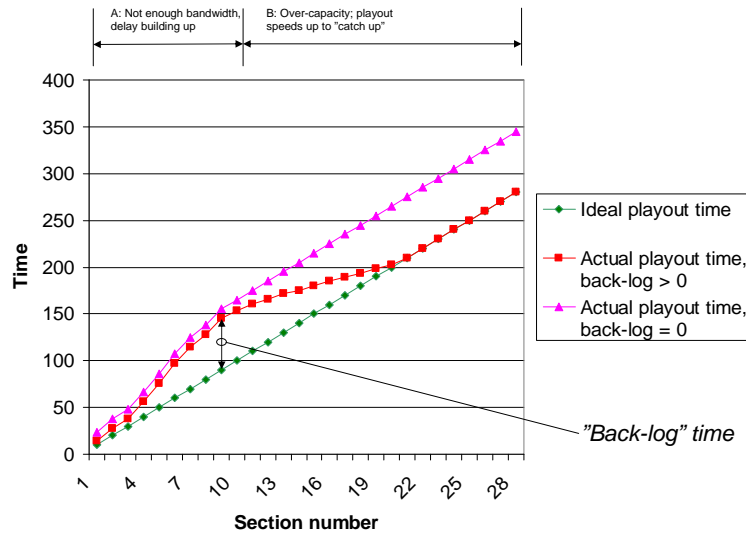



Figure 5.10 Illustration of back-log principles

5.10 Service fallback

5.10.1 General

The CP524 offers a SW module for redundancy on service level. The module monitors the alarm level for two services and selects the best service according to the user specified switching criterias.



Note: Service fall-back is a licensed feature and this tab is only visible if the licence key is installed.

A block diagram of the service fallback switcher is shown in figure 5.11

The service fallback switch controller only relates to *alarm levels* for the two corresponding services and the ports for each service. It is up to the user to configure appropriate alarm levels for each of the alarms an input/service is able to generate. The switching criteria are configured as follows:

For each alarm level (starting with the highest, most severe level), the following configuration is done:

- Enable/disable switching for this level
- Required alarm level of the other (spare) input to allow switching

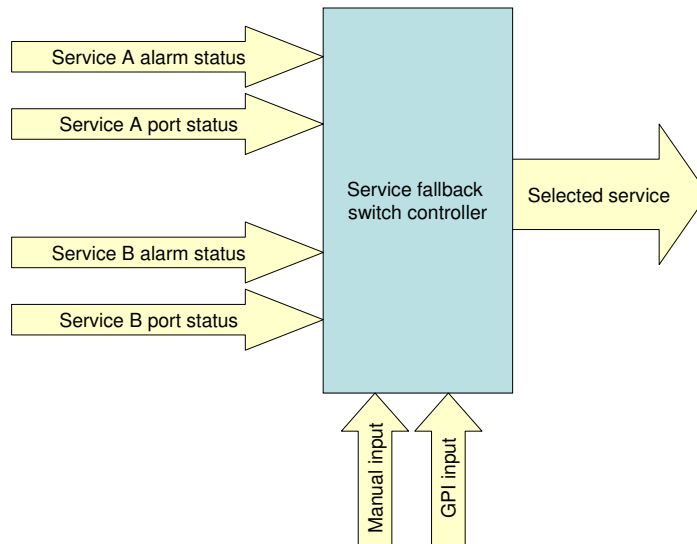


Figure 5.11 Service fallback block diagram

- The confirm time for this level (how long to wait before doing a switch)

The required level of the other service needs to be lower than the configured level, e.g. when configuring the switch criteria for “Critical (6)” main level, the spare input must be on level “Major (5)” or lower.

Example: A very simple configuration may be to *only* switch on “Critical (6)” level and require “OK (1)” level on the spare input.

The switch controller is designed as a state machine that uses two timeout values in order to avoid regular switching between the two inputs.

A simplified state chart of the controller is shown in [5.12](#).

In “auto” state, the switch controller is “armed” and continuously listens to change in the top level alarm status for each service. For each change event, the controller evaluates the levels and checks if the switching criteria is met. If the answer is “yes”, the controller does the following:

- If the `confirm_time` is zero, the controller does a switch immediately and jumps to a wait state where it will wait `switch_timeout` seconds before it re-enters the auto state.
- If the `confirm_time` is larger than zero, the controller jumps to a `wait_confirm` state to actually confirm that the switch criteria still is met after the configured time. If the criteria is still met, the controller performs a switch and jumps to the wait state. If the criteria is no longer met, the controller does no switching and jumps back to the auto state.

Both the `confirm_time` and `switch_timeout` can be individually configured for each service switcher.

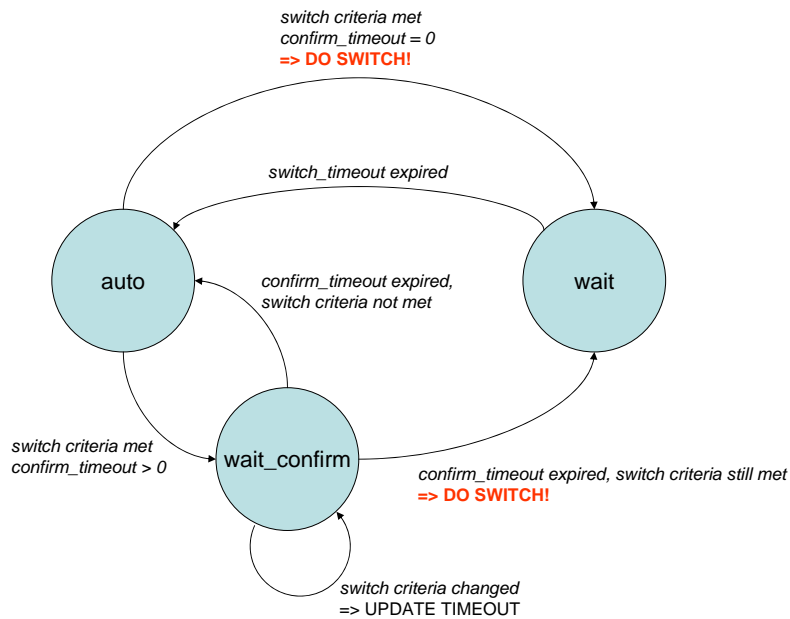


Figure 5.12 Service fallback switch controller state machine

The state of the switch controller (including timing information) is available in the GUI.

5.10.2 Details on confirm timeout handling

The `confirm_time` is configured for each severity level. I.e. a confirmation time for "critical" main input level can be set lower than for "major" and so on.

For example, 5 seconds may be configured for the "critical" state while 20 seconds may be configured for the "major" state.

A special case deserves more explanation: multiple alarms, with different severity levels, during the `wait_confirm` state. The controller is designed so that it will not "stay forever" in the `wait_confirm` state and will respond to the most critical alarm.

The controller has separate timers for each severity level, and each timer has an independently configured `confirm_time`. When an alarm event is detected the timer for that alarm level will be started and the switch will enter the `wait_confirm` state. When the timer reaches the `confirm_time` then the controller will perform a switch and enter the `wait` state. If, whilst the switch is in the `wait_confirm` state, a second alarm event occurs with a different alarm level then the timer for that alarm level will be started and will run "in parallel" with the timer for the first alarm event. There is then a "race" between timers and in this case the first timer to reach its `confirm_time` will cause the controller to perform a switch and enter the `wait` state at which point all alarm timers are reset.

Three example scenarios illustrate the behaviour. Assume that the controller is configured to switch at both "major" and "critical" levels.

The `confirm_time` values are configured as follows:

Major: 30 seconds

Critical: 5 seconds

Example scenario 1

- A major event is detected and the switch controller jumps to the `wait_confirm` state and the alarm timer for the major event alarm level is started.
- After 10 seconds, a critical event is detected and the alarm timer for the critical event alarm level is started. After a further 5 seconds the critical event alarm timer reaches its `confirm_time` and the controller will perform a switch. (The critical alarm timer “beats” the major event timer in the “race” to switch).

Example scenario 2

- A major event is detected and the switch controller jumps to the `wait_confirm` state and the alarm timer for the major event alarm level is started.
- After 28 seconds, a critical event is detected and the alarm timer for the critical event alarm level is started. After a further 2 seconds the major event alarm timer reaches its `confirm_time` and the controller will perform a switch. (The major alarm timer “beats” the critical event timer in the “race” to switch).

Example scenario 3

- A major event is detected and the switch controller jumps to the `wait_confirm` state and the alarm timer for the major event alarm level is started.
- After 10 seconds, a critical event is detected and the alarm timer for the critical event alarm level is started. After a further 2 seconds the critical event clears and the critical event timer is reset without a changeover occurring. After a further 18 seconds the major event alarm timer reaches its `confirm_time` and the controller will perform a switch. (The critical alarm exits the “race” after 2 seconds without a switch being carried out).

5.10.3 Manual switching on GPI

The service fallback module has the option to be manually controlled by a GPI (general purpose input) signal on the relay/alarm connector (see [6.1.6](#)).

This GPI signal can also be used to trigger a unit reset. Naturally, only one of the functions can be used at a time.

When used as an input to a service switcher, the GPI signal is used for manual switch over, performing the same action as when pressing the ‘switch to main’ or ‘switch to spare’ buttons (see [Section 8.6.2.5.4](#)).

[5.13](#) shows the timing constraints on the GPI input signal. The input signal is sampled 10 times a second, and a state change is detected on 3 consecutive samples in the same state after a flank.

The black lines in the diagrams show the input GPI signal, which is used to generate an internal GPI state signal shown in red. Whenever the GPI input state changes an event is sent to the service fallback switch controller, which will perform a switch if switching on GPI is enabled

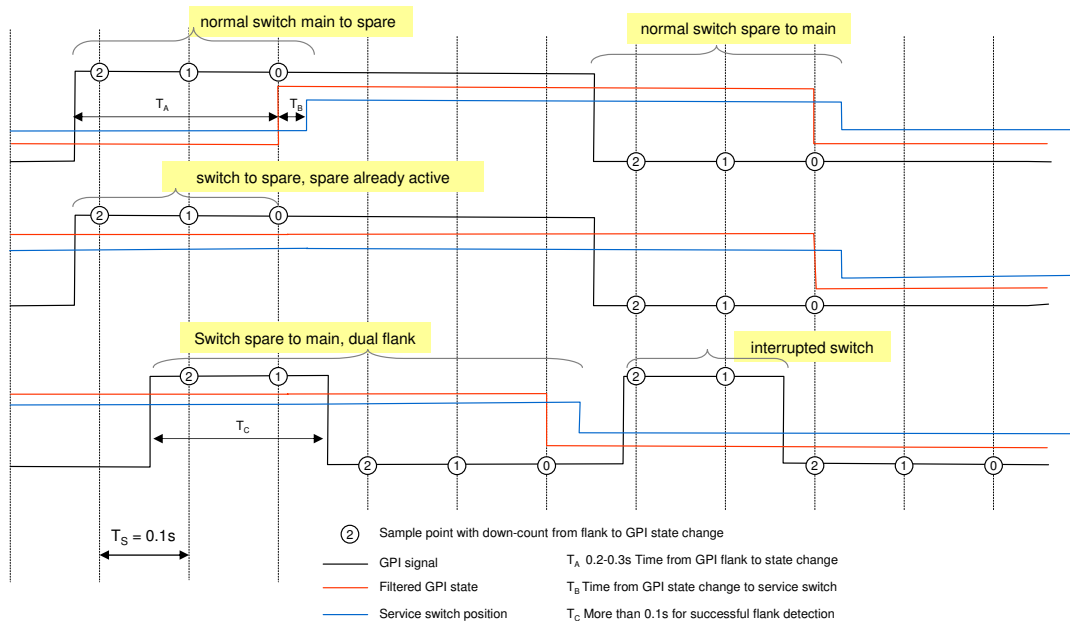


Figure 5.13 GPI timing diagram

and the new state signalled is opposite to the currently active service. The blue line, which indicates the currently active output service, shows that there is a delay T_B between the GPI state change and the actual performance of the switch.

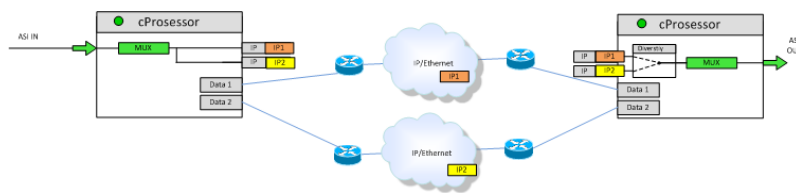
The first part of the last time line in the diagram shows how the GPI line should be controlled to perform a manual switch if the current level of the GPI is already in the same position as the wanted switch position. A pulse of slightly more than one sampling interval is required before pulling the signal back, to be able to detect a flank.

5.11 Hitless switching

The CP524 enables hitless switching by combining smallcast on the transmitter side with RTP/IP diversity reception on the receiver side. Hitless switching provides redundancy by protecting the stream against errors in IP transmission, but in a different manner compared to Forward Error Correction (FEC). FEC is designed to protect the stream against single or short burst packet losses, whereas hitless switching provides protection against loss of complete data input, for example, due to link or equipment failure.

The main idea of hitless switching is to transmit two identical copies of the data stream over separate network paths. At the receiver side, the data from the two incoming streams are combined at packet level to form one data stream. This way, if one of the network paths experiences severe packet loss or complete link failure, data from the other network path can be used to output an error free stream.

At the transmitter side, the CP524 allows sending identical copies of the data stream to a user defined list of destinations by enabling smallcast. During smallcast transmission all identical streams are tagged with the same, randomly generated Synchronization Source ID (SSRC). For each destination, the network interface (or a VLAN on any the interfaces) and separate unicast



or multicast destinations are selected so that the two data streams used for diversity reception are routed to their respective network paths directly at the CP524 or at the first subsequent network node.

At the receiver side, the IP source parameters are first configured as the master and slave sources (i.e. first and second IP source). When the data streams have identical SSRs, they are assumed to be identical streams and used for diversity reception. Diversity reception operates on the RTP packet level. The two incoming data streams are combined to form one error free stream as long as there is one correctly received packet from either input stream. There will be packet loss at the combined stream only when the packet is received on neither of the two IP sources. The data stream resulting from combining the two incoming data streams will then be processed as one RTP packet stream. RTP/IP diversity reception is a licensed feature and is required at the receiver side. No licence is required for smallcast transmission.



Note: If the same data streams are received at both sources, the sources will act as equal providers of data. If received streams at the sources are not identical, the data from the master IP source will be used and data from the slave IP source will be discarded.

5.12 Redundancy controller

The Embedded Redundancy Controller is a generic software module that implements redundancy schemes. The module is included in the operational device; external PCs are therefore not required for operation.

One separates between *main* and *spare* devices. A spare device continuously monitors the health of an associated main device. When the spare detects a critical alarm condition in the main device, the spare will take the necessary actions to replace the main device. The redundancy controller will never switch back to the main device automatically; this operation requires manual operator intervention.

The main device requires no additional configuration when used in a redundancy scheme. The only configuration needed is in the spare device since this unit controls the switching. The Redundancy Controller licence must be present in main and spare devices.

The communication between the devices relies on a proprietary XML protocol.

5.12.1 Operation

All redundancy control enabled T-VIPS devices advertise a set of services. A service might be an IP transmitter port, ASI port, SDI port etc. Any service on a T-VIPS device with redundancy control can be a spare for any compatible service on another T-VIPS device licenced for

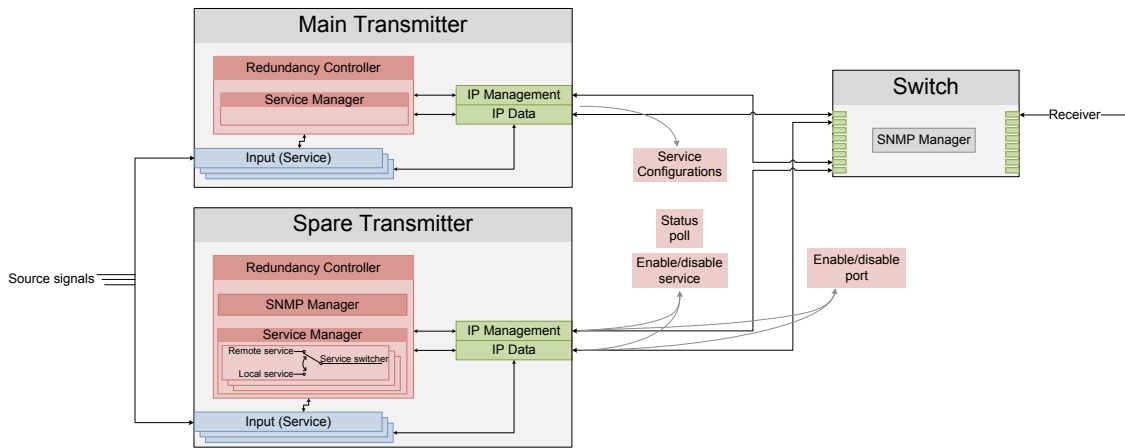


Figure 5.14 An overview of the embedded redundancy controller

redundancy control. The main tasks of the Embedded Redundancy Controller is to monitor the health of the main device and if necessary take over control of transmission of one or several services.

To be compatible, the two services must be of the same type and have the same service version number.

The Embedded Redundancy Controller provides a strict one-to-one redundancy solution. Two spare services cannot backup the same main service. A spare service cannot backup another spare service. A main service cannot have two spare services.

The system will always be in one of the three states shown in table 5.5.

Table 5.5 Typical states of the redundancy controller

State	Remote	Local
Normal operation	Output enabled	Output disabled
Remote service has alarm	Output disabled	Output enabled
No contact with remote device	Unknown, typically port on switch disabled	Output enabled

Normal Operation

The remote services are output and the local services are disabled. The redundancy controller polls the remote device for status and service configuration. In addition a set of SNMP OIDs can be monitored. These OIDs are set when a switch to local services is performed due to loss of contact with the remote device. The OIDs are also set when manually switching the entire redundancy controller between remote and local services.

Remote service has alarm

When the remote service has an alarm and the switch criteria are fulfilled the service switcher for that particular service will take the necessary actions to replace the remote service. This includes disabling the remote service before applying the remote service configuration to the local service and finally enabling output of the local service.

No contact with remote device

When the spare device loses contact with the remote device all service switchers will switch to local transmission. In addition a set of OIDs can be set via SNMP. The purpose of this is to be able to stop the transmission from the main device, even if there is no contact with it. The most typical use is to configure a switch behind the remote device to stop the data transmission from it.

The Embedded Redundancy Controller also offers automatic switch back to remote. After a switch to the local unit has been performed, the local unit continue to poll the remote device. When the remote device has recovered it is possible to perform an automatic switch back. The automatic switch back scheme is seperated into three different options, "Return if OK", "Return if local alarm", "No return".

Return if OK

This option will return automatically to the remote device, when the remote device has recovered and is OK.

Return if local alarm

This option will return automatically to the remote device if the remote device has recovered **and** the local unit is in an erroneous state.

No return

The no return option will disable automatically switch back. However, it is still possible to do a manually switch back to remote.

6 Physical Description

6.1 Connecting the CP524

6.1.1 Physical description overview

The front panel provides two LEDs per CP524. The meaning of each LED indicator is shown in table 6.1.

Table 6.1 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 also replicated on the rear panel, which is shown in figure 6.1.

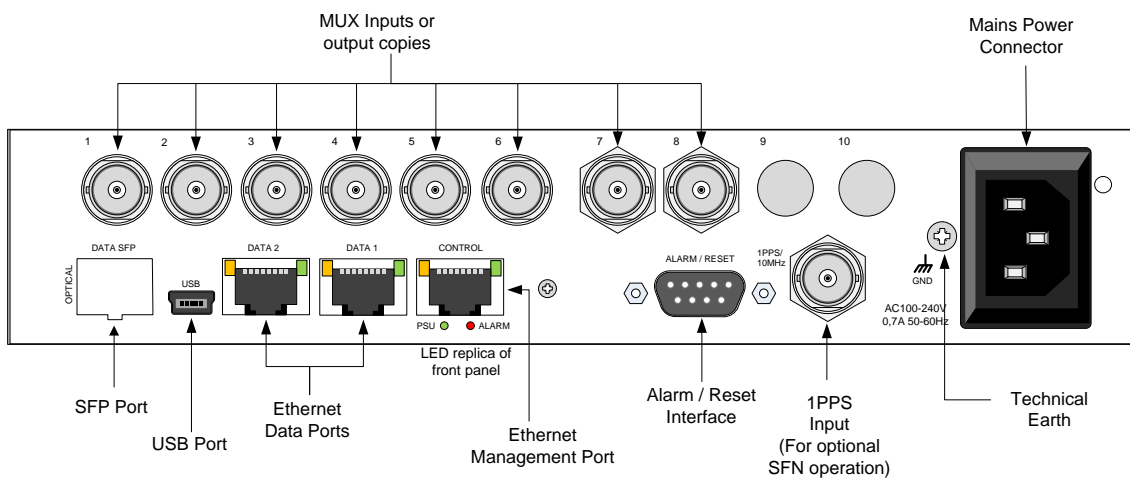


Figure 6.1 Rear panel

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

6.1.2 ASI ports

The CP524 is shipped with 8 ASI connectors on the back panel. The layout is as shown in figure 6.1. The ports have flexible direction control to best meet the usage scenario of the device.

The CP524 can generate up to 4 transport stream outputs, and each ASI port can either be used as an output carrying a copy of a TS, or as an input to an input switch or the multiplexer.

Switching the direction on a port does not require a re-boot, and can be performed while the other ports are in service.

6.1.3 ASI input ports

All physical ports are available for use as inputs, but the number of ports simultaneously enabled as inputs is limited by the licence key Number of input ports activated.

6.1.4 ASI output ports

Any of the physical ports can be configured to carry any of the output signals. The number of different transport stream outputs is limited by the licence key Output transport streams.

6.1.5 1 PPS Input

This coaxial connector is not used in the CP524.

6.1.6 Alarm/Reset

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 [8.4.2.3](#) for a description of how to program the relays.

The pin out of the connector is shown in table [6.2](#).

Table 6.2 Alarm/Reset
connector pin out

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

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

6.1.7 Electrical Ethernet data ports

The CP524 comes with two Ethernet data ports. These data ports can be used to carry MPEG transports streams if the licence key Ethernet data interface is installed.

These ports can also be used for management of the device.

6.1.8 Ethernet management port

The CP524 provides one Ethernet port for control and management. Connect the management port to the management network. The LEDs for the management port are used as follows:

Table 6.3 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

6.1.9 The SFP module

The SFP module (SFP = small form-factor pluggable) is a third-party product providing an extra, optional interface to the CP524. 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 6.2 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 CP524 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 CP524 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 8.4.8](#)).

The SFP interface must be expressly enabled from the CP524 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.

Note that when using the SFP slot, the "DATA 2" Electrical Ethernet port is automatically turned off.

6.1.10 Serial USB interface

USB interface:

- USB 1.1
- 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. The USB interface is intended for initial IP address setup.

6.1.11 Power Supply

Section [4.5](#) provides details of the power supply, protective earth and security. Read all these instructions, prior to connecting the units power cable.

6.1.12 Technical Earth

Connect the Technical earth to a suitable earth point.

7 Operating the Equipment

The CP524 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 CP524. 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.

7.1 Accessing the graphical user interface

The default IP address of the CP524 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 CP524 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 7.3.1](#).

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

Configuring the device functionality according to operational needs is done using the Web interface, see [Chapter 8](#).

7.2 Password protection

Remote access to the device is controlled by password protection. If you access the CP524 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.

7.2.1 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.

7.3 Changing the IP address of the unit

The CP524 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**.

7.3.1 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 CP524. Configure the PC to be on the same sub net as the CP524. See [Figure 7.2](#).
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 7.1](#) 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 7.2](#) shows how to configure the network interface in Windows XP to communicate with the CP524 with factory default settings. The IP address/netmask

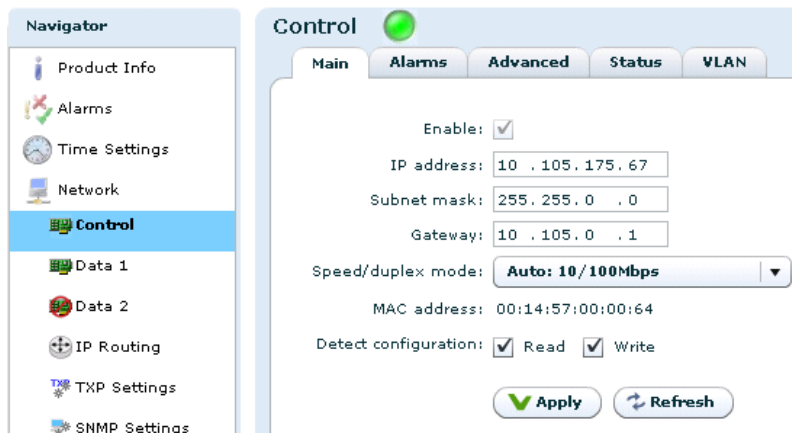


Figure 7.1 Configuring network settings via the Web GUI

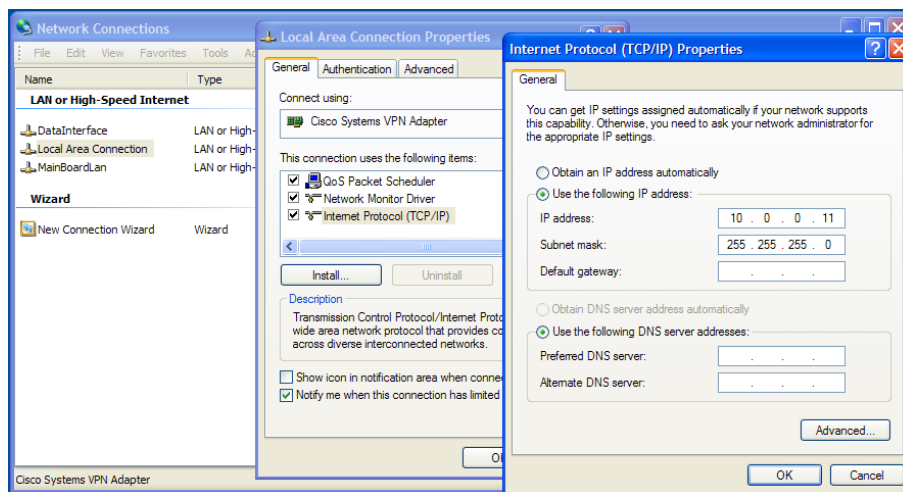


Figure 7.2 Setting static IP address 10.0.0.11 in Windows XP

is set to 10.0.0.11/255.255.255.0 which is on the same sub net as the CP524, 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 *'

7.3.2 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 CP524 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 CP524 contains a USB driver to use for serial communication with the device on the USB port. The MS Windows driver installation script is configured to give a one-to-one relationship between the physical USB port number on the PC and the COM port number to use on the PC. Drivers retrieved from <http://www.ftdichip.com> will also work, but these may not have the same COM port number mapping.

8 WEB Interface

The CP524 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 CP524 and get status information.

8.1 Login

Access the CP524 by entering its IP address in the address field of your favourite browser. When accessing the CP524 the first time, the progress bar ([Figure 8.1](#)) should appear while the Flash application is loading from the device.

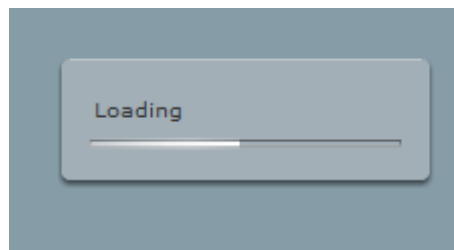


Figure 8.1 Flash application loading

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

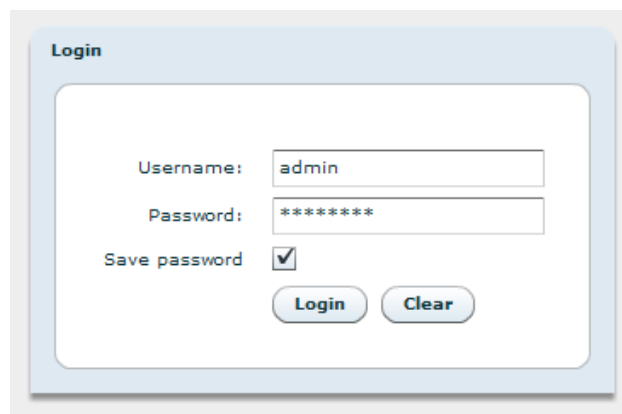


Figure 8.2 GUI login window

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

8.2 Status header

After successful login the start page is shown. The top part of the page (shown in [Figure 8.3](#)) is called the status header.



Figure 8.3 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 8.4](#). This pane is used to navigate between sub-pages of the tab.

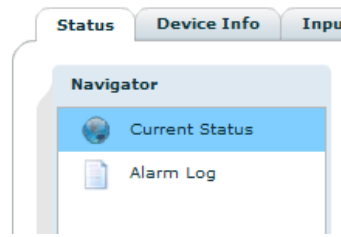



Figure 8.4 Status navigator

 **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.

8.3 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).

8.3.1 Current Status

Current Status

Status Summary

Device: ● Clock Reg: ○
PSI/SI/PSIP Load: 13%

Network diagram showing connections between ASI/310M 1-8, Unicast/Data 2, IP 1/2, MUX, and TS-OUT 1-4. Data flows are indicated with arrows and values like 20 Mbit/s, 20 Mbit/s, 21 Mbit/s, 20 Mbit/s.

Network Interfaces

- Control Link: 100 Mbit/s
- Data 1 Link: 1000 Mbit/s
 RX load: 634.7 Mbit/s
 TX load: 41.8 Mbit/s
- Data 2 Link: 1000 Mbit/s
 RX load: 42.7 Mbit/s
 TX load: 0.0 Mbit/s

Summary Options

Collapse IP inputs:

Current Alarms

Description	On Time	Alarm Type	Source	Alarm ID	Details

Figure 8.5 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.

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 CP524.

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](#).

8.3.2 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 is starting up	518

Alarms in log: 8 Enable updates

Figure 8.6 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 8.4.2.4](#). 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 CP524.

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.

8.4 Device Info

The device info page contains all the information and settings that are not related to a single input or output port. It is divided into multiple sub pages accessed via the navigation list to the left. In the list of physical interfaces in the navigation list, the currently active interface is shown in bold. See [Figure 8.7](#).

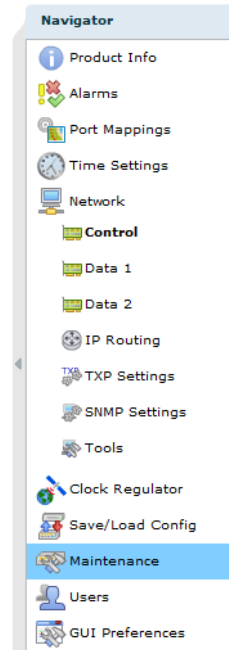


Figure 8.7 Device Info navigator

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

8.4.1 Product info

The product info page contains general device information.

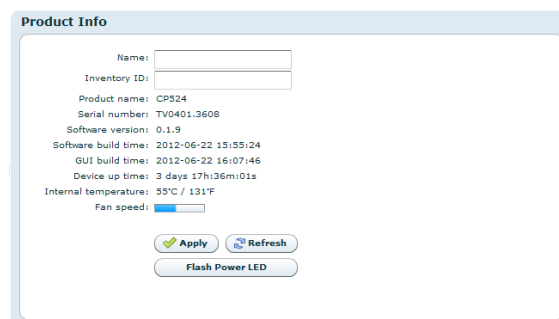


Figure 8.8 Product Information

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 8.4.7](#). The device name is shown in the web GUI status header (see [Section 8.3.1](#)), and in the web browser title bar to facilitate identification of each device.

Product name

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

Serial number

The serial number of the device.

Software version

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

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

The convention for the SW version numbering is as follows:

major_version

Incremented for significant SW changes.

minor_version

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

patch_version

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

Software build time

Reports the time of which the current release image was built.

Device up time

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

Internal temperature

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

Fan speed

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

Flash Power LED button

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

8.4.2 Alarms

The Alarms page is shown in [Figure 8.9](#):

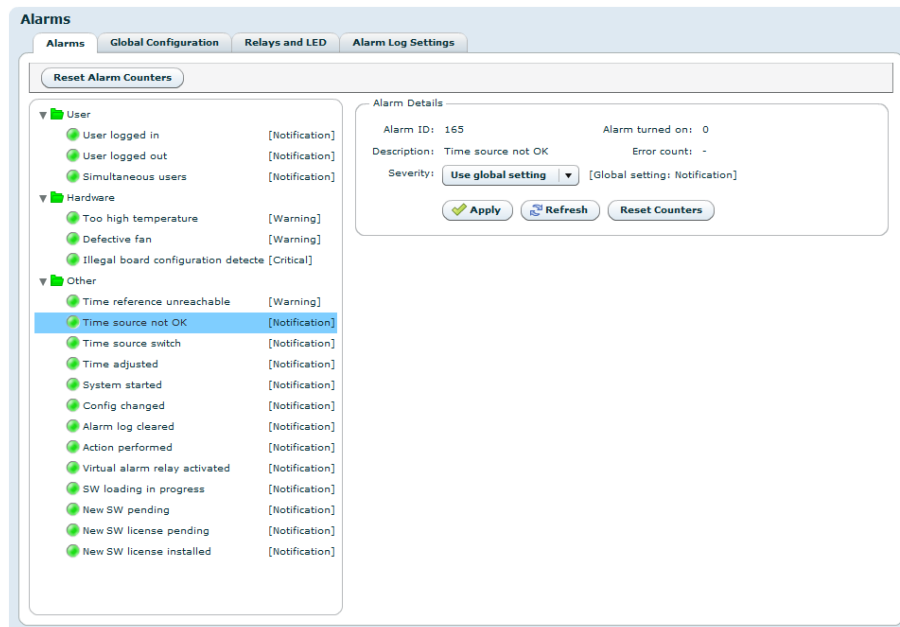


Figure 8.9 Alarm configuration

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

8.4.2.1 Device alarms

The page shown in [Figure 8.9](#) 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

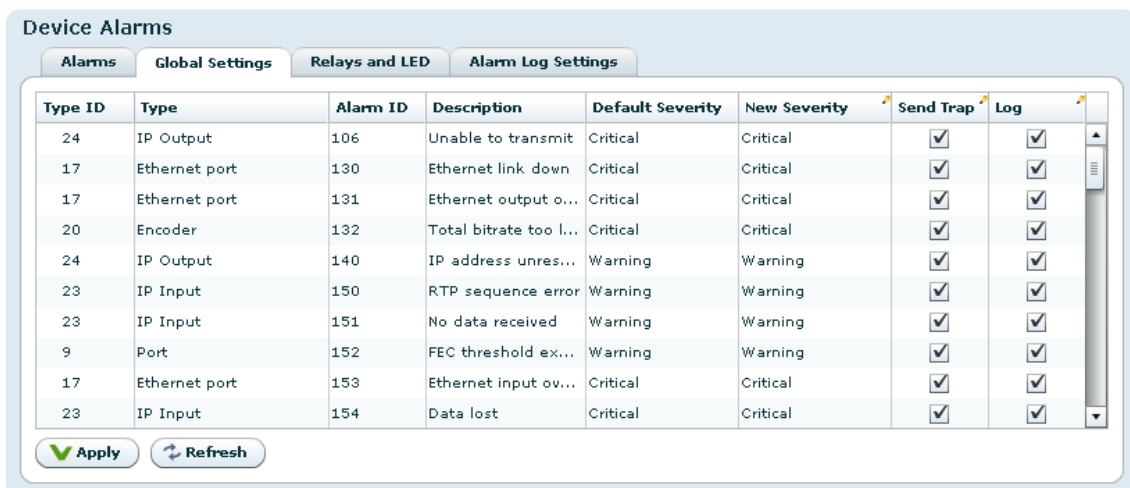
Not used.

'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.

8.4.2.2 Global configuration




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"/>

Figure 8.10 Global alarm configuration

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

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

Edited rows are highlighted until changes have been applied.



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

8.4.2.3 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.

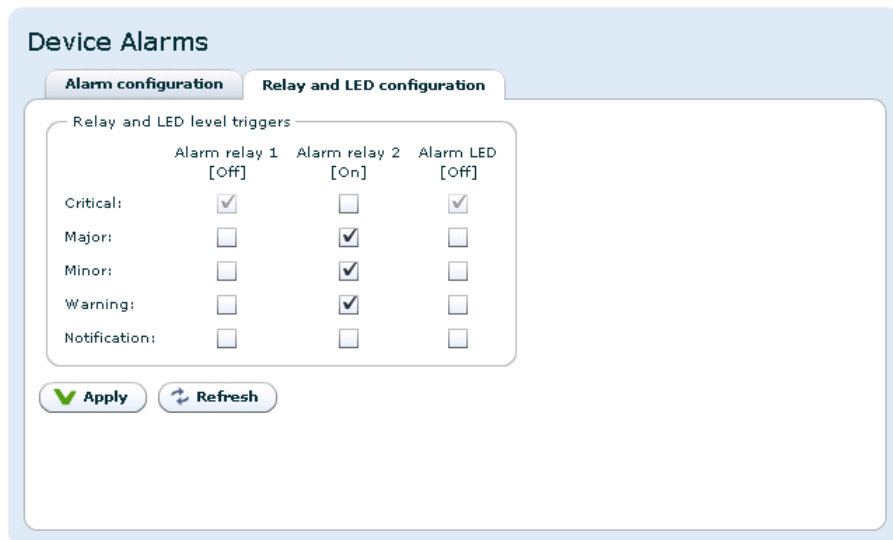


Figure 8.11 Relays and LED configuration

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

The Virtual Relays field shown in [Figure 8.11](#) 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 8.1** shows the field values you may enter in an expression.

Table 8.1 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 8.2 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 8.2.a Legal operators to use in expressions

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

Table 8.2.b Legal operators to use in expressions

Operator	Description	Sample
*	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 8.3](#).

Table 8.3 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.

8.4.2.4 Alarm log settings

This page is used to set alarm log properties.

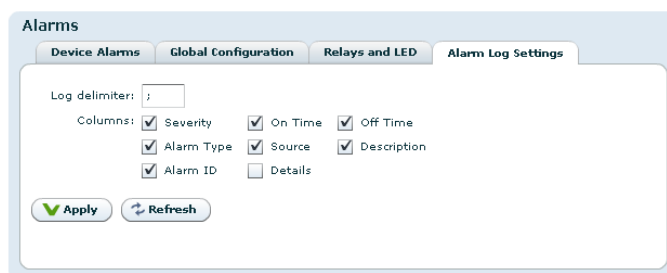


Figure 8.12 Configuring the alarm log

Log delimiter

This parameter is used when exporting the alarm log. It specifies the column separator

character. The default value for the delimiter is ;. The character used may affect auto-importing of the exported file into your favourite tool used to inspect the file content.

Columns

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

8.4.3 Port Mappings

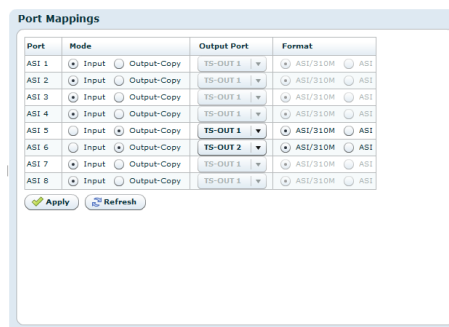


Figure 8.13 ASI port direction control

This page offers an interface to configure the direction of the installed ASI ports. The valid options are visible as selectable radio buttons for each port.

The number of ports shown in the port map grid corresponds to the number of physical connectors installed in the chassis and the meaning of the different choices are:

Mode

Direction of the port, with two choices:

Input

Use the port as an ASI input to the multiplexer. All input ports can be used, but the number of inputs that can be enabled simultaneously is limited by the licence key Number of input ports activated.

Output-Copy

Use the port as an ASI output, transmitting the multiplex generated by the unit.

The valid selections are also documented in [Section 6.1.2](#).

Format

Additional option for output ports, only available in ATSC+DVB mode. This option makes it possible to transmit both ASI and SMPTE 310M simultaneously, the ports carrying the same content.

ASI/310M

The format on the output port follows the format configured on the TS-OUT port.

ASI

The port is always using ASI, even when the TS-OUT is configured to SMPTE 310M.

Configure the mapping that best matches your needs and press apply to activate the new matrix. Re-configuration does not require re-booting. The choices made will be reflected in the logical block diagram of the device on the status screen (see also [Section 8.3.1](#))



Note: The port map settings are tagged to follow the device (see [Section 5.6.2](#), and even though the parameters are exported in the configuration file format, they are not overwritten when loading a configuration file via the GUI to another device.

8.4.4 Time Settings

Figure 8.14 Time Settings

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

The page consists of 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.

8.4.5 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 8.15 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.

8.4.5.1 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.

8.4.5.1.1 Main

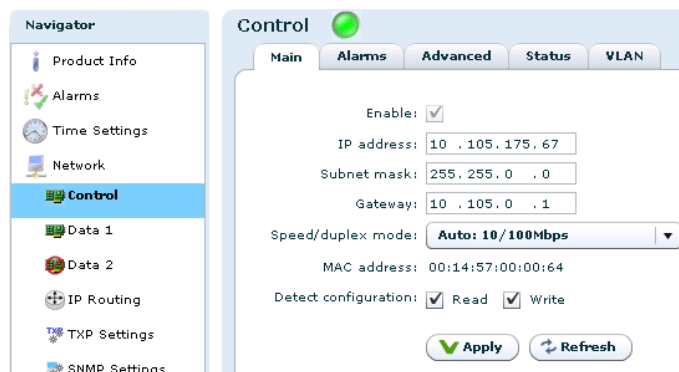


Figure 8.16 Main IP settings

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)[\)\(http://en.wikipedia.org/wiki/Duplex_mismatch\)](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 CP524 visible for the T-VIPS Detect on the LAN. If the Write option is enabled the IP address of the CP524 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.

8.4.5.1.2 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 8.4.2](#) for alarm configuration details.

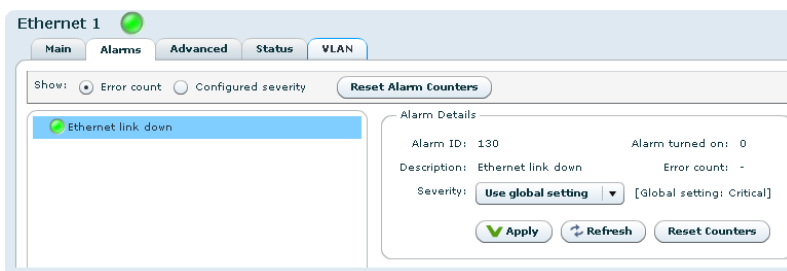


Figure 8.17 Network interface alarms

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.

8.4.5.1.3 Advanced

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

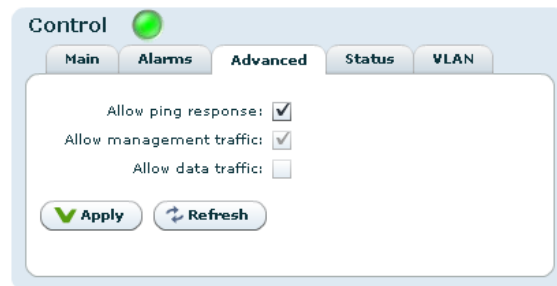


Figure 8.18 Advanced IP settings

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 8.6.4.1](#).

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.

8.4.5.1.4 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:

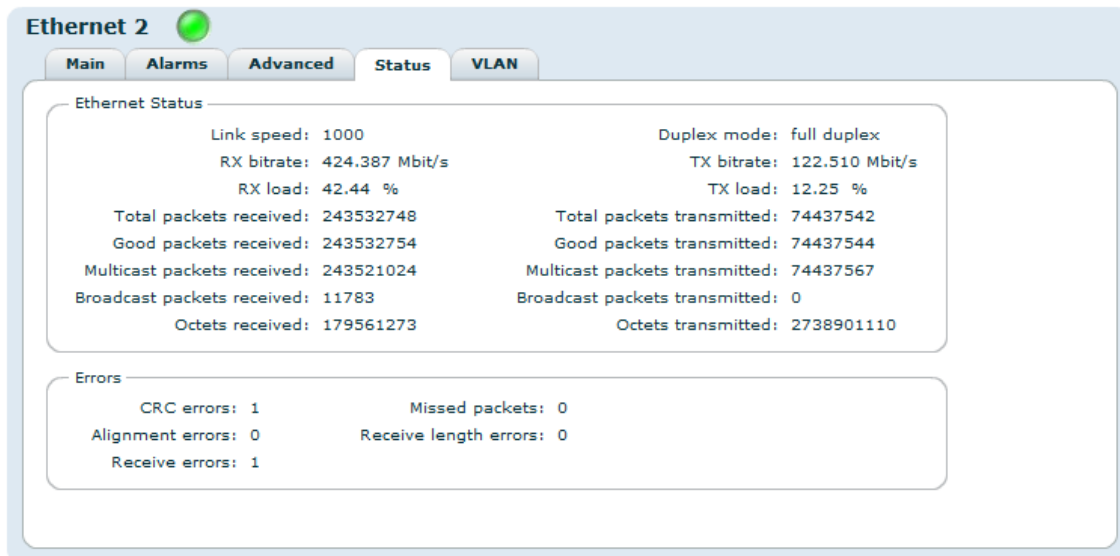


Figure 8.19 Interface Status

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.

8.4.5.1.5 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 8.20 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.

8.4.5.1.6 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 8.4.8.1, 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 CP524 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 8.22**, 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.

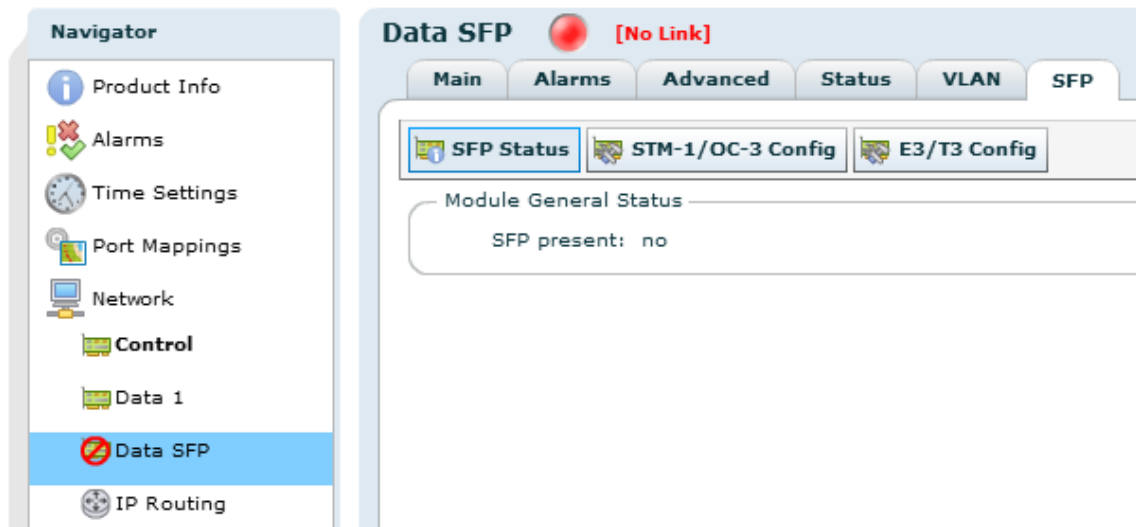


Figure 8.21 The Device Info > Network > SFP tab

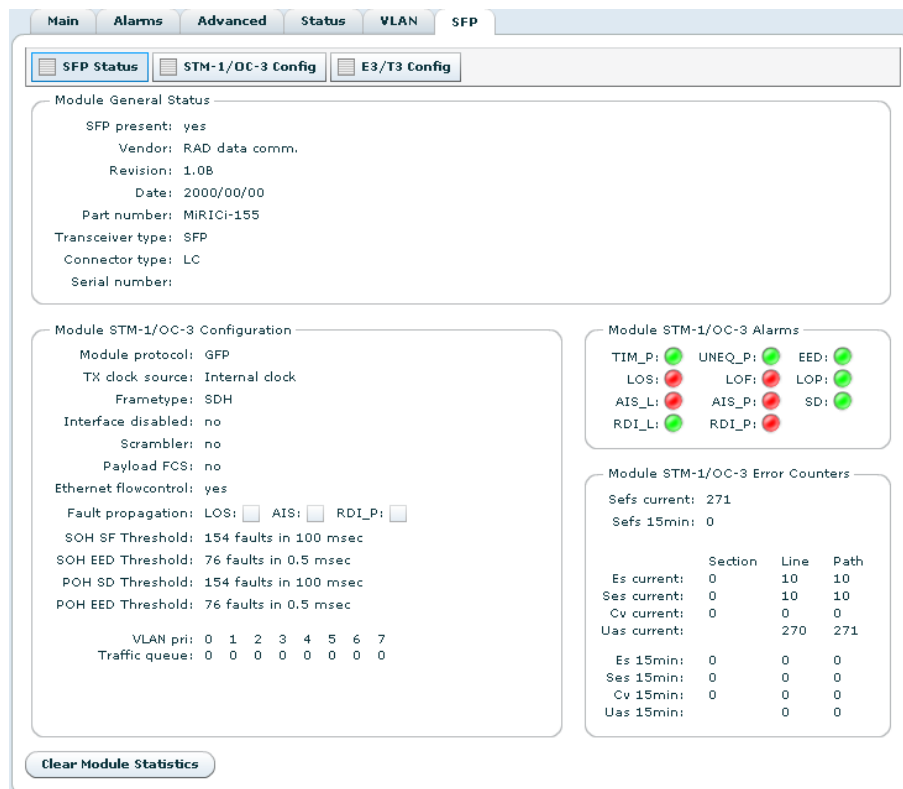


Figure 8.22 The SFP status page

The Module General Status field displays the status of the module as seen by the CP524.

SFP Present

Indicates that the module has been detected by the CP524.

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 CP524.

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 8.23](#) 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 CP524, 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 CP524.

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.

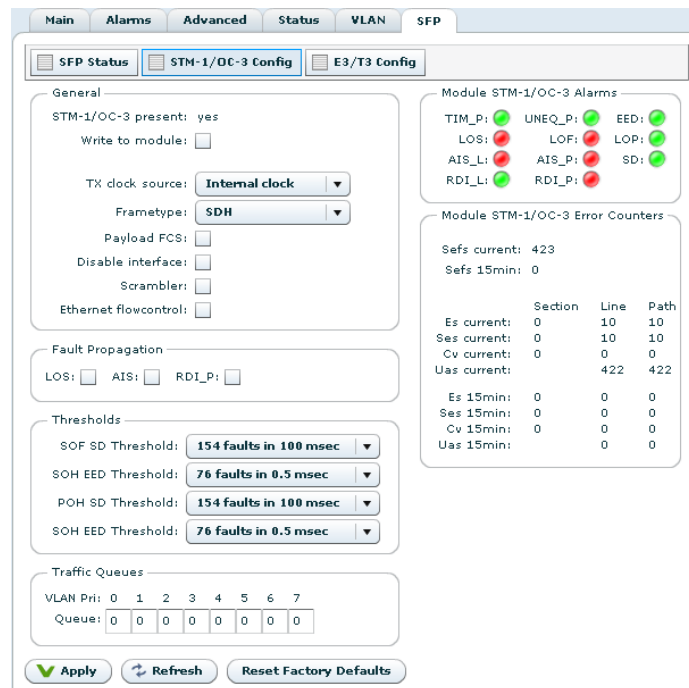


Figure 8.23 The configuration page for the STM-1/OC-3 SFP module

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 CP524 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 8.24** the page contains four fields to set operational parameters. Editing the configuration settings will alter the SFP configuration file stored in the CP524, only.

E3/T3 present

Indicates if the module has been detected by the CP524.

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 8.24 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 CP524 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.

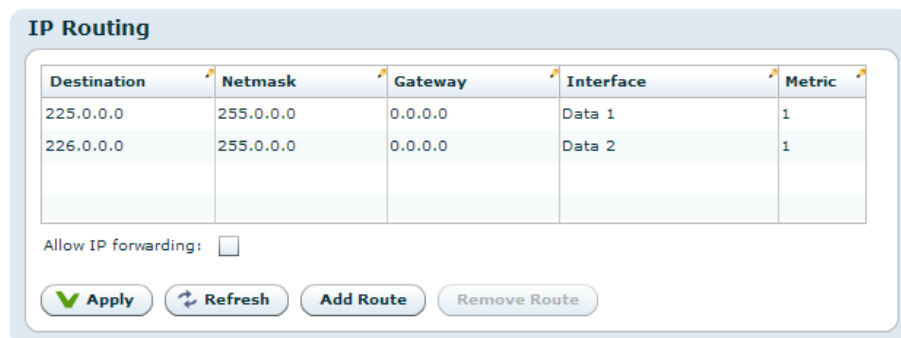
Refresh

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.

8.4.5.2 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 8.25 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.

8.4.5.3 TXP Settings



Figure 8.26 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.

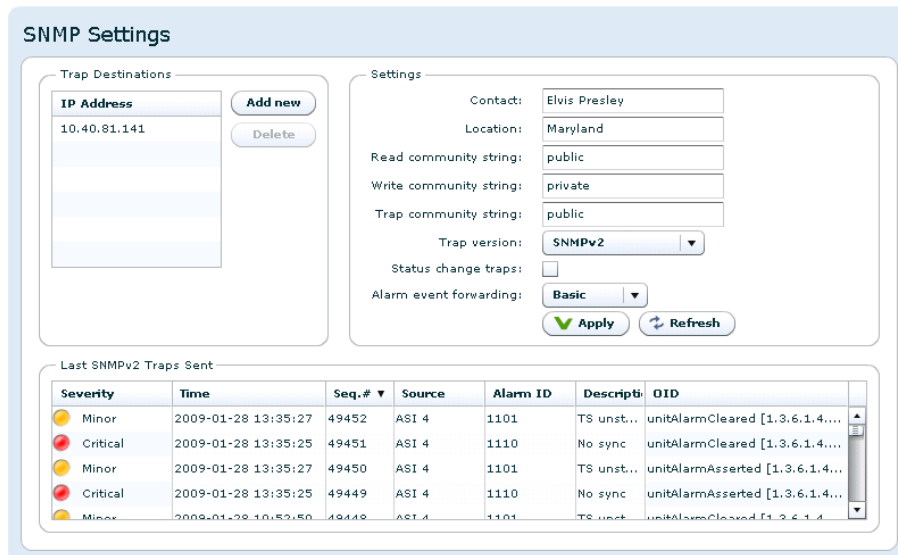
Below follows a simple example of how to get the units uptime. A description of the TXP protocol can be found on the T-VIPS Product CD, or by contacting T-VIPS Support.

```
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>
```

8.4.5.4 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.



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

Figure 8.27 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 9.4](#) in [Chapter 9: SNMP](#).

8.4.5.5 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.

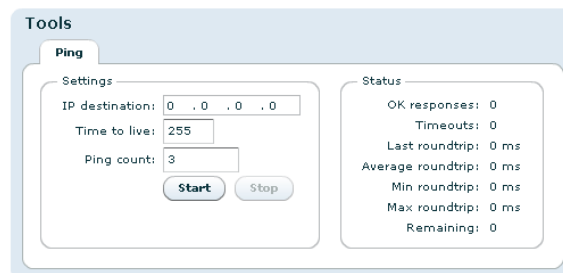


Figure 8.28 The Ping tool

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 8.4.5.1.3](#)) 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.

8.4.6 Clock Regulator

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

8.4.6.1 Main

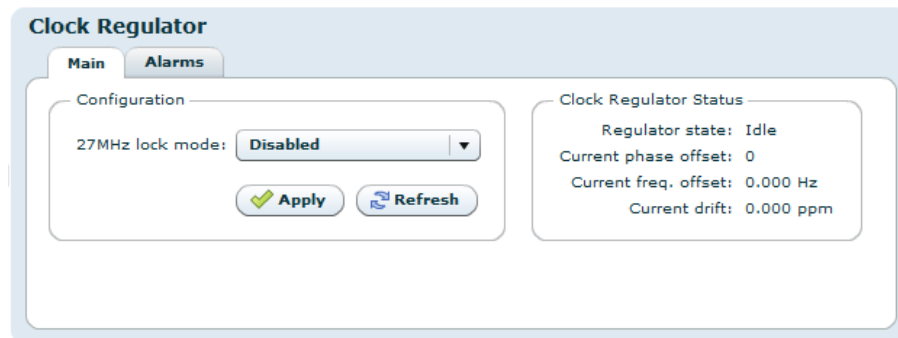


Figure 8.29 Clock regulator

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.

8.4.6.2 Alarms

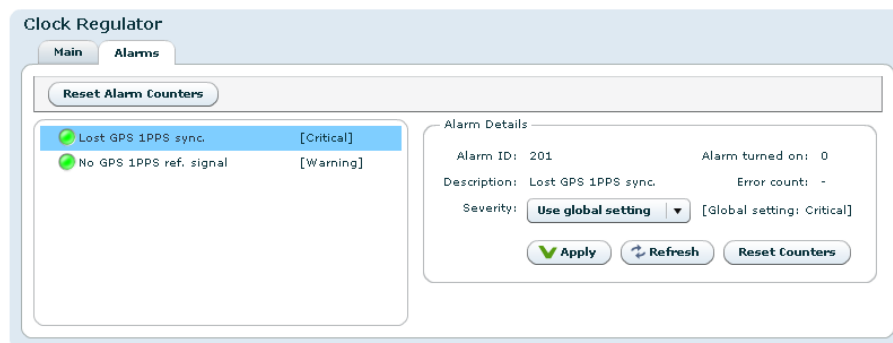


Figure 8.30 Clock regulator Alarms

These are the Clock regulator specific alarms. Clicking an alarm opens the field to configure the alarm. Please see [Section 8.4.2](#) for alarm configuration details.

8.4.7 Save/Load Config

This page provides an interface for managing the device configuration as “snapshots”. From here, snapshots of the device configuration settings can be taken and stored locally, or exported from the device as XML files. Also, previously stored snapshots may be imported and applied. The device allows for up to 8 configuration snapshots to be stored and managed locally, not including the current running configuration.

8.4.7.1 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.

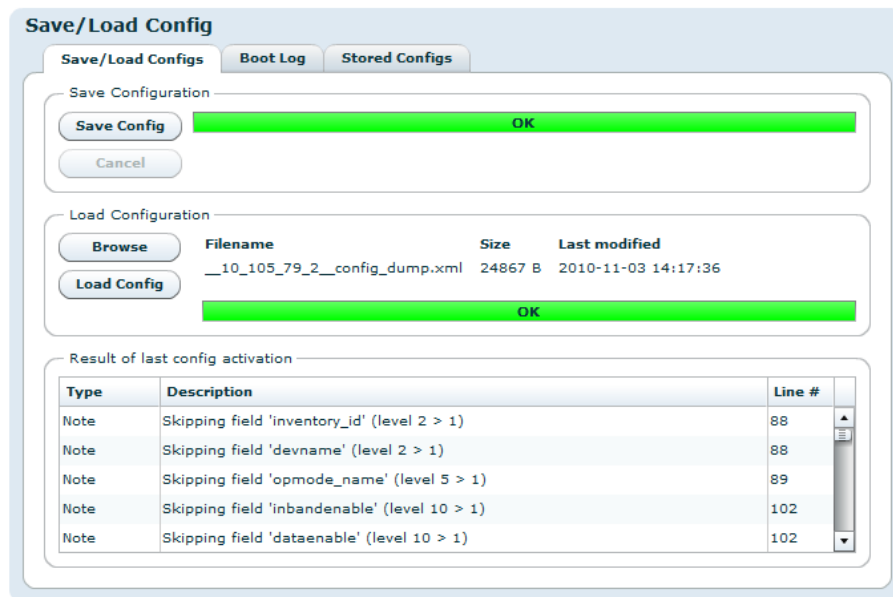


Figure 8.31 Saving and loading of configuration files

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.

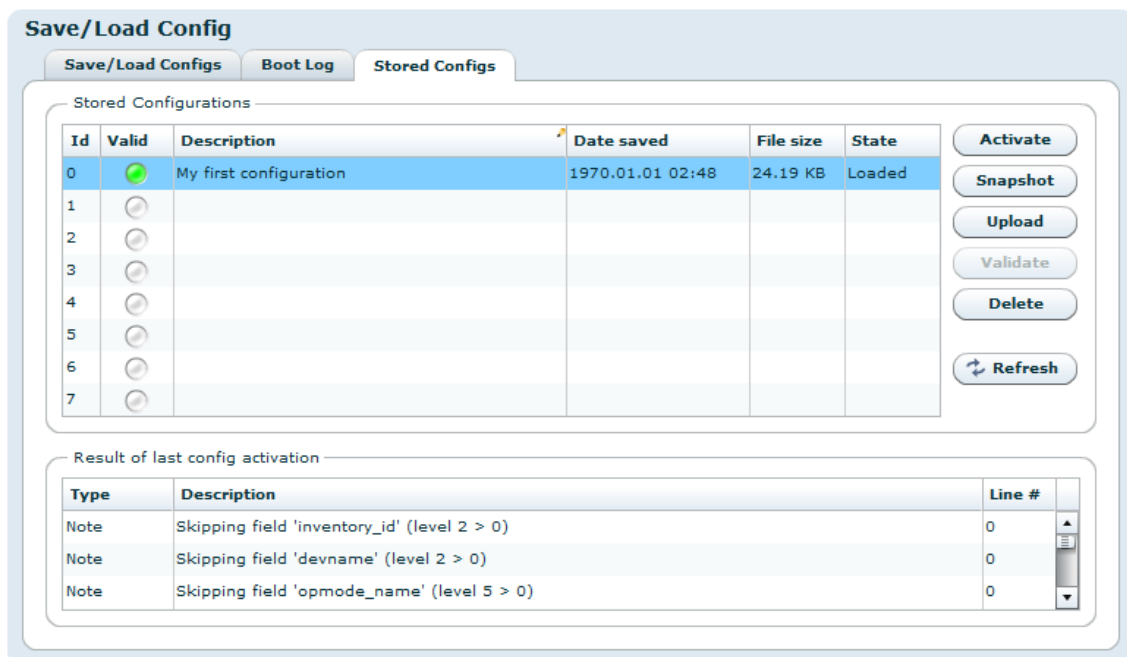
Partial configuration files are supported to allow a subset of configuration options to be changed instead of the entire unit configuration. Partial configuration files are validated as differences from the current running configuration upon import before being made active.

8.4.7.2 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.

8.4.7.3 Stored Configs

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



The screenshot shows the 'Save/Load Config' web interface with the 'Stored Configs' tab selected. The interface contains a table of stored configurations and a section for the result of the last configuration activation.

Id	Valid	Description	Date saved	File size	State
0		My first configuration	1970.01.01 02:48	24.19 KB	Loaded
1					
2					
3					
4					
5					
6					
7					

Result of last config activation

Type	Description	Line #
Note	Skipping field 'inventory_id' (level 2 > 0)	0
Note	Skipping field 'devname' (level 2 > 0)	0
Note	Skipping field 'opmode_name' (level 5 > 0)	0

Figure 8.32 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.

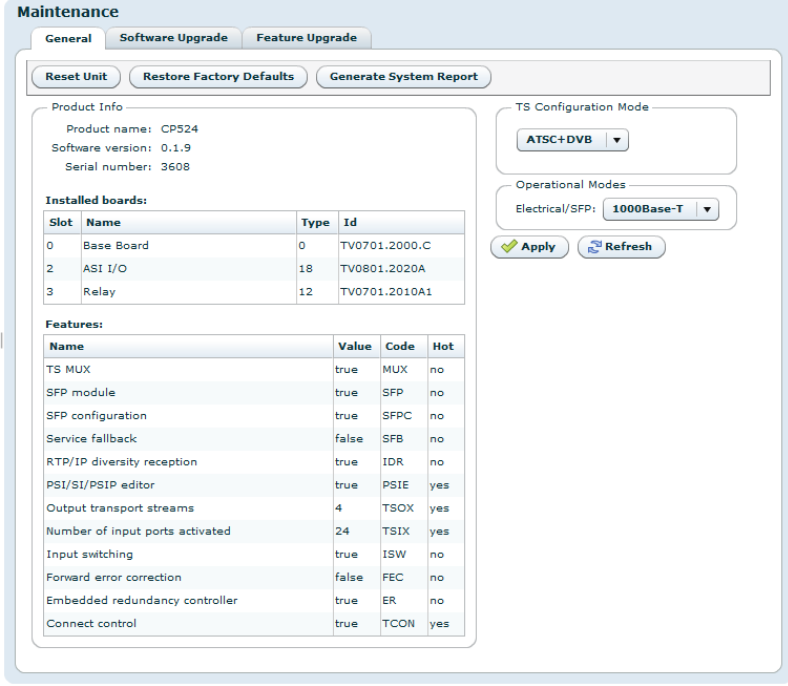
At the bottom of the page is the Results of last config action field, which will show the result of the last action performed.

8.4.8 Maintenance

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

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

8.4.8.1 General



Maintenance

General | Software Upgrade | Feature Upgrade

Reset Unit | Restore Factory Defaults | Generate System Report

Product Info
 Product name: CP524
 Software version: 0.1.9
 Serial number: 3608

TS Configuration Mode
 ATSC+DVB

Operational Modes
 Electrical/SFP: 1000Base-T

Apply Refresh

Installed boards:

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

Features:

Name	Value	Code	Hot
TS MUX	true	MUX	no
SFP module	true	SFP	no
SFP configuration	true	SFPC	no
Service fallback	false	SFB	no
RTP/IP diversity reception	true	IDR	no
PSI/SI/PSIP editor	true	PSIE	yes
Output transport streams	4	TSOX	yes
Number of input ports activated	24	TSIX	yes
Input switching	true	ISW	no
Forward error correction	false	FEC	no
Embedded redundancy controller	true	ER	no
Connect control	true	TCON	yes

Figure 8.33 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.

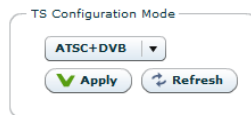


Figure 8.34 TS Configuration Mode


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 8.35. 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 8.35 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.

8.4.8.2 Software Upgrade

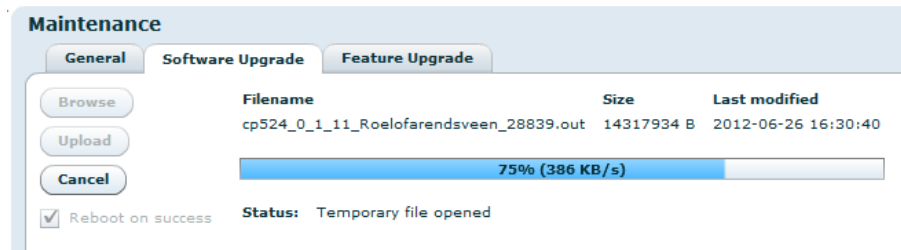


Figure 8.36 Software Upgrade

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 8.4.1](#)) to verify that the update was successful and the latest software revision is active.

8.4.8.3 Feature Upgrade

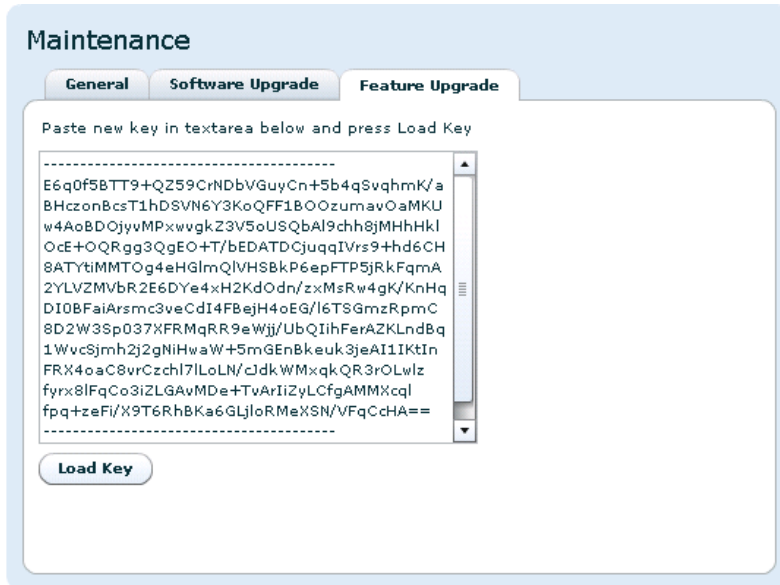



Figure 8.37 Feature Upgrade

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 8.4.8.1](#).

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

8.4.9 Users

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

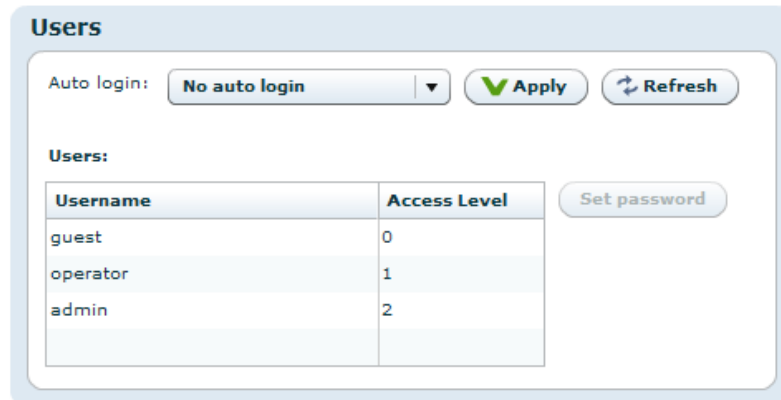


Figure 8.38 Users page

feature from the default ("No auto login") to another setting bypasses the initial login screen (Figure 8.2) 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.

8.4.10 GUI Preferences

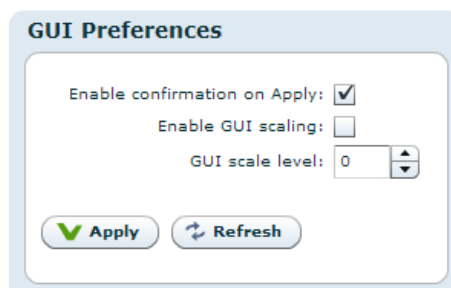


Figure 8.39 GUI Preferences page

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.

8.5 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.

8.5.1 Inputs Overview

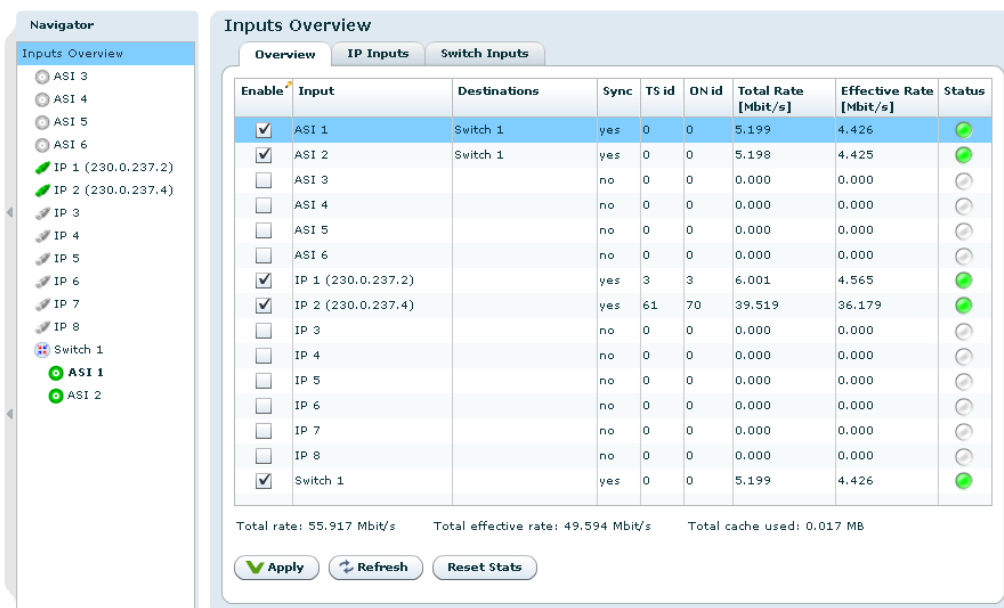


Figure 8.40 Inputs Overview

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

Enable

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

Input

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

Sync

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

Total Bitrate

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

Effective Bitrate

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

Alarm Status

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

Below the table three values as shown. They are:

Total input rate

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

Total effective input rate

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

Total cache used

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

The Reset Stats button at the bottom of the page gives access to a dialogue box that allows reset of channel statistics. **Figure 8.41** shows the dialogue box. Select the statistics items you want to reset and then press Apply.

8.5.1.1 IP Inputs

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

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

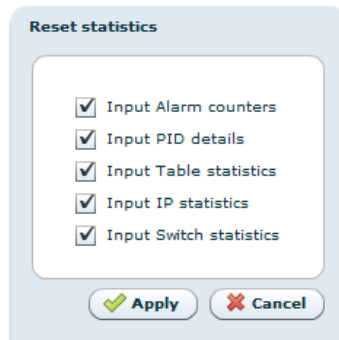


Figure 8.41 Reset statistics dialogue box

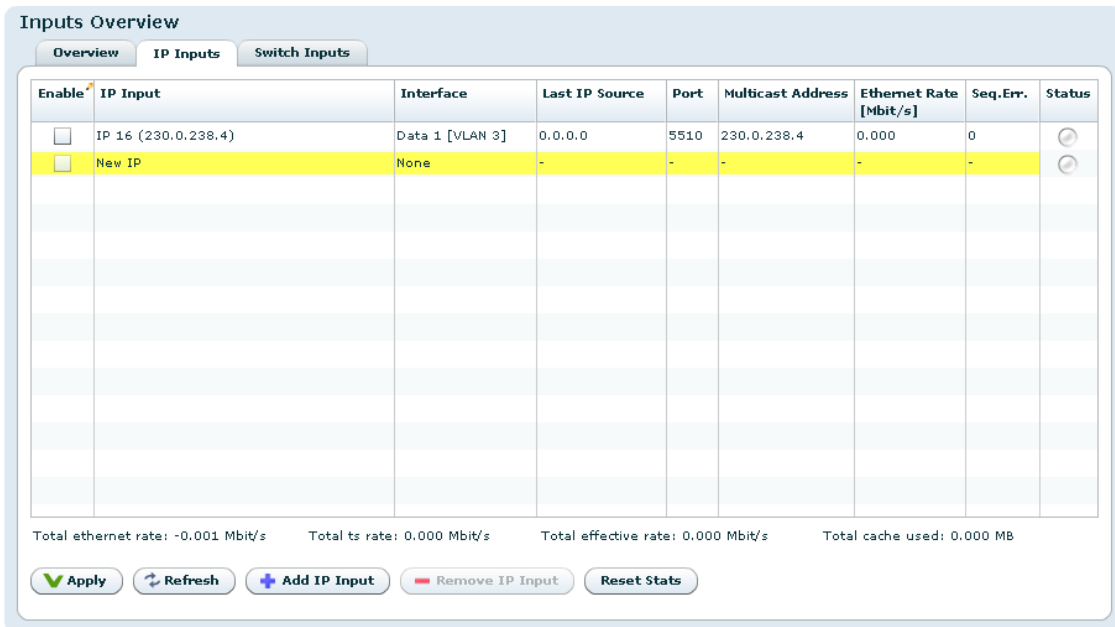


Figure 8.42 Inputs Overview - IP Inputs

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.

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).

8.5.1.2 Switch Inputs

If the unit is equipped with the Input switching feature, the Switch Inputs tab is shown on the Inputs Overview page. The page lists the defined input switches and offers controls to add and remove switch inputs.

Columns in the grid are:

Enable

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

Input Switch

The name of the switch input, consisting of the factory defined label with the logical port number and the user defined name. The port numbers for switch inputs start at 64.

Switch Status

Status text from the switch state machine. In the normal state, this shows active state and the time the switch has been in this state.

Selected Input

Shows the currently selected physical port

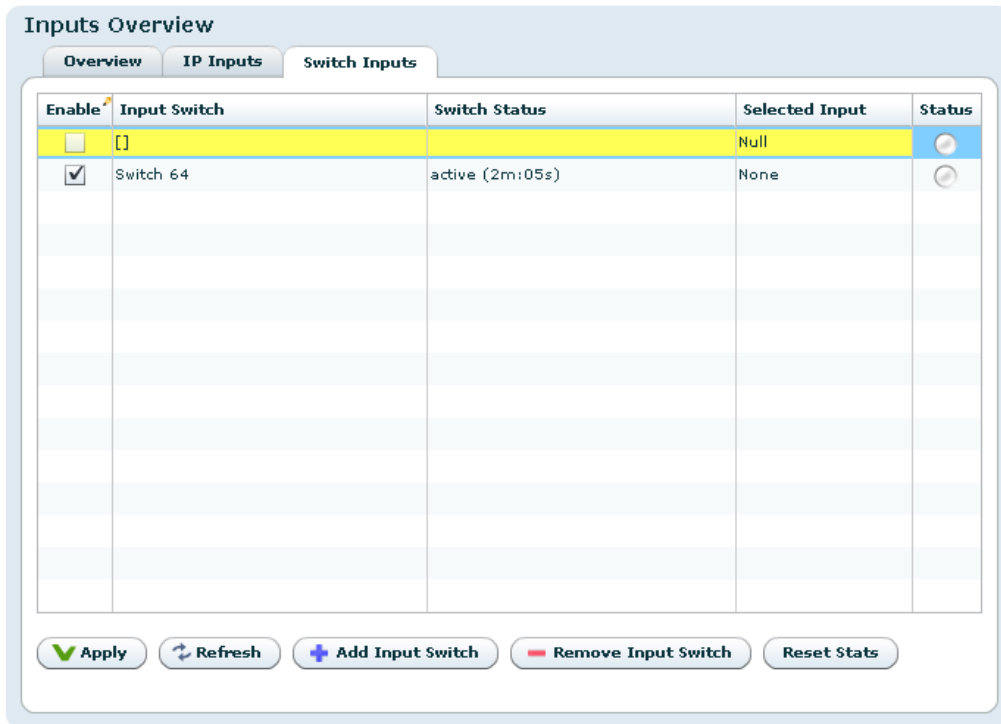


Figure 8.43 Inputs Overview - Switch Inputs

Status

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

To add a switch press the Add Input Switch button and press Apply to commit. When a switch is added, it appears in the left hand side navigator with an adjacent pluss sign. Selecting the switch will take you to the configuration page for the switch.

Removing a switch is accomplished by selecting the switch to remove in the datagrid and press the Remove Input Switch button.

The Reset Stats button is used to clear statistics counters for the switches.

8.5.2 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 8.44 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 8.3.1](#).

8.5.2.1 Main

The Main page is divided into three sections, the first one being the Transport Stream Details field. This field contains information and some configuration parameters concerning the 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.

Input format

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

TS mode

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

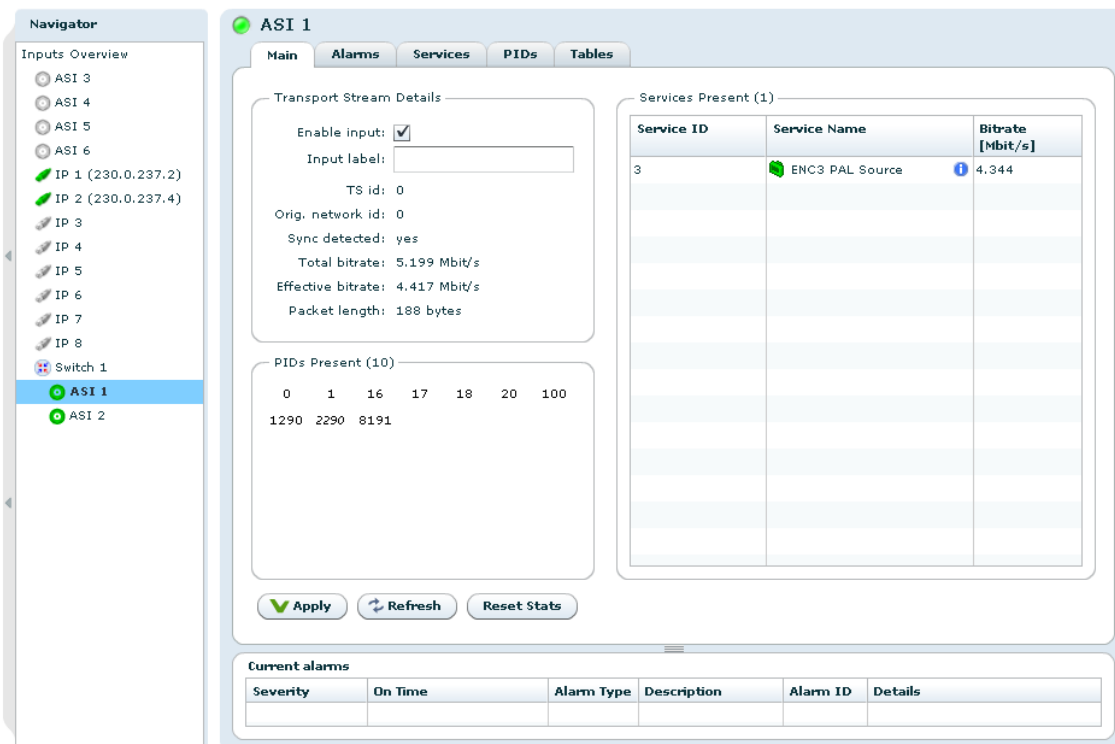


Figure 8.45 Main

TS id

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

Orig. Network id

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

Sync detected

Shows whether the input transport stream has been synchronised.

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.

8.5.2.2 Alarms

The Alarms page lets the user configure and view the status of all alarms belonging to the selected input.

In figure 8.46 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 8.47).

Error count

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

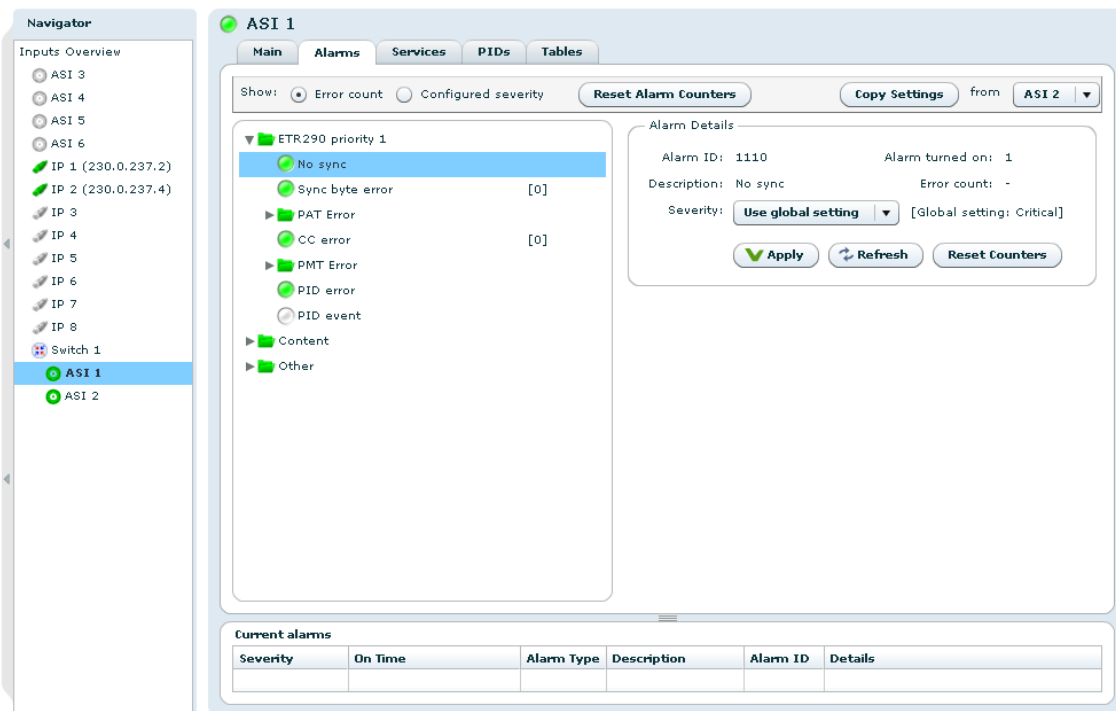


Figure 8.46 Input alarm configuration

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 8.47. By clicking on the alarm nodes in the tree the details for the selected alarm is shown in the Alarm details section (figure 8.48).

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.

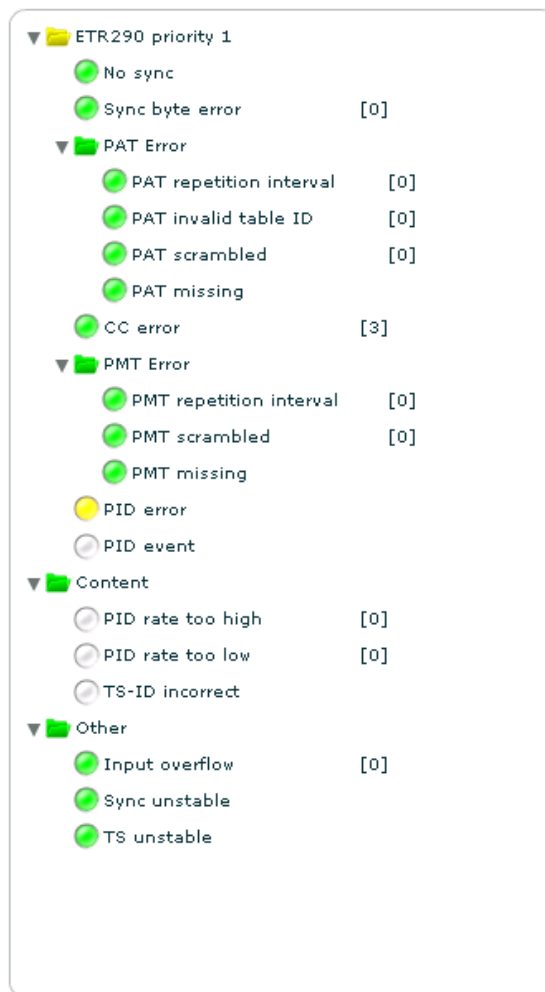


Figure 8.47 Input alarm tree

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

The alarm details section includes the following information and buttons.

Alarm ID

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

Alarm Details

Alarm ID: 1131 Alarm turned on: 0

Description: PAT repetition interval Error count: 0

Severity: Use global setting ▼ [Global setting: Warning]

Off time: 15 s [Default: 15]

Max interval: 500 ms [Default: 500]

Apply Refresh Reset Counters

Figure 8.48 Alarm details

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

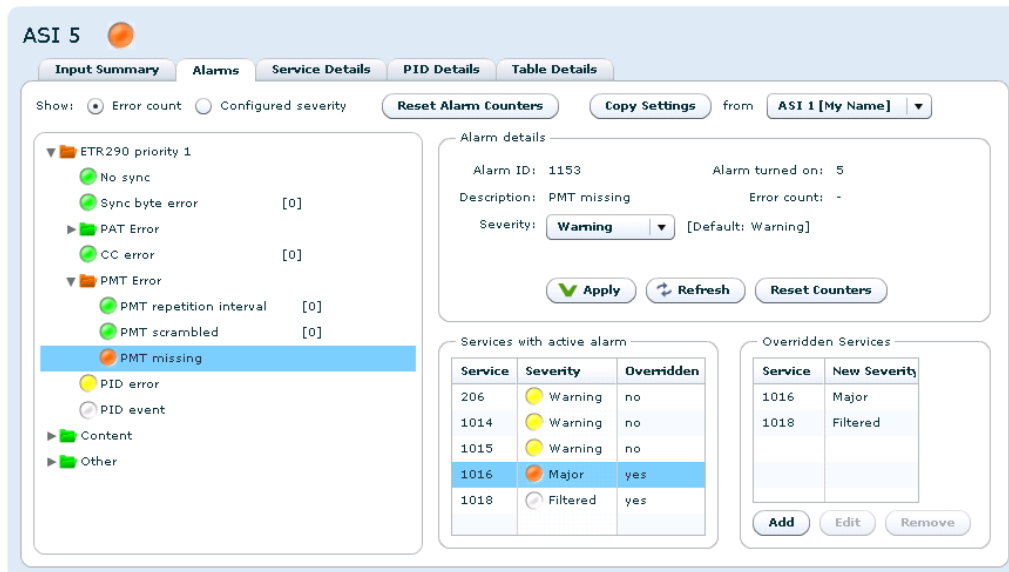
This field shows the value configured for this alarm in the global settings. If the alarm severity level is set to *global default* in the "Severity" pull-down list, this is the value that will be used.

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



ASI 5

Input Summary | Alarms | Service Details | PID Details | Table Details

Show: Error count Configured severity

Reset Alarm Counters Copy Settings from ASI 1 [My Name]

Alarm details

Alarm ID: 1153 Alarm turned on: 5
Description: PMT missing Error count: -
Severity: Warning [Default: Warning]

Apply Refresh Reset Counters

Services with active alarm

Service	Severity	Overridden
206	Warning	no
1014	Warning	no
1015	Warning	no
1016	Major	yes
1018	Filtered	yes

Overridden Services

Service	New Severity
1016	Major
1018	Filtered

Add Edit Remove

Figure 8.49 Alarm severity per sub-ID (typically Service or PID)

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

Service/PID

The id of the sub-item.

Severity

The current severity of the item.

Overridden

Indicates whether the sub item has been overridden.

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

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

Service/PID

The id of the Sub item.

New severity

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

New limit

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

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

8.5.2.3 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 8.50.

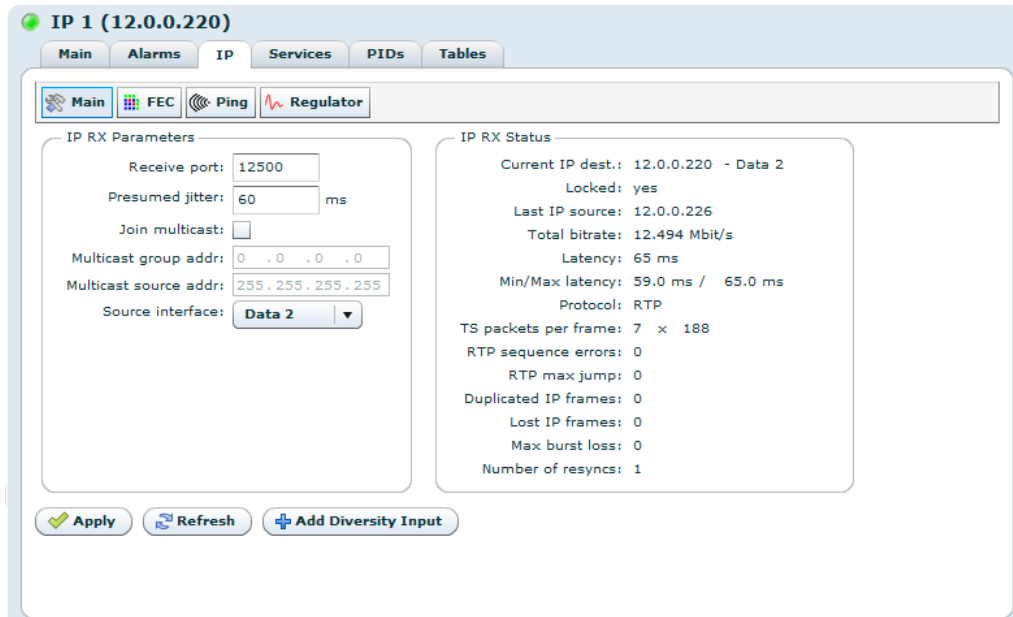


Figure 8.50 IP Configuration

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.

Add diversity input

If the product is installed with the IP diversity (IDR) feature an additional button will appear at the right side of the "Apply" and "Refresh" button. This button will add another IP channel that will combine the two IP channels into a diversity pair.

The GUI will dynamically adapted to configure the RTP/IP Diversity reception feature and a new page called "Diversity" will appear.

8.5.2.3.1 RTP/IP Diversity Reception

This tab will only be visible if a diversity input has been added. Please see [5.11](#) for detailed technical description of RTP/IP Diversity Reception.

The Diversity sub page is shown in figure [8.51](#).

This page allows configuration of the IP parameters for the two IP inputs that form the diversity reception. Additionally, detailed IP status information for both channels and the diversity reception is shown.

The Diversity Input Configuration field allows for setting the presumed jitter of the diversity reception. Since both IP inputs uses the same regulator to tune on the bitrate and latency in the network, the presumed jitter value will affect **both** IP inputs. The jitter value should be set to account for the network path with the largest delay / jitter.

Diversity Input Status

Locked

"Yes", when the unit has locked to one of the input streams and has correctly estimated the bitrate of one the input streams. "No", when the unit has not been able to receive from any of the input streams correctly.

Receiver latency

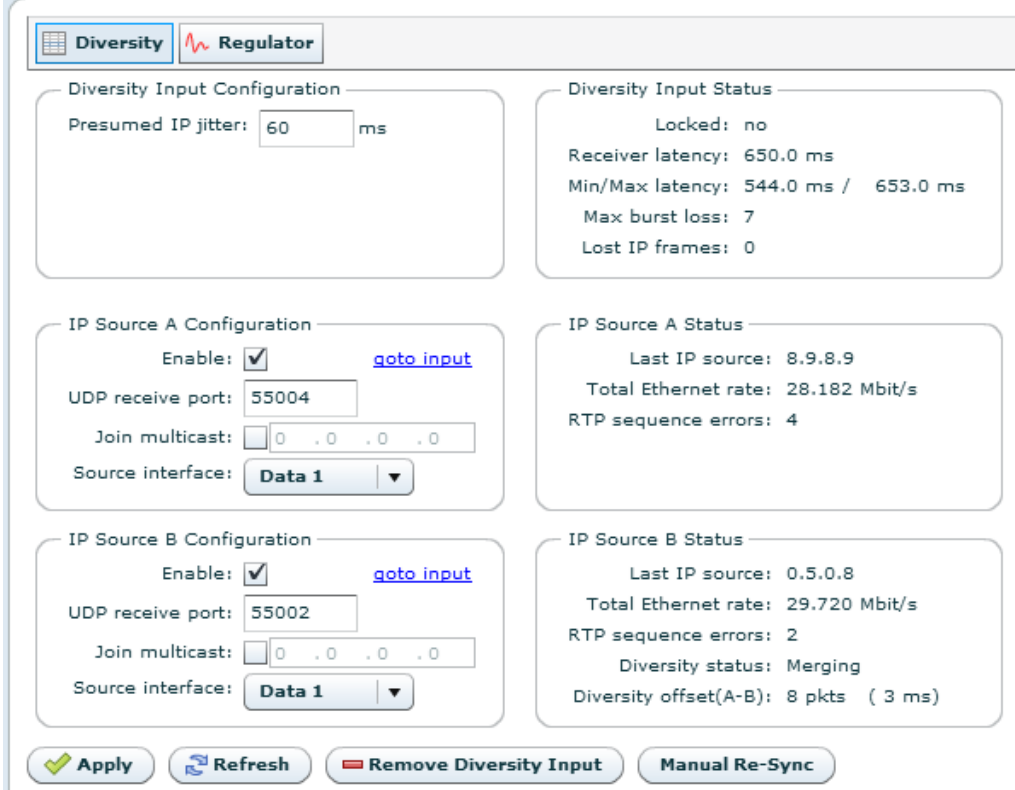
The currently measured latency of the input after the diversity operation. This parameter reflects the network jitter the unit can handle at the moment.

Min/Max latency

This shows the minimum and maximum latency measured since the statistics was last reset.

Max burst loss

The maximum number of consecutive packets lost.



The screenshot shows the following configuration details:

- Diversity Input Configuration:** Presumed IP jitter: 60 ms
- Diversity Input Status:** Locked: no, Receiver latency: 650.0 ms, Min/Max latency: 544.0 ms / 653.0 ms, Max burst loss: 7, Lost IP frames: 0
- IP Source A Configuration:** Enable: [goto input](#), UDP receive port: 55004, Join multicast: 0 . 0 . 0 . 0, Source interface: Data 1
- IP Source A Status:** Last IP source: 8.9.8.9, Total Ethernet rate: 28.182 Mbit/s, RTP sequence errors: 4
- IP Source B Configuration:** Enable: [goto input](#), UDP receive port: 55002, Join multicast: 0 . 0 . 0 . 0, Source interface: Data 1
- IP Source B Status:** Last IP source: 0.5.0.8, Total Ethernet rate: 29.720 Mbit/s, RTP sequence errors: 2, Diversity status: Merging, Diversity offset(A-B): 8 pkts (3 ms)

Figure 8.51 RTP/IP Diversity Reception Configuration

Lost IP frames

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

IP Source A Configuration

Enable

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

UDP received port

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

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. If this parameter is checked it is possible to enter the multicast group address the input will join.

Source interface

The interface on which this input will listen for data.

IP Source A Status

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 Ethernet rate

The total IP rate received on this input

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.

IP Source B Configuration**Enable**

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

UDP received port

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

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. If this parameter is checked it is possible to enter the multicast group address the input will join.

Source interface

The interface on which this input will listen for data.

IP Source B Status**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 Ethernet rate

The total IP rate received on this input.

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.

Diversity status

This parameter will show the status of the diversity operation. Three possible states are allowed. These are "Merging", "Not synchronized" and "Disabled".

"Merging" refers to normal operation where packets are being merged together as intended.

"Not synchronized" means that the two IP input streams are not properly aligned and synchronized.

“Disabled” refers to that the IP source status B is disabled.

Diversity offset(A-B)

Offset between source A and B measured in RTP sequence number and corresponding value in time. Measurements are A-B, i.e if positive, A is on a higher RTP sequence number at the same time instance and has therefore less delay since IP transmitter.

Positive: A is received first.

Negative: B is received first.

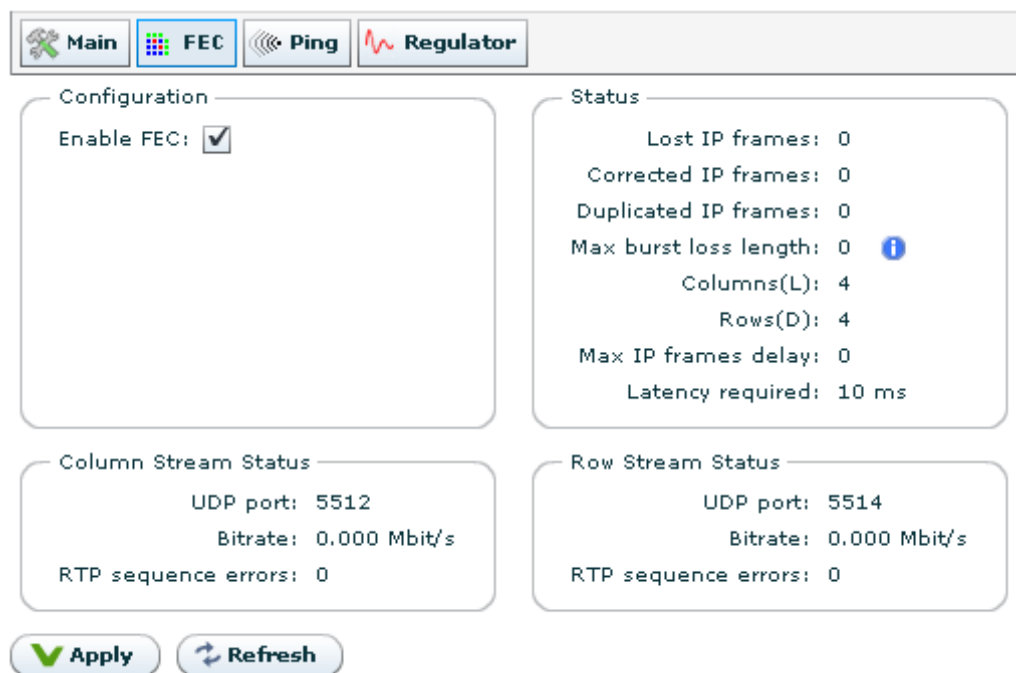
Zero: A and B has been transport with equal transport delay within 1ms.

By pressing the button “Remove diversity input”, IP source B will be removed and source A will resume to be a standard IP source again.

The Manual re-sync button will resynchronize the data storage buffer being used by both IP source A and B.

8.5.2.3.2 FEC

The FEC sub page is shown in [Figure 8.52](#). This page displays the status of the forward error correction processing of the IP input.



Configuration	Status
Enable FEC: <input checked="" type="checkbox"/>	Lost IP frames: 0
	Corrected IP frames: 0
	Duplicated IP frames: 0
	Max burst loss length: 0 i
	Columns(L): 4
	Rows(D): 4
	Max IP frames delay: 0
	Latency required: 10 ms
Column Stream Status	Row Stream Status
UDP port: 5512	UDP port: 5514
Bitrate: 0.000 Mbit/s	Bitrate: 0.000 Mbit/s
RTP sequence errors: 0	RTP sequence errors: 0

Figure 8.52 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](#).

8.5.2.3.3 Ping

The Ping sub page is shown in figure [8.53](#).

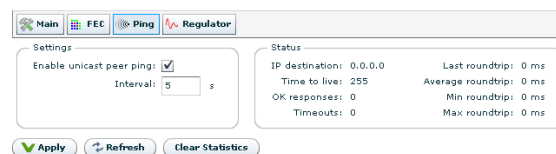


Figure 8.53 Ping page

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.

8.5.2.3.4 Regulator

The Regulator sub page is shown in figure 8.54.

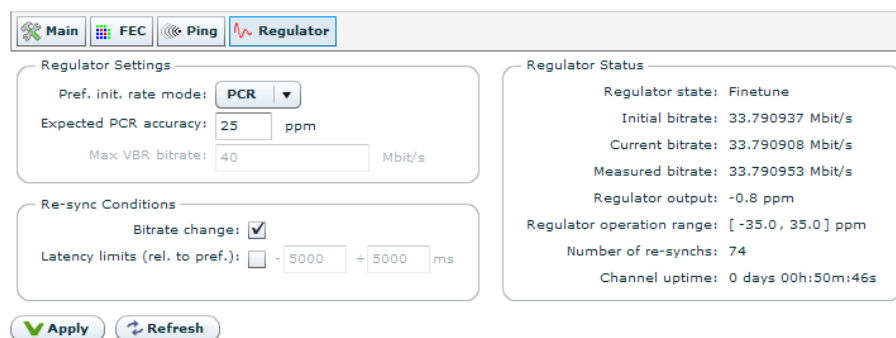


Figure 8.54 Regulator page

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

Pref. Init. Rate Mode

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

PCR

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

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 8.5.2.1](#)).

8.5.2.4 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 [8.55](#)).

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:

Service ID

The service id of the selected service.

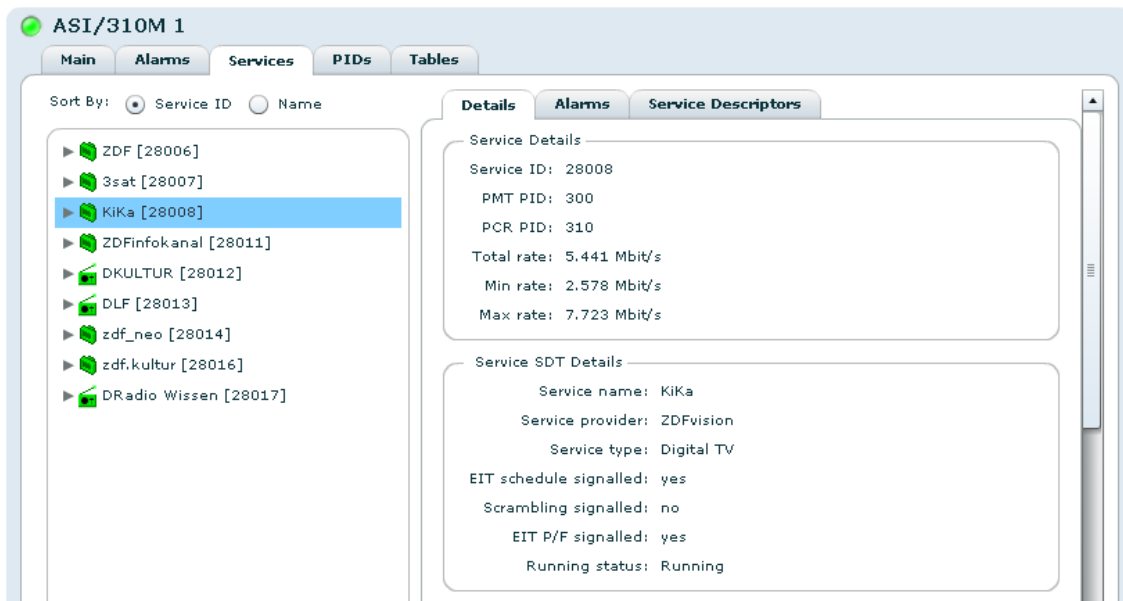


Figure 8.55 Service details overview when service list is not expanded.

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 8.3.2](#).

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 8.56](#).

Each component is shown with the following information:

Component type symbol

Symbol showing the kind of component.

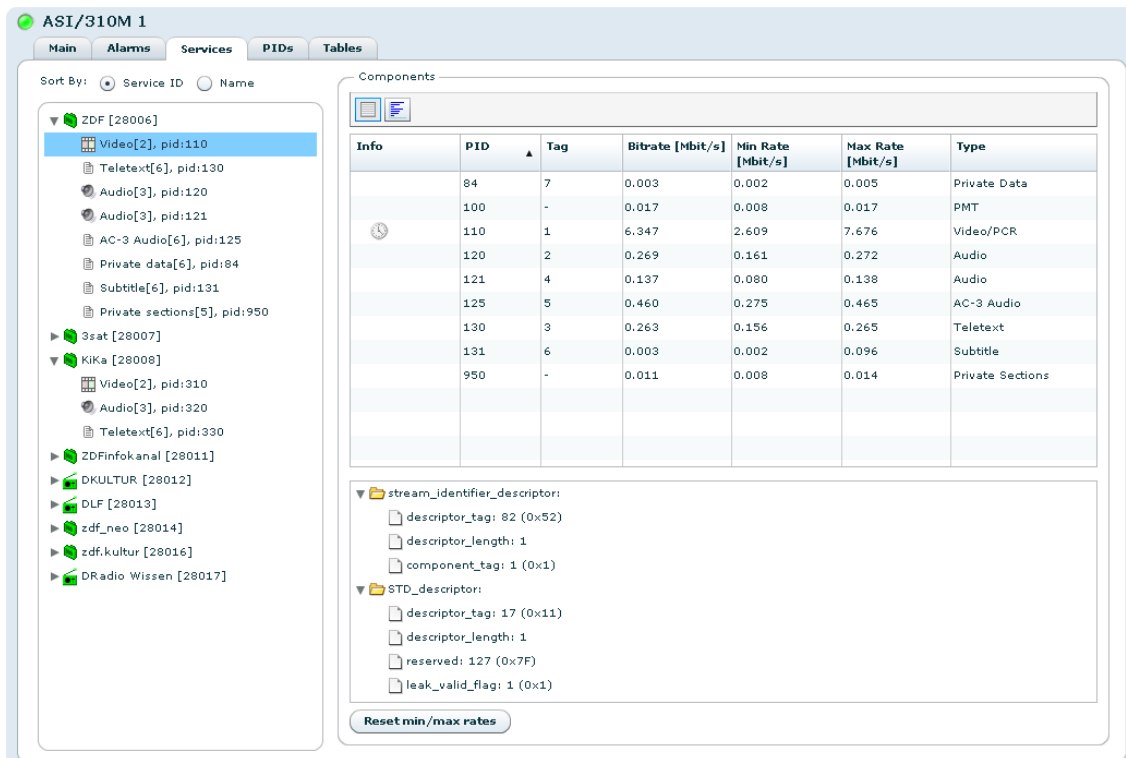


Figure 8.56 Service details full component overview

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 8.5.2.5](#). 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.

8.5.2.5 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	0.015	0.012	0.017	0	0		57686
	1	-	CAT	0.003	0.002	0.003	0	0		11537
	16	-	NIT	0.000	0.000	0.002	0	0		1177
	17	-	SDT/BAT	0.002	0.000	0.003	0	0		5768
	18	-	EIT	0.042	0.030	0.066	0	0		185922
	20	-	TDT/TOT	0.003	0.002	0.003	0	0		11538
	100	-	PMT	0.008	0.005	0.009	0	3		28843
	1290	-	Video	3.996	3.631	4.008	0	3		15280712
	2290	-	Audio/PCR	0.334	0.302	0.335	0	3		1281930
	8191	-	Null Packets	0.799	0.713	1.167	0	0		3079593

Figure 8.57 PID Details, table view

The PID table contains the following columns:

Info

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



Figure 8.58 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 8.59. To the left is the bar chart showing the PIDs and

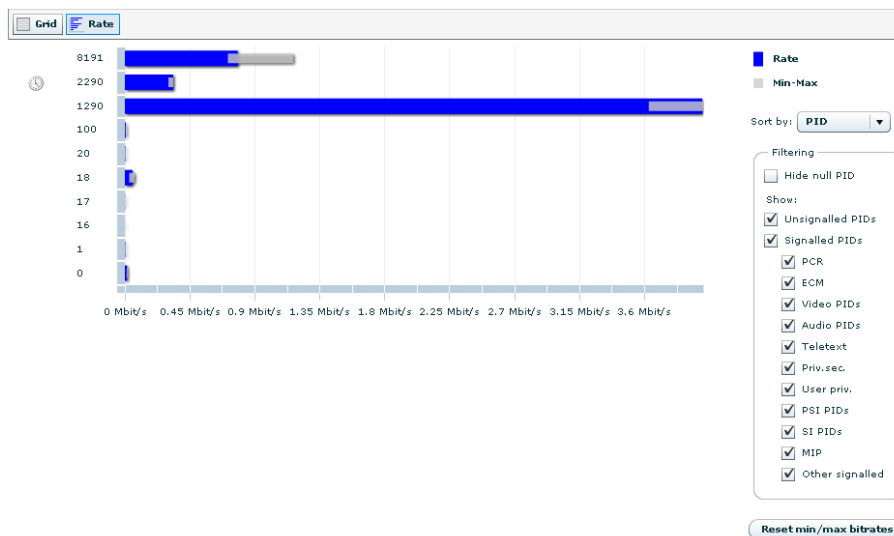


Figure 8.59 PID Details, rate view

Vertically, the chart displays one bar for each of the packet streams present on the input. Adjacent to the PIDs the symbols shown in figure 8.58 are shown if relevant.

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

To the right of the chart a field of options are provided to configure the view. The Sort by drop down menu on top lets the user sort the bar chart by different parameters. The Filtering frame lets the user choose which PIDs to show. Checking the Hide null PID check box removes the null PID from the chart. Unchecking any of the other check boxes removes the corresponding PIDs from the chart.

Below the Filtering frame the Reset min/max bitrates button is provided. Hitting this button resets the min and max rates counters of all PIDs.

8.5.2.6 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.

8.5.2.7 Tables

Figure 8.60 shows the table details in list view.

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

Above the table the following information and buttons can be found:

Shown tables

The number of table that fall into the chosen folder compared to the total number of tables.

Shown size

The size(in bytes) of the tables that fall into the chosen folder compared to the total size of the tables.

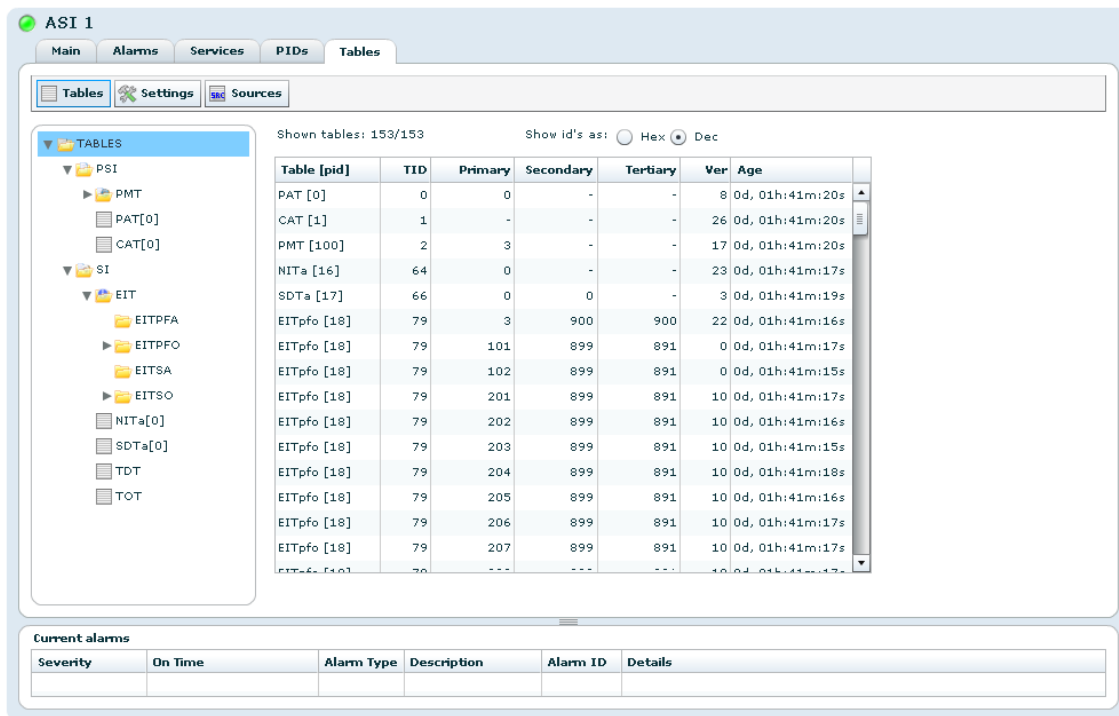


Figure 8.60 Table details, overview.

Show ID's as

Configure to view id's and keys in hexadecimal or decimal notation.

The right hand side table of the sub page has the following columns:

Table

The type of information table and (in braces, []) the PID containing it.

TID

The table ID.

Primary

The primary extension ID of the table. Hovering the mouse cursor over the value displays a tool tip describing the meaning of this key in the context of the table.

Secondary

The secondary extension ID of the table. Hovering the mouse cursor over the value displays a tool tip describing the meaning of the secondary ID in the context of this table.

Tertiary

The tertiary extension ID of the table. Hovering the mouse cursor over the value displays a tool tip describing the meaning of the key in the context of this table.

Ver

This is the last received version of this table.

Age

The time elapsed since the table was last updated. Selecting a single table from the tree to the left or double clicking a line within the table opens a view displaying the parameters of that table. The parameters are the same as are shown in the table view.

8.5.2.8 Settings

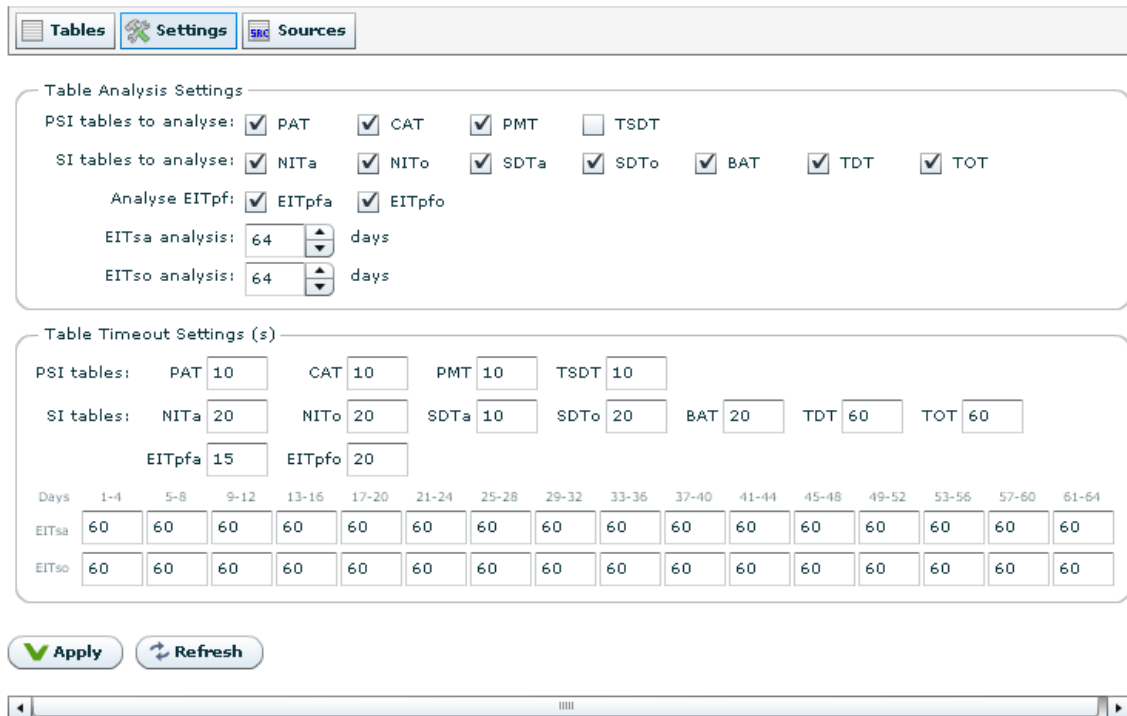


Table Analysis Settings

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: 64 days

EITso analysis: 64 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

Days	1-4	5-8	9-12	13-16	17-20	21-24	25-28	29-32	33-36	37-40	41-44	45-48	49-52	53-56	57-60	61-64
EITsa	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
EITso	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60

Apply Refresh

Figure 8.61 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 8.61 shows the page as displayed in DVB mode.

In ATSC mode the page looks different, as shown in figure **8.62**



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:

Table Analysis Settings

PSI tables to analyse: PAT CAT PMT TSDT

PSIP tables to analyse: MGT TVCT CVCT RRT EIT ETT STT

Table Timeout Settings (s)

PSI tables: PAT 10 CAT 10 PMT 10 TSDT 10

PSIP tables: MGT 10 TVCT 10 CVCT 10 RRT 120 STT 10

PIDs:	0	1	2-1	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

Figure 8.62 Table analysis configuration in ATSC mode.

- 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.

8.5.2.9 Sources

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 8.63 and contains a grid with the following columns:

Table	Source PID	Default Src PID
NITa [64]	16	16
NITo [65]	16	16
SDTa [66]	17	17
SDTo [70]	17	17
BAT [74]	17	17
EITpfa [78]	18	18
EITpfo [79]	18	18
EITsa [80]	18	18
EITso [96]	18	18
TDT [112]	20	20
RST [113]	19	19
TOT [115]	20	20

Figure 8.63 Non-standard table source PID configuration.

Table

The table type to configure with its table ID in decimal in brackets.

Source PID

The input PID to use in the section filter for this table ID. Click the grid cell to edit it. Edited fields are shown in yellow until applied.

Default Src PID

The default PID used for this table type. Use this value if you want to go back to DVB compliant input filtering.

After making the changes in the grid press Apply to activate the changes. You can then go back to the table listing to see whether the expected tables are received on the new PID value.



Warning: Changing the PID values used in the input filtering must be performed with care. If you specify a PID that contains a high bandwidth PID it may cause the unit to malfunction.

8.5.3 Switch

This page has two sub-tabs; Main and Alarms. In all sub-pages for a switch a list of current alarms is shown. This list is identical to the list displayed in the Current Status view, and described in section [Section 8.3.1](#).

8.5.3.1 Main

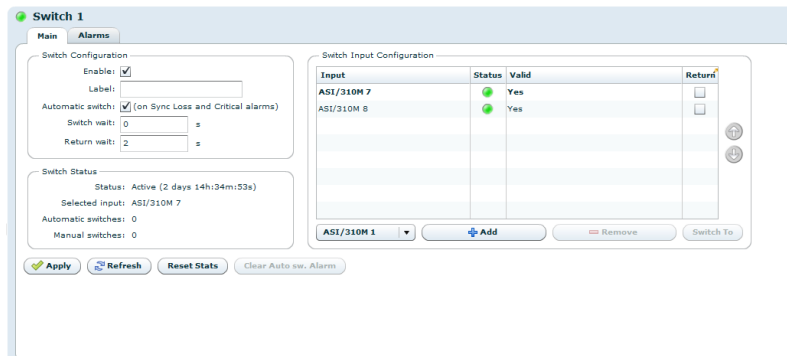


Figure 8.64 Input switch configuration

The Main sub page is used to configure input switching of a group of inputs. The page is accessed by selecting a switch in the left hand side navigator on the Inputs tab, or by double clicking the switch entry on the Inputs Overview > Switch Inputs page. See section [Section 8.5.1.2](#) for instructions how to create a switch input.

The availability of input switching is determined by the SW licence key Input switching.

Ports can be added to the switch in two ways.

1. Drag physical ports in the left hand side navigator, dropping them into the switch group at the wanted priority position.
2. Select the wanted port in the drop down in the Input switch configuration and press the Add button. Press Apply to commit.

A physical port can only be used in one switch group. When a physical port is used in a switch group, it cannot be used directly as a physical port when configuring services and PIDs.

Switch configuration

Enable

Enable/Disable the switch as a source. When disabling the switch, no data will be forwarded to the output from the switched input.

Label

A user specified name for this switch.

Automatic switch

Enable/disable auto-switching. If turned on, automatic switching will happen according to switching rules. The switch will always select the highest prioritized input that is valid. Valid input are in sync and does not have a Critical alarm condition. If disabled, switching is only done manually by selecting port and pressing Switch To. If disabled, the alarm Auto switching disabled will be set to warn that no auto-switching will happen. If disabled the unit will remember the selected input, even during power loss.

Switch wait

Time to wait before switching, in case switching condition disappears. Given in seconds

with decimals, but resolution is currently 0.5 seconds. Set this to 0 for fastest possible switching.

Return wait

Return wait activated when switching away from a port. It will not be possible to return to a port before Return wait seconds has passed. The return wait is a state for each input, so it will be possible to auto-switch to other ports that has not recently been switching away from. The return wait period can be used to avoid frequent switching between inputs.

Status

Shows current state, Idle, Active, Wait or Hold with some timing information.

Selected input

The currently selected input.

Automatic switches

Number of automatic switches performed since Reset Stats was last activated. When a switch has been done, an alarm event can be found in the alarm log.

Manual switches

Number of manual switches performed since Reset Stats was last activated. When a switch has been done, an alarm event can be found in the alarm log.

Switch Input Configuration

List of inputs pertaining to the switch group. Columns are:

Input

Name of the input port

Status

Input alarm status

Valid

Status of input saying if the input will be considered as valid when performing an automatic switch. If not Valid and selected the switch will try to switch to the highest prioritised input that is Valid.

Return

Whether to automatically return to this port if is valid, even when the currently selected port is valid. Will only return to higher prioritized sources.

Add port by selecting the port in the drop-down list and pressing Add.

Remove a port by selecting the port in the grid and pressing Remove.

Switch manually to a port by selecting it in the grid and pressing Switch To.



Note: When doing manual switches in Automatic switch mode, the switch might automatically switch away from the selected input after the Return Wait time has passed.

8.5.3.2 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 8.4.2.1.

8.6 Outputs

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

The labelling of the outputs is a combination of the user defined name of the output and the physical number of the output port.

8.6.1 Outputs Overview



Figure 8.65 Outputs overview

The Outputs Overview page shows a short table summary of the logical TS outputs of the device. The table has the following columns:

Enable

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

Output

The name of the output, consisting of the user defined name combined with the physical label.

Total Bitrate

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

Effective Bitrate

The effective bitrate (total less null packets) of the transport stream currently transmitted, in Mbit/s.

Alarm Status

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

8.6.2 Output



Figure 8.66 Output header

When selecting an output a new page on the right hand side with information about the selected output is displayed. The top part of that page is common for all sub pages and is divided into two main sections. The left hand section shows the name and the current alarm status of the output.

All current alarms pertaining to this output are displayed in a tool tip by holding the mouse cursor over the alarm status indicator.

The right section consists of a utilisation bar and a number showing the total rate that is currently being transmitted on this output. The utilisation bar shows how much of the total rate is filled with data. A tool-tip on the utilisation bar shows the current effective bitrate.

Beneath the name of the output is a tab navigator, which contains the different sub pages with information about the selected output. The choices are:

Main

This page lets the user configure several parameters of the output stream.

Alarms

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

IP

This page allows configuration of the IP output.

Services

This is where the selection and configuration of services to transmit on the output is performed. The sub-dialogues also allow configuration of service components within each service.

PIDs

In this page it is possible to modify the behaviour of individual input PIDs prior to building the output transport stream.

Tables

This page is used to configure the behaviour of the PSI/SI/PSIP signalling.

Pri Queues

This page is used to manage the output priority queues for traffic prioritisation and shaping.

Outgoing

This page shows a detailed view of the PIDs and services in the output transport stream.

8.6.2.1 Main

Figure 8.67 Output Configuration, Manual.

The Main page lets the user configure port level parameters on the selected Output.

The page is shown in figure 8.68 for manual bitrate config mode and in figure 8.67 for OFDM bitrate config mode. The screen is divided into several sections each with its own sub chapter below.

The Main Configuration section lets the user configure the following parameters:

Enable output

Enable or disable the output.

Output label

This lets the user type in a label for the selected output. The label is only used for presentational purposes.

Regeneration mode

This option controls how the output is regenerated. Two possible values are allowed, either “Normal” or “Transparent”. In “Normal” mode the unit will operate as a normal MUX and will consider PSI/SI/PSIP settings and service configuration.

If “Transparent” mode is selected then the user has to choose which input that should be transparently passed through the system. When using this option all PIDs from the selected input will be passed through and the PSI/SI/PSIP settings and service configuration will not be considered.

Output format

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

TS mode

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

Bitrate config

This lets the user manually set the bitrate or set it through a series of OFDM parameters . If the output format is set to SMPTE 310M this option is hidden.

Set output bitrate

If manual bitrate config is chosen this field lets the user set the bitrate. If OFDM is chosen or the output format is set to SMPTE 310M the output bitrate cannot be altered. Thus this option is disabled.

Current bitrate

This shows the current measured total bitrate of the output transport stream. This value may vary slightly from the configured value due to measurement errors.

Effective bitrate

This shows the effective bitrate of the output transport stream.

Forced stuffing

This parameter is used if there is a need to guarantee a minimum amount of null packets (PID 8191) in the output transport stream. When enabled the parameter specifies the maximum number of non-null packets to transmit before inserting a null packet. The forced null packet inserter operates at the priority level just below the MIP packet inserter. The stuffing bitrate resulting from the configured value and the corresponding percentage of the total stream is displayed to the right and is visible before pressing apply. The range of the parameter is 1-65565. Typing 1 would mean transmitting a null packet in every second packet position; typing 99 would guarantee 1% stuffing.

Stuffing packets

This status parameter shows the number of stuffing packets transmitted on the output. The value can be cleared with the R button next to it. The main intention with this parameter is to display the efficiency of the MUX when trying to achieve a stream fully saturated with EIT insertion.

ASI mode

This lets the user choose how to transmit the transport stream packets on this output, burst mode or spread mode. If output format is set to SMPTE 310M this option is hidden.

Packet length

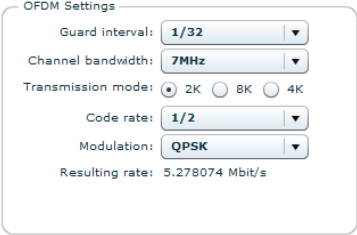
This lets the user configure the output to transmit 188 or 204 byte transport stream packets. If output format is set to SMPTE 310M this option is hidden.

The TS Identifier Settings section enables you to select how to handle TS-ID and Original Network ID in regenerated PSI/SI tables.

Remap TS Identifiers

Check this box to manually enter the TS-ID and Original Network ID to use for the output stream. **In ATSC mode Original Network ID can not be overridden.** If the box is unchecked you must select the input that carries the TS-ID and original network ID that should be auto-tracked.

The OFDM Settings section:



OFDM Settings

Guard interval:

Channel bandwidth:

Transmission mode: 2K 8K 4K

Code rate:

Modulation:

Resulting rate: 5.278074 Mbit/s

Figure 8.68 Output Configuration - OFDM settings.

If the bitrate is configured based on OFDM parameters a new section appears to the right of the Main Configuration section, as show in figure 8.68. This section allows the configuring of the following parameters:

Guard interval

This is where the guard interval between symbols is set.

Channel bandwidth

The bandwidth to use for this channel.

Transmission mode

Selects the transmission mode to use, i the number of carriers per symbol.

Code rate

Selects which code rate to use in the range of 1/2 to 7/8.

Modulation

This lets the user choose the modulation scheme to use for this output.

Resulting rate

This value shows the resulting bitrate if hitting 'Apply' with the selected OFDM parameters.

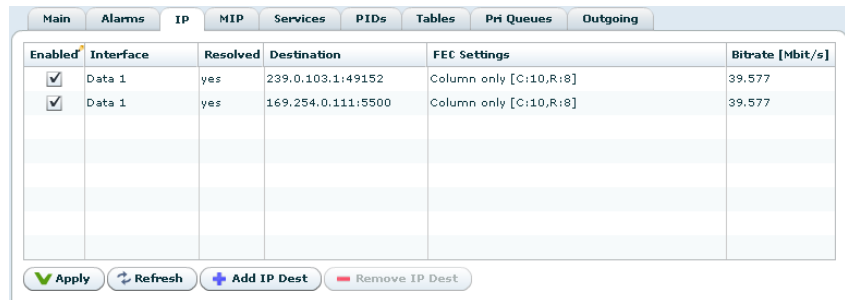
8.6.2.2 Alarms

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 8.5.2.2](#)).

8.6.2.3 IP

This page provides a table showing all available ip outputs, listing salient features of each and providing quick access to enabling or disabling each output, [Figure 8.69](#).



Enabled	Interface	Resolved	Destination	FEC Settings	Bitrate [Mbit/s]
<input checked="" type="checkbox"/>	Data 1	yes	239.0.103.1:49152	Column only [C:10,R:8]	39.577
<input checked="" type="checkbox"/>	Data 1	yes	169.254.0.111:5500	Column only [C:10,R:8]	39.577

Figure 8.69 IP outputs list.

The table contains the following columns:

Enabled

Check or uncheck this box to enable or disable the output. Click Apply to confirm.

Interface

The port of the output.

Resolved

Indicates Yes if the IP destination has been reached.

Destination

IP address and port number of the destination.

FEC Settings

Shows if output FEC has been applied and the column and row sizes, as applicable.

Bitrate

The total output bitrate, including FEC (if applied).

Double clicking on a table line takes you directly to the specific page for configuring the output. Refer to [Section 8.6.4.1](#).

8.6.2.4 Services

The Services page ([Figure 8.70](#)) lets the user configure which services to transmit and which to stop, selected from the services available in the input. The user can also remap service ids from this page and perform service component manipulations.

At the top of the page the user may choose to pass "All" services through by default if no other rules shall be applied to the services. Any changes to the service constellation on the input port will then be reflected to the output. Press the Apply button next to the drop down menu to activate the setting. If "None" is selected each service that shall appear on the output must be expressly enabled.

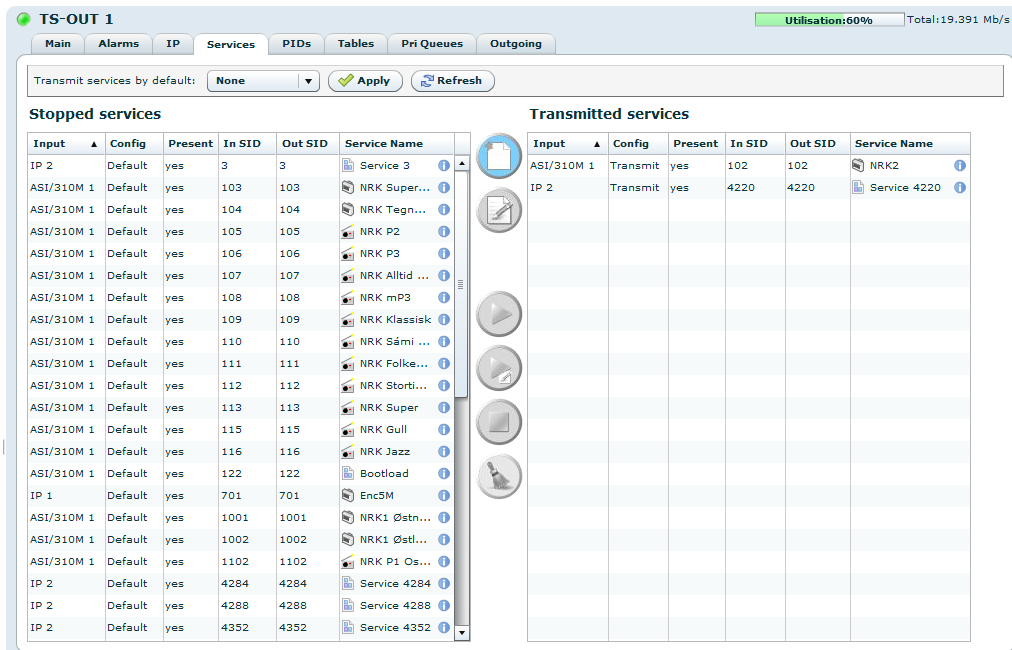


Figure 8.70 Service configuration page

Beneath the default transmit setting are two tables showing what services are currently stopped and what services are currently being transmitted. Both tables have the same columns:

Input

The port on which the service is present.

Config

This is the current configuration applied to the service. If the service has not been configured, this column says Default and the service adheres to the default rule, appearing in the appropriate table. A service configured to Transmit will always appear in the transmitted table and a service configured to Stop will always appear in the stopped table.

Present

This tells whether the service is currently present in the input signal. Therefore it also tells if a service configured to be transmitted is actually transmitted. If the present column says no, it is not present and therefore not transmitted. Services that are not present in the input are greyed out in both tables.

In SID

This is the service-ID, or program number as it appears in the source input.

Out SID

This is the service-ID, or program number, as it will be transmitted. In services with default configuration this will always be equal to the incoming service-ID.

Service name

This is the name of the service. If no SDT actual is present on the chosen input or if it is not being analysed, this column will show a dummy name. For ATSC services, the service

name is a concatenation of the short channel name, and major/minor channel numbers. To the right of the name is an information icon.

Information icon

Leave the cursor over the blue *i* icon to the right in each service row to display more input information about a service.

Double-clicking a row in the table will bring up the service edit dialogue for that service. Right-clicking on a row in the table lets the user add, remove or edit the configuration of the chosen service(s). These procedures are described below.

In between the two tables is a row of buttons ([Figure 8.71](#)) allowing the user to add, remove or edit a configuration of the chosen service(s).

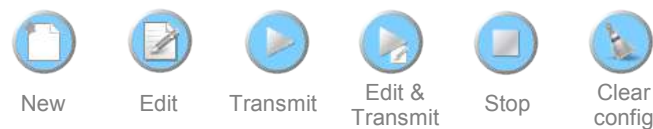


Figure 8.71 Service configuration action buttons

The buttons are grey when they are inactive and blue when they are clickable. The buttons are as follows:

New

This button creates a new configuration from scratch. This button is always active. When clicking it a new dialogue opens where the user can select what input the configuration should apply to, what service-ID of the chosen input the configuration should apply to, what ID the service should have in the output and what kind of configuration to apply. This can be used to apply a configuration to a service that is not currently present on the input.

Edit

This button allows the user to edit configurations already created. This button is activated by selecting one or more services from either list that have a configuration applied to it. When the button is hit a dialogue will open, which lets the user edit the configuration.

The top of the dialogue shows which service is currently being edited (service-ID in brackets). If more than one service is selected, two buttons allow the user to switch between selected services.

The service edit dialogue is covered in more detail in [Section 8.6.2.5](#).

Transmit

This button becomes active when selecting one or more services with no configuration or a configuration to be stopped. Clicking it applies a configuration with "Transmit" mode and default parameters to the selected service(s). This means that the selected service(s) will be transmitted. The change is immediate, with no extra request for confirmation.

Edit & Transmit

This button becomes active when selecting one or more services with no configuration or

a configuration to be stopped. Clicking it opens the same dialogue as the Edit button, but with the Config Mode drop down list set to "Transmit" by default. The service(s) will not be transmitted until Apply in the dialogue is hit.

Stop

The button becomes active when selecting one or more services with no configuration or a configuration to be transmitted. Clicking it applies a configuration to the selected service(s) with "Stop" mode. This means that the selected service(s) will be stopped. The change is immediate with no extra request for confirmation.

Clear Config

This button becomes active when selecting one or more services with a configuration applied to it. It removes the configuration from the selected service(s). This means that the services will be handled according to the default service behaviour.

8.6.2.5 Service edit dialogue

As seen above the service edit dialogue is accessed via various operations leading to configuration of one or more services. If more than one service is being configured the dialogue will have two buttons to switch between the services.

The service edit dialogue has the tabs General, Service Descriptors and Components, which are described in the following sections.

8.6.2.5.1 Service Edit – General

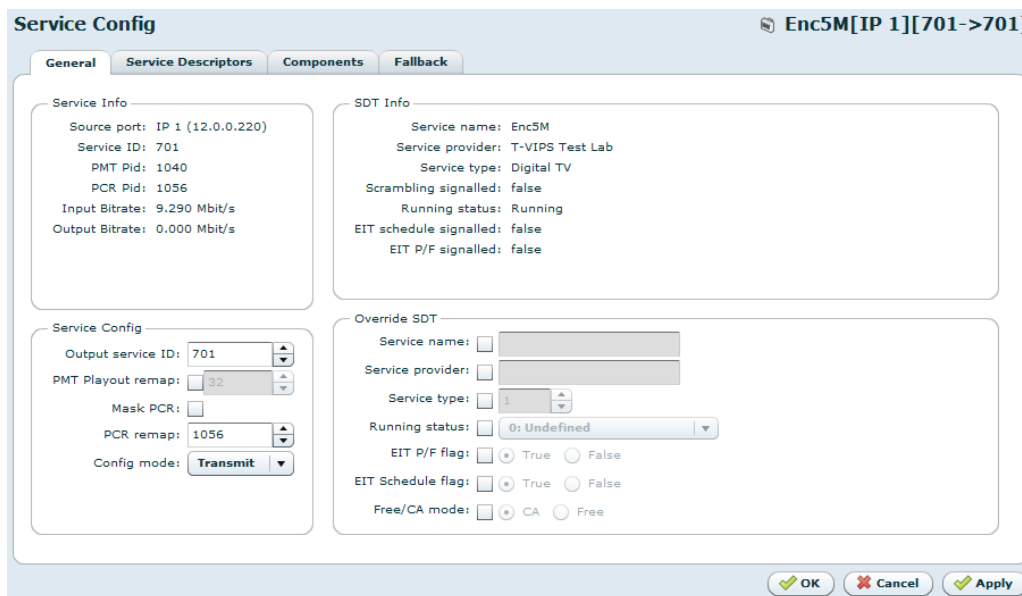


Figure 8.72 Service edit dialogue - General tab

The general tab is divided into four frames as shown in **Figure 8.72**.

The Service Info frame shows input status information for the service. It is greyed out if the service is not present on the input.

Source port

Input port that carries the service.

Service ID

The input Service ID of the edited service.

PMT PID

The input service PMT PID signalling the edited service.

PCR PID

The PCR PID related to the edited service, as signalled in the input PMT. This PID is often the same PID as the video PID, but may also be a separate PID.

Input Bitrate

Bitrate calculated for the input services by adding the bitrates of all PIDs signalled in the service.

Output Bitrate

Bitrate calculated for the output services by adding the bitrates of all PIDs signalled in the service.

The Service Config frame allows the user to configure parameters for the service in the output transport stream:

Output service ID

The service-ID to use in the PSI of the output. This value will replace the service-ID found in the input PAT and PMT.

PMT Payout remap

Check this box if the output PMT shall have a different value from that of the input PMT. Enter the new PID value for PMT in the box provided. If left unchecked the incoming PMT PID will be re-used in the output.

Mask PCR

A special feature to suppress a signalled PCR PID if it is not used. PCR is deemed not to be in use if

1. PCR PID is not signalled as a component in a PMT component loop, or
2. this PMT does not signal any Video nor Audio PIDs.

When PCR is not in use and the "Mask PCR" parameter is set, the PID signalled as PCR is ignored in the routing process. Also the PCR PID is set to 8191 ("Null" packet) in the re-generated PMT.

This feature can be used when handling time-shared services that share a Video/PCR PID that should be locally remapped to different output PID values depending on which service is currently active, while the PCR field is not set to 8191 on the services that are off air, causing a PID conflict.

PCR remap

The field enables the user to remap the PCR PID to a new value on the output. The PID will be assigned the new PID value on the output, and the PCR field in the PMT will be re-stamped. By default this field displays the PCR PID currently signalled in the input.

If a value different from the incoming PCR PID value is entered, a config entry for the PID is written to the global remap table to remap the PID in all services sharing this PID. Since the config entry specifies an input PID to output PID mapping the remap entry will not match if the PCR PID changes in the input. The new PID will therefore not be remapped.

It is also possible to remap PCR PIDs by adding a reference to the PID in the component list of the Components tab. Thus, if a service has PCR embedded in one of the component PIDs, it is preferable to configure re-mapping using the Component tab.

Config Mode

Whether to write a "Stop" or "Transmit" config entry for the service. The other parameters are only relevant if this parameter is set to "Transmit".

The SDT Info frame:

If the **TS mode** of the output port is **DVB** this frame shows information from the service loop in the SDT actual of the input. If SDT actual is not present in the input this section is disabled and shown in grey.

- Service Name
- Service Provider
- Service Type
- Scrambling signalled (Free_CA flag)
- Running status
- EIT schedule signalled bit
- EIT p/f signalled bit

When the **TS output mode** is **ATSC**, the SDT Info section is replaced by a VCT Info section, as shown in [Figure 8.73](#).

The following information for ATSC services is shown:

- Channel name
- Major/minor channel number
- Service type
- Modulation mode
- Channel TSID

VCT Info

Channel name: KLCS-DT
 Channel number: 58 . 3
 Service type: ATSC Digital TV
 Modulation mode: ATSC 8VSB
 Channel TSID: 309
 Access controlled: false
 Source ID:

Override VCT

Short channel name: Dude TV
 Major channel number: 1
 Minor channel number: 23
 Channel TSID: 309
 Program number: 345
 Source ID: 1
 Modulation mode: 4: ATSC (8 VSB)
 Service type: 2: ATSC Digital TV

Figure 8.73 Service edit dialogue - VCT info

- Access controlled
- Source ID

The Override SDT section offers to override incoming SDT fields in outgoing SDT actual. Each of the fields listed can be overridden independently of the others. Fields not overridden will track the values of the incoming SDT actual.



Note: Overriding of SDT fields requires that SDTa analysis is turned on on the input, that there is an SDT on the input and that SDTa is set to "Payout Regenerated" on the output.

The fields that can be overridden are:

Service name

Name from service descriptor.

Service provider

Provider name from service descriptor.

Service type

Type from service descriptor.

Running status

Running status field from SDT service loop.

EIT P/F flag

EIT present/following presence flag from service loop.

EIT Schedule flag

EIT schedule flag from service loop.

Free/CA mode

Scrambling indicator from service loop.

To override a field, enable the check box next to it and assign the wanted value for the field.

The Override VCT section is also visible only if the **TS output mode** is **ATSC**. It offers the possibility to override incoming VCT fields in the outgoing VCT. Each of the fields listed can be overridden independently of the others. Fields that are not overridden will have the same values as the incoming VCT.



Note: Overriding of VCT fields requires that VCT analysis is turned on on the input, that there is an VCT on the input and that VCT is set to "Playout Regenerated" on the output.

The fields that can be overridden are:

Short channel name

Overrides the short channel name in the VCT.

Major channel number

Overrides the major channel number in the VCT.

Minor channel number

Overrides the minor channel number in the VCT.

Channel TSID

Overrides the channel transport stream ID in the VCT.

Program number

Overrides the program number in the VCT. This should normally be left unchecked, to follow the remapping of the program number.

Source ID

Overrides the Source ID field in the VCT. Remark that the value chosen here must link to a source ID in the EIT on the output.

Modulation mode

Overrides the modulation mode in the VCT.

Service type

Overrides the service type field in the VCT.

8.6.2.5.2 Service Edit - Service Descriptors

There are two status frames on this tab (see [Figure 8.74](#)). On the left the PMT Program Descriptors shows the descriptor list from the program information loop in the PMT of the service, and on the right SDT Descriptors shows the service descriptor loop for the service from "SDT actual" in the input. If either descriptor loop is empty, the corresponding frame does not show any information. If the output is an **ATSC** service, the SDT descriptor frame is not shown.

There are also two configuration frames, the PMT Program Descriptor Rules frame and the SDT Descriptor Rules frame. If the **output mode** is **ATSC** the latter is not shown. These may be used

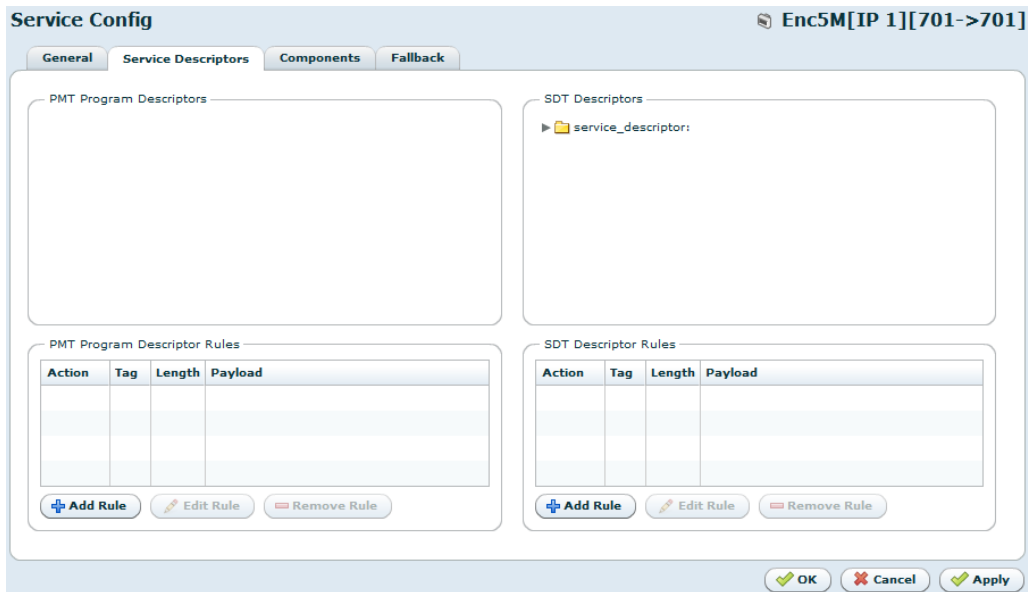


Figure 8.74 Service edit dialogue - Service Descriptors tab

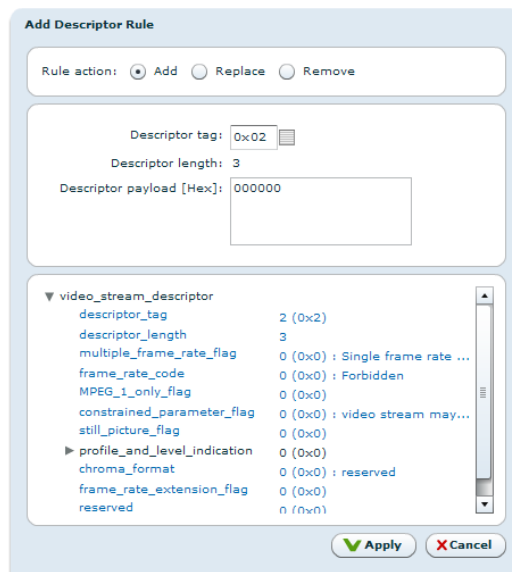


Figure 8.75 Service Descriptors tab - Add rule

to add, replace or remove descriptors in PMT or SDT, respectively. This is done by pressing Add Rule, which brings up the dialogue as shown in [Figure 8.75](#).

Note that this dialogue is slightly different when removing a descriptor, which only requires that the tag value is entered.

Descriptor tag

Specify the descriptor tag value, in hexadecimal notation, for the descriptor you want to

add/replace/remove. Clicking on the small icon next to the text field brings up a helper dialoge converting the hexadecimal code to a textual description.

Descriptor length

This field is automatically set based on the chosen descriptor tag.

Descriptor payload

The payload of the descriptor.

In the window below the text fields is a status summary. This field will give more information about the specified descriptor, and will state if the length of the descriptor payload is outside specifications.

8.6.2.5.3 Service Edit - Components

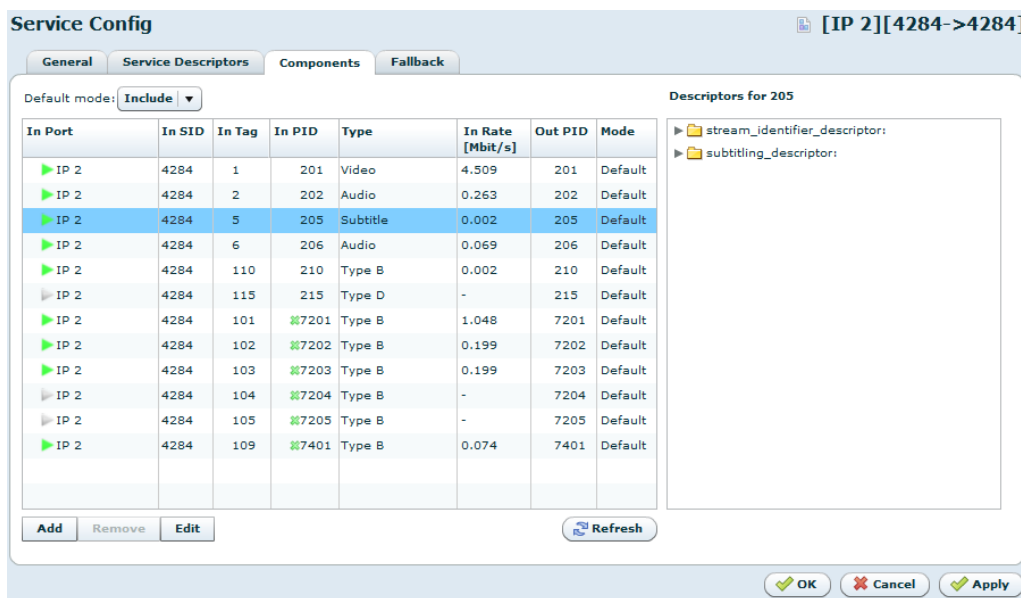


Figure 8.76 Service edit dialogue - Components tab

In the Components page the user may perform filtering and remapping of service component PIDs. Components rules may be added either by matching PID value or by matching component tag from the stream identifier descriptor if this is present on the input. Each rule may configure a mode, priority and local-to-service remap value of the component. In addition global remaps may be added from this dialogue for shared components.

If a component is matched by more than one rule, the precedence of the rules is

1. Global remap
2. PID rule
3. Tag rule

This means that if a global remap is configured any local remap is ignored. If both a PID rule and a Tag rule applies to a component the parameters configured in the PID rule are used. If a shared component is configured with different priority in different services the highest priority is always used in the routing.

At the top are two parameters controlling the default behaviour when routing components of this service.

Default Mode

The default way to handle service components that have no other rule. When set to Include any service component not specified further below will be transmitted unchanged. If set to Exclude components that have no specific rule saying Include will be stopped.

Default priority queue

This parameter sets the default priority of components routed without applying an overriding rule.

The data grid in [Figure 8.76](#) shows a view of PIDs that are signalled in the PMT of the service and the results of configuration rules that have been added to the service. The components displayed include the ECM PIDs found in CA descriptors associated with the service. PID rules may be added to match a shared/separate PCR PID as well, even though such PCR PIDs are not displayed as a component in the grid.

When clicking a row, a request is launched towards the unit to collect the component descriptors of this component from the input PMT. These are shown to the right when the answer to the request is received.

The columns in the grid are:

In Port

The source port of the PID. A symbol indicates the current status of the component. A "play" symbol is shown for components that will pass, a "stop" symbol is shown for components that will be stopped. If the component is not present at the moment the respective symbol is shown in grey. A "plus" symbol is used to indicate a component that has been added to the service, i.e. not present in the incoming PMT.

In SID

The input service ID carrying this PID

In Tag

The component tag found in the stream identifier descriptor of the given component when available. A matching tag rule found for this component is indicated with a pencil next to the tag value.

In PID

The input PID value of this component stream. A matching PID rule found for the PID is indicated with a pencil next to the PID value.

In Type

The decoded component type of this stream.

In Rate

The input bitrate of this PID.

Out PID

The PID value to use and signal in the output. A remapping configured for the component is indicated with an "R" for a local-to-service remapping, and an "R" over a globe for global remapping.

Mode

The rule to apply for this component. The options are:

Default

Use the default mode for the service as specified in Default Mode

Include

Transmit and signal this component if signalled in input.

Exclude

Stop elementary stream and remove signalling of this component.

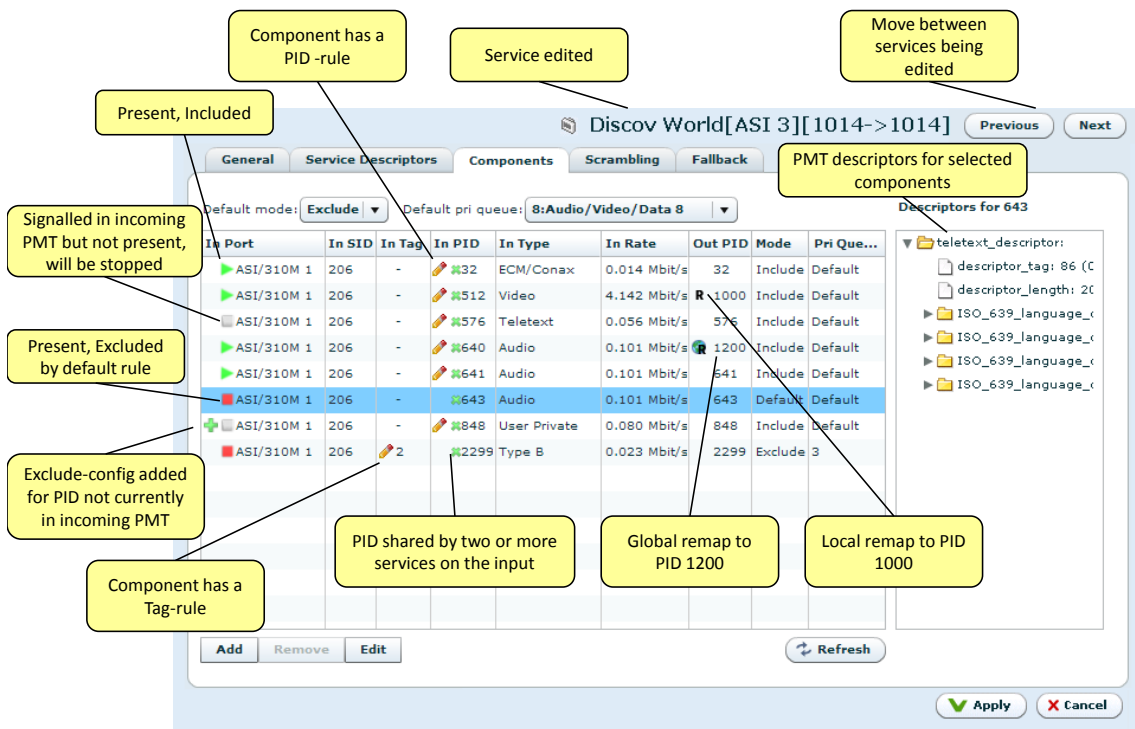


Figure 8.77 Component dialogue - Important elements.

Figure 8.77 points at important screen elements on the Components tab.

There are three main operations in the component dialogue: Add, Remove and Edit. These are described in the following.

The Add button

This is used to add a new service component that is signalled in a service on any input port(s) or to add a custom component. In this way you may add configuration for a service component that is not present at the moment, or you may add signalling of a service component from

a different service to include this PID in the output. Note that this may not work in target decoders if the component carries the PCR.

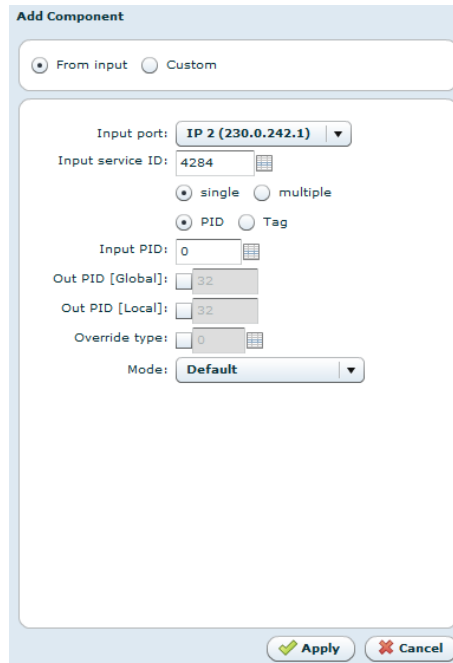


Figure 8.78 Component add dialogue - Components tab

Clicking the Add button and selecting From input brings up a dialogue [Figure 8.78](#) where the port for the PID, the service containing the PID, and then the PID itself (or a component tag) is selected. A new output PID may be assigned to the component as well, selecting either between global or local remap as described before.

Input Port

The input port where the component is or will be signalled. A selection box shows available input ports.

Input service ID

The service in which the signalling should be regenerated. Type a service ID or selection one from the list of services currently present on the selected input port.

Single - Multiple

Two modes of adding. Use "Single" to add a single PID, in which case the remapping options will be available, or "Multiple" to add mode and priority parameters for a whole range of PIDs or tags. Ranges are specified in much the same manner as the page range option in the MS Windows print dialogue. (E.g. 100-103,105, which means numbers 100 through 103, plus 105).

PID - Tag

Whether to add PID a rule or a tag rule.

The remaining entries (Out PID, Override type, Mode and Priority) are as described for the component edit dialogue. See [Figure 8.81](#).

Clicking the Add button and selecting Custom brings up the dialogue as shown in figure [8.79](#). This dialogue shows the status of the added component. The drop down menu lists all the custom components added in this CP524. When a component is selected from the list the status will be shown in the field below. PID remapping may be done at the bottom of the dialogue window.

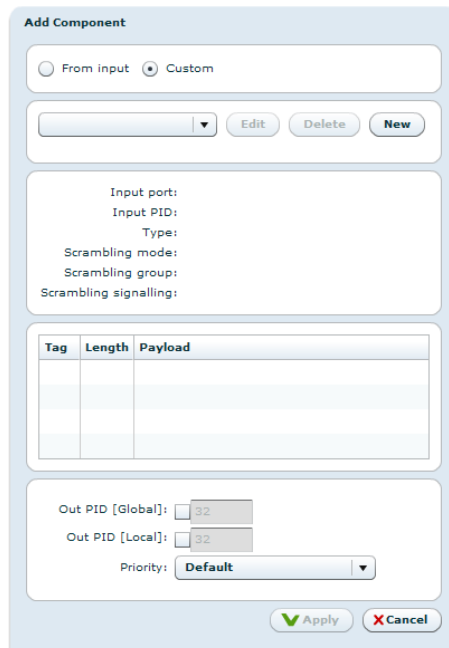


Figure 8.79 Component add dialogue - Custom components

To add a new component, press New. This brings up the dialogue as shown in [Figure 8.80](#).

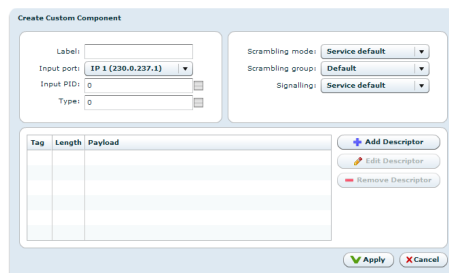


Figure 8.80 Component add dialogue - New custom component

In the dialogue you may add signalling for unsignalled incoming PIDs. The dialogue consists of one frame for defining PID value and PID type, one for component scrambling, and one for adding component descriptors.

Label

Specify a textual description of the component. Only used internally to identify new components.

Input port

Specify incoming port for the unsignalled PID.

Input PID

Specify incoming PID value, or select an unsignalled PID from the list. The list of unsignalled PIDs on the selected input port is shown when clicking on the icon next to the text field.

Type

Select the PID type you want to be signalled for the new PID. Click on the icon to the right for a list of possible types.

Scrambling mode/group/signaling

Enable this if you want to scramble the component.

The lower part of the dialogue in [Figure 8.80](#) enables adding component descriptors. Adding a descriptor is done by clicking Add Descriptor. See section [8.6.2.5.2](#) for further information.

The Remove button

This button removes entries that have previously been added. This only works for entries labelled with a plus sign.

The Edit button

Figure 8.81 Component edit dialogue - Components tab

The handling of a present component can be determined by selecting the row (or multiple rows) and clicking the Edit button below the grid in [Figure 8.76](#). This pops up another dialogue [8.81](#) where rules for this component may be added or edited. The same can be achieved by double-clicking the row in the table or right-clicking the row and selecting Edit.

Fast short-cuts to configure mode parameters of a component PID rule are available by selecting the component to which a rule should be edited and select either "Include", "Exclude" or "Default".

The Status frame in [Figure 8.81](#) shows the pre-filled values of the key fields needed to add a rule for the selected component.

In the PID Config frame parameters for a PID rule or global PID remapping may be added. The PID Config section has the following fields:

Out PID [Global]

This field is used to add global remapping for the input PID, which will be shared by all services referring to this service. New values entered here will be written to the global PID remapping table and will also be visible in the PIDs tab. The remapping value is only used if the PID is referenced in a service. Global remapping always takes precedence if there are both local and global remapping entries found for a component.

Out PID [Local]

This field can be used to remap a PID only when it is signalled in this specific service. If the PID is shared with other services this configuration entry must be used with care. Configuration conflicts may easily occur; different services may configure different output PID values for the same input PID.

The field is mainly intended for use in time-share multiplexes where a PID moves between services at different times of the day, and a different output PID is required in each service.

Also, this field may be used on a tag rule to achieve a fixed output PID for a given tag in this service, even when the input PID changes. If a configuration renders a PID conflict, an alarm will be raised by the unit.

Mode

"Include", "Exclude" or "Default". What how to handle the component if it is signalled on the input.

Pri Queue

Priority queue to use for this component. For shared components the highest priority queue assigned is used.

The Tag Config frame is used to add a rule for a specific component tag. Normally one would choose either to use a PID rule or a Tag rule for one component. If both rule types are added, the PID rule will be matched first taking precedence over any settings of the tag rule.

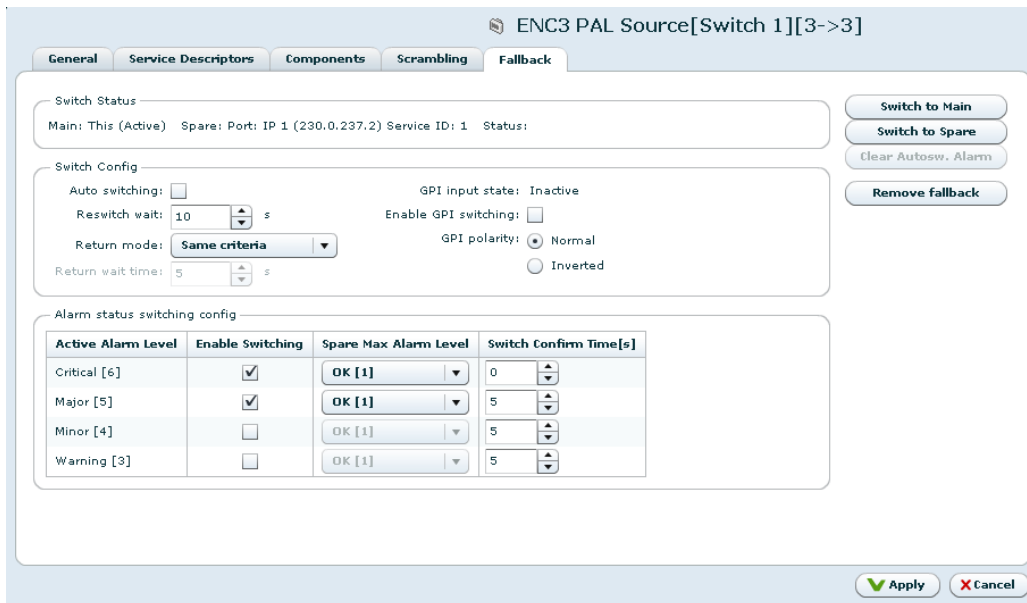
If more than one component was selected, the dialogue will look slightly different. At the top will be a list of components currently being edited. Only mode and priority queue may be edited. If selected components have different values in any of the two fields, the drop down will be set to Multiple. Keeping the drop down set to this value will preserve the current values for the components.

8.6.2.5.4 Service Edit – Fallback

On the fallback tab you may add and configure a fallback service. If no fall-back service is configured yet, the tab shows fields to select a fall-back service, otherwise the page consists of three main sections.



Note: Service fall-back is a licensed feature and this tab is only visible if the licence key is installed.



Active Alarm Level	Enable Switching	Spare Max Alarm Level	Switch Confirm Time[s]
Critical [6]	<input checked="" type="checkbox"/>	OK [1]	0
Major [5]	<input checked="" type="checkbox"/>	OK [1]	5
Minor [4]	<input type="checkbox"/>	OK [1]	5
Warning [3]	<input type="checkbox"/>	OK [1]	5

Figure 8.82 Service edit dialogue - fallback tab

In the top right corner are two switch buttons. When you click on one of these buttons, you switch immediately to that input. You get a confirmation box, but once you click OK in it the switch happens immediately, regardless of any configured minimum delays. There is also a button Clear auto sw. alarm. This is enabled when the alarm “Auto switch performed” is enabled and raised (Alarm ID 510). This alarm is intended as a notification to the operator that an automatic switchover has been done.

Pressing the Clear auto sw. alarm button will confirm and clear the alarm. Note that this alarm is disabled by default in the configuration. In order to use it you need to visit the Device Info page and set the alarm severity to a level different from filtered.

The top section shows the current status of the switch. It shows the main and spare ports and which of them is active at the moment. The state of the switch is also shown. The switcher has the following states:

Active

While in active state, the alarm status of the active input is monitored. If it changes to a severity that has switching enabled, the alarm severity of the spare input is checked. If it is

lower than the maximum allowed severity as configured the state changes to the Waiting for alarm Confirmation state. Upon initialisation the switch enters the active state after a 20 second timeout.

Waiting for alarm Confirmation

While in this state, a timer starts counting down from the configured wait time. When in Return if main OK mode the wait time is "Return wait time", while in the other modes the wait time is the "Switch wait time" for the active alarm level. If the alarm levels of the active and spare inputs are no longer in a state that warrants switching the device returns to the "Active" state. If the timer reaches zero a switch is performed and the device enters to the "Waiting" state.

Waiting

In this state a timer starts counting down from the configured "Reswitch wait" time, which is the minimum time between switches. When it reaches zero the device returns to the Active state.

The Switch Config section contains these configuration parameters:

Auto switching

Checking this box enables automatic switching. When enabled the switch will switch based on the alarm status of the inputs, following the rules set up in the Alarm status switching config section.

When auto switching is enabled the switcher is configured to one of three return modes:

Return if main OK

When the main input becomes OK again, the controller will automatically switch back to the main input.

Same criteria

The controller will switch between the inputs automatically when the switch criteria are met.

Never switch back

The controller will do one automatic switch from the main input. The switch controller can be rearmed by a manual switch to the main input.

When GPI is available, the current GPI signal level is presented, together with parameters to enable switching based on GPI. Read more about switching based on GPI in [Section 5.10.3](#).

GPI input state

Shows whether the GPI input state is Active or Inactive.

Enable GPI switching

Choose whether switch controller should react to GPI state changes.

GPI polarity

Option to invert the logic on which service is selected when GPI goes active. Normal means spare is selected if GPI turns active, main is selected when it goes inactive.

The Alarm status switching config section at the bottom of the page is only active when you have enabled alarm status switching. It dictates when to perform switching. On the left is a table containing all possible alarm severities. For each severity you can choose whether you want to perform a switch when that severity is reported on the currently active input. In addition you can configure what the maximum alarm severity can be on the spare input.



Note: You can not enable switching on certain alarm severity levels without also configuring switching on all higher severities. The web interface automatically makes sure you follow this rule.

To the right of the table you can configure the Switch wait period. This value is the number of seconds the state that warrants a switch must be in place before actual switching is performed.

8.6.2.6 PIDs

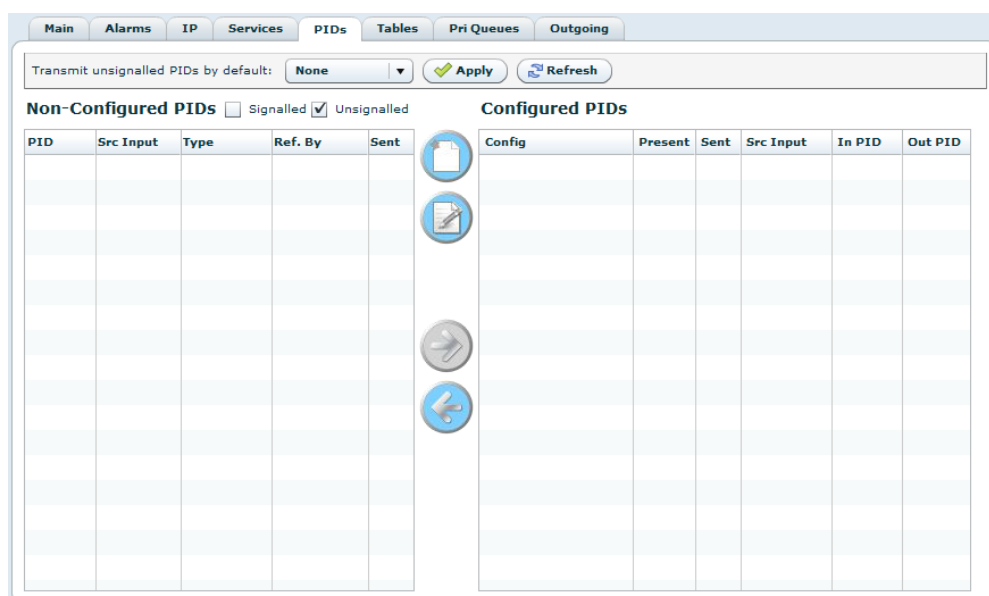


Figure 8.83 PID configuration screen

The PIDs page allows to manually configure PIDs to be transmitted or stopped, without the PID having to be signalled in the PSI.

This page is mainly used to set up rules for unsignalled PIDs, but may also be used to configure PIDs that are part of a service. Another frequent use of this dialogue is to enter a new PID value for the EMM in the output. When applying re-mapping in the service component dialogue ([Section 8.6.2.5.3](#)), the remapping rules become visible here.

At the top of the page the user may choose to pass unsignalled PIDs through by default if no other rules are applied to the PID. Press the Apply button next to the Drop-down menu to activate the setting. Any new unsignalled PID appearing on the input will then be passed on.

Beneath the Drop-down menu are two tables. The left hand table shows all PIDs that have no configuration added; the right hand table shows all configured PIDs. When a configuration is

added to a PID, it will disappear from the left hand table and appear in the table to the right. Above the left hand table are two checkboxes. They determine simply what PIDs to list in the left hand table; they do nothing to the configuration of the unit.

The left hand table has the following columns:

PID

The packet id. The blue information icon offers a tool-tip with more information about the PID.

Src Input

This tells the PID input port.

Type

For signalled PIDs this shows the PID type. For unsignalled PIDs this column is empty.

Ref. By

Shows a comma separated list of all service ids that reference this PID. If the list extends beyond the cell, holding the mouse cursor over the cell will show all service ids.

Sent

This shows whether the PID is currently being transmitted.

The right hand table has these columns:

Config

This column shows what kind of configuration applies to the PID. It tells the device what to do with the PID.

Pri

The priority assigned to this PID routing.

Present

This tells whether the PID is present on the input. If it is not, this says "No" and the PID is greyed out.

Sent

This shows whether the PID is currently being transmitted.

Src Input

This is the input for which the configuration is valid. A configuration will only apply to the selected PID if it comes from the specified source input.

In PID

This is the input packet id. The blue information icon carries more information about the PID in its tool-tip.

Out PID

This is the packet id allocated to the transmitted packet. Remapping a packet id will cause this id to be different from "In PID".



Figure 8.84 PID configuration buttons

Between the two tables are a series of buttons (**Figure 8.84**) that can be used to add, remove or edit a configuration. The buttons are grey when inactive and blue when they are clickable. The buttons are as follows:

New

This button allows the user to create a new configuration from scratch. This button is always active. When clicked a new dialogue opens where the user can select the input for which the configuration should be applied, the packet id in that input signal for which the configuration should apply, what output PID value and what kind of configuration to apply to it (see Edit below for further description). This can be used to apply a configuration to a PID that is not currently present on the input.

Edit

This button allows the user to edit configurations already created. This button is activated by selecting one or more PIDs from the list of configured PIDs. When the button is hit, a dialogue will open allowing the user to edit the configuration.

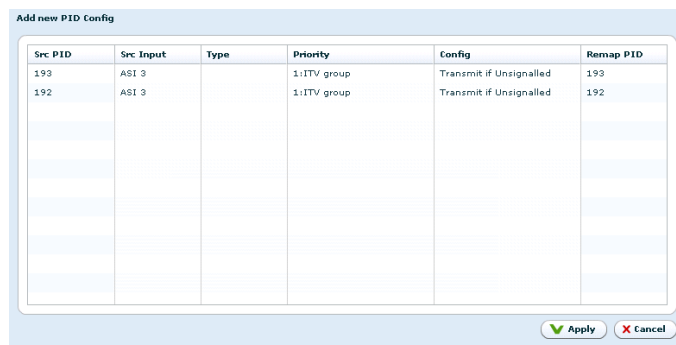


Figure 8.85 PID configuration edit

The dialogue **8.85** consists of a table showing the selected PIDs. It has the following columns:

Src PID

The PID on the input.

Src Input

The input port the PID is coming from.

Type

The PID type, empty for unsignalled PIDs.

Priority

The priority to use for this PID routing. This field determines in which priority queue the TS packets for this PID are put when routed through the unit. The priority level determines

which data to drop first in the event of an overflow. See separate chapter for a description of the different priority queue levels.

Config

The configuration to apply to the PID. By clicking on this cell, a Drop-down menu will appear where the user can choose which configuration to apply. Options in the config Drop-down menu are as follows

Stop if unsignalled

Stop this PID if it is *not* signalled in PSI.

Stop if signalled

Stop this PID if it *is* signalled in PSI.

Stop always

Stop this PID, whether it is signalled in PSI or not.

Transmit if unsignalled

Transmit this PID with given new PID value if the PID is *not* signalled in PSI.

Transmit if signalled

Transmit this PID with given new PID value if it is signalled in PSI. When a remap is entered in the service edit dialogue ([Section 8.6.2.5](#)), the GUI writes this kind of entry into the PID table, and it will be visible in the configured PID list.

Transmit always

Always transmit this PID, with the given new PID value.

Remap PID

The identifier wanted for the packet when transmitted. By clicking on the Cell, the wanted id can be inserted.

Add

This button opens the same dialogue as is opened when the Edit button is clicked. The only difference is that this button is activated when PIDs in the non-configured list is selected.

Remove

This button removes the configuration from the selected PID(s).

8.6.2.7 Tables

The Tables page allows the user to configure the payout of PSI/SI tables. It is divided into several sub pages. Toggling between pages is done by clicking on the icons at the top of the "Tables" page.

8.6.2.7.1 Main

In this page the user can configure the backlog time for table playout, EIT packing and the way to play out supported tables.

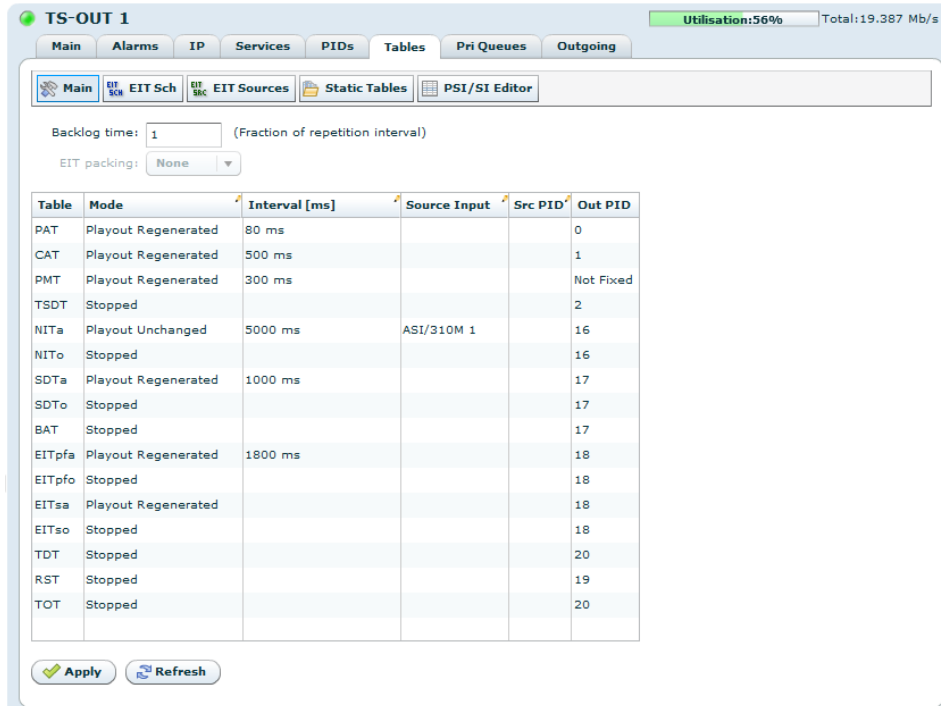


Table	Mode	Interval [ms]	Source Input	Src PID	Out PID
PAT	Playout Regenerated	80 ms			0
CAT	Playout Regenerated	500 ms			1
PMT	Playout Regenerated	300 ms			Not Fixed
TSDT	Stopped				2
NITa	Playout Unchanged	5000 ms	ASI/310M 1		16
NITo	Stopped				16
SDTa	Playout Regenerated	1000 ms			17
SDTo	Stopped				17
BAT	Stopped				17
EITpfa	Playout Regenerated	1800 ms			18
EITpfo	Stopped				18
EITsa	Playout Regenerated				18
EITso	Stopped				18
TDT	Stopped				20
RST	Stopped				19
TOT	Stopped				20

Figure 8.86 Table configuration main page

Note that "Backlog time" and "EIT packing" are not visible if the output is in ATSC mode. The "EIT packing" option is available if the appropriate licence has been installed.

The "Backlog time" is specified as a fraction of the table repetition interval. Its usage is described in detail in [Section 5.9.5](#).

The "EIT packing" parameter is used to control the packing of EIT sections into TS packets. The different modes are:

None

Each section is started in a new TS packet, and padding will always be inserted after a section to fill up the last TS packet.

Light

In this mode the player will always try to pack sections together. However, no more than one section will start per TS packet. Also, section headers are not allowed to be split between two TS packets.

Tight

This is the mode that will give the highest possible packing (and therefore the lowest resulting bitrate). Several sections are allowed to start in the same TS packet, and section headers may be split between different TS packets.

Legacy

This is a special mode designed for compatibility with some brands of set top boxes. It is the same as the "Light" mode, except that no "EIT schedule actual" and "EIT schedule other" sections are allowed to be transmitted in the same TS packet.

SI/PSIP table handling falls into two main categories, "Passthrough" or "Playout" modes.

Passthrough modes

All modes that start with the word "Passthrough", implies that the table is passed through the unit by mapping a PID stream through, much the same was as for the video and audio elementary streams. When a table is treated in "Passthrough" mode, all other table types that are transmitted on the same PID must be treated the same way. In these modes it is not possible to configure a new repetition interval for the table.

Playout modes

The other category involves playing out the table with the embedded SI playout module. These modes are recognised by having "Playout" in their name. When a "Playout" mode is selected, tables on the same PID can be multiplexed from different sources, and it is possible to specify the wanted repetition interval for the table.

The table in [Figure 8.86](#) shows the main table configuration screen consisting of a grid where the columns are:

Table

The short name of the table configured in this row.

Mode

How to handle this specific table. The options depend on the type of table. Double-click on the table cell to open the pull-down list of selections.

Stopped

The table will not be present on the output unless mapped through manually on the PIDs page.

Passthrough PID

The well-known table PID is passed through directly from the selected input.

Passthrough Remap

The user specifies a PID value and source port, and this elementary stream will be remapped to the well-known table PID in the output. This mode can be used to remap an unsignalled PID on any input port to the well-known PID in the output.

Playout Unchanged

The complete table is collected from the input data base of the selected input and played out as is. For PMT this means that all PMT sections on the input are posted for playout, and likewise for EITpfa. This mode is typically used for forwarding of BAT and SI-other tables (SDTo, NITo, EITpfo, EITso), while the SI-actual tables are set to "Playout Regenerated". For PSIP tables other than TVCT/CVCT, this is the only supported playout mode. (Note that it is also possible to configure pass-through for the tables in the PSIP base PID 8187).

Playout Regenerated

Regenerate mode is used for tables that need to be totally rebuilt due to changes in the service configuration.

Playout Static

This mode is used in conjunction with the "Static SI Configuration" described in [Section 8.6.2.7.5](#). The tables are retrieved from the static si database and played out unchanged.

Playout Internal

Used in order to generate TDT/TOT from the internal real time clock.

Interval

Playout interval in any playout mode, in milliseconds.

Source input

Input port from which to take the table. Only showed if appropriate.

Src PID

Source PID to use when in pass-through remap mode.

Out PID

Status field showing the PID value that will be used for this table.

Priority

Priority queue used for PID when configured to a pass-through mode.

Some rules must be observed when configuring table handling. For instance, if one table is in a passthrough mode, all other tables using the same PID must be in the same passthrough mode. If any of the configurations are illegal, the corresponding cells will turn red. Hovering the mouse over the red text will show a tip text explaining what is wrong. You will not be able to apply the changes until the errors have been cleared.




Note: If you are remapping TS-ID and Network-ID or changing the service composition of the output, you would normally configure PAT, CAT, PMT, and SDT actual to Playout Regenerated. In addition "EIT p/f actual" and "EIT schedule actual" can be configured to Playout Regenerated to ensure that only the sub-tables for the mapped services are played out, and that the TS-ID and service ID is re-stamped according to the service configuration.

8.6.2.7.2 EIT Sch

This page is not available when the output is in ATSC mode.

The page contains the EIT schedule configuration field where user can configure the playout of the EIT Schedule tables. The following parameters may be configured:

Figure 8.87 EIT Schedule Configuration

 **Note:** The playout of EIT schedule requires that analysis of EIT schedule is turned on at the input.

Playout arbitration mode

This parameter selects arbitration characteristics for playout of EIT schedule sections. This mode only has effect when a specific table ID (e.g. 0x50) is split into two or more groups with different repetition rates.

The pull-down list provides a choice of values. The value chosen determines the number of sections that will be played out in sequence at a time for a given table ID. The meaning of the different values are:

Section

Sections from different groups can be played out in any order. Segments from different groups may be interleaved.

Segment

When playout of one segment (8 sections) start, it will not be interrupted by other segments until playout of the current segment is complete.

Group

Playout of one group (several segments) must be completed before any other group will be allowed to transmit segments. This mode will lead to quite large variations in measured repetition rate, but the playout sequence will be orderly.

The default value for EITs playout arbitration mode is "Segment".

Use constant section interval

This parameter is only effective when the arbitration mode is set to "Section". The parameter specifies how the sections of a particular table (indicated by a table ID) will be played out. If set to true, the player will calculate an *average* section repetition interval for all groups

and play out exactly one section at the end of each interval. If set to “false”, each group will be played out independent of each other. Sections within each group will have a distance that corresponds to the repetition interval for sections within that group only. If the arbitration mode is set to “Segment” or “Group” a constant section interval will always be used.

The "Use sliding window", "Use expired events" and "Expired Actual Interval/Other Interval" options are not supported yet, but may become available in the future.

Groups

The EIT schedule can be divided into up to 4 different groups with different playout intervals, each group consisting of an integer number of days (1 quarter of a sub-table). This is typically used to configure faster playout of the EIT data for the first days, and slower repetitions for EIT data for later days.

When setting a group to 0 days the group is not used.

8.6.2.7.3 EIT/ETT Sch

This page is not available when the output is in DVB mode.




Figure 8.88 EIT/ETT Schedule Configuration

The playout intervals for PSIP EIT/ETT tables is configured on a separate page, ([Figure 8.88](#)) accessed on the toolbar at the top of the Table Config page.

EIT base PID

Base PID for PSIP EIT tables, i.e. the PID of EIT-0.

ETT base PID

Base PID for PSIP ETT tables, i.e. the PID of ETT-0.

Number of EITs/ETTs

Number of EIT and ETT tables being sent, minimum 4 and maximum 128.

Interval (ms)

The repetition interval for EIT-0 and ETT-0 as configured on the main "Table Configuration" page.

Increment (ms)

The increment in repetition interval between table EIT(0) and EIT(1), and between EIT(k) and EIT(k+1).



Note: The playout of EIT/ETT requires that analysis of input EIT/ETT tables is enabled or that the tables are downloaded from a PSIP generating system such as the Triveni GuideBuilder.

8.6.2.7.4 EIT sources

This page is not available when the output is in ATSC mode.

Out Service ID	In Service ID	Schedule	Present/Following
1	1	ASI/310M 1	ASI/310M 1
2	1	ASI/310M 1	ASI/310M 1
3	1	ASI/310M 1	ASI/310M 1
4	1	ASI/310M 1	ASI/310M 1

Figure 8.89 EIT source configuration

The EIT source configuration table [Figure 8.89](#) specifies the remapping of EIT actual from any port and service ID to output service ID. If the EIT P/F actual is found on the specified Source SID and port then it will be inserted as EIT P/F actual on the specified output SID. If EIT P/F actual is missing and EIT P/F other exists then EIT P/F other will be inserted as EIT P/F actual on the specified output SID.

The EIT source configuration table is only in use for EITs in regenerated mode.

8.6.2.7.5 Static SI

The static PSI/SI tables used for playout is added through this page ([figure 8.90](#)).

Tables are added by using the Add button, or removed using the Remove button. When adding a table a dialogue is displayed where you can paste the table sections as an ASCII-encoded hexadecimal string ([Figure 8.91](#)).

Only one table can be committed at a time. When adding tables with more than one section all sections have to be pasted contiguously in the text area of the dialogue and then committed.

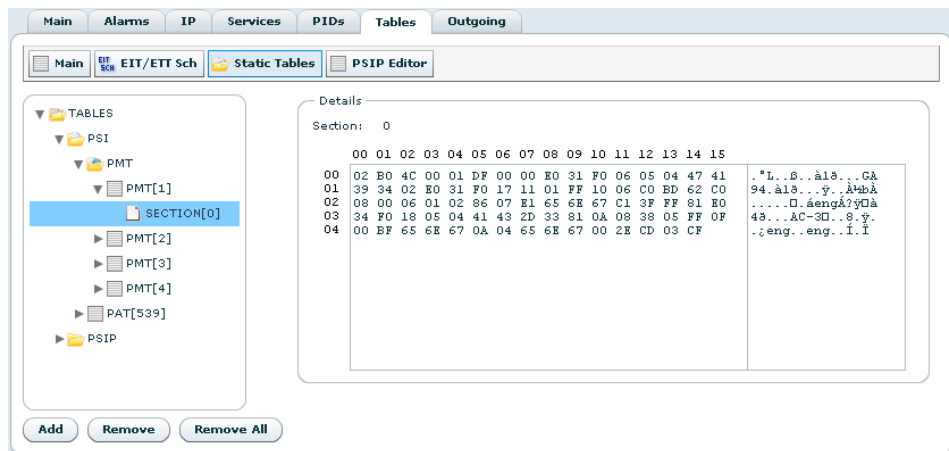


Figure 8.90 Static SI configuration

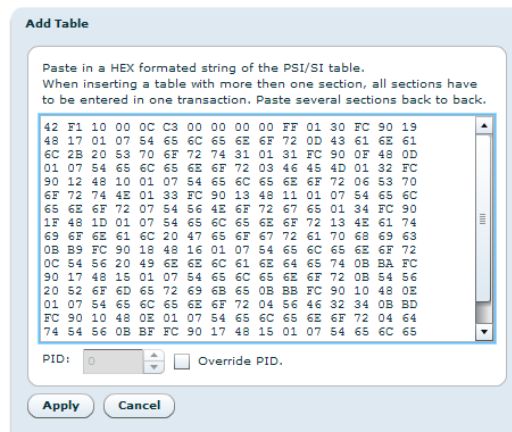


Figure 8.91 Add static SI table dialogue

When adding a PMT table be sure to enter the correct PID for this table. This PID must agree with the entries in the PAT. All tables can be transmitted on an alternate PID; this is done using the "Override PID" option.

The onus is on the user to ensure that added tables have the correct content and correct syntax. All table sections must start with the appropriate table id and end with the four byte CRC. The CRC is recalculated on a commit, thus the CRC does not have to be evaluated beforehand.

A simple method to obtain a correctly formatted hexadecimal string is to copy the decoded section of the wanted table under "Tables" on a T-VIPS CP545 or equivalent equipment.

8.6.2.7.6 PSI/SI/PSIP editor

The PSI/SI/PSIP editor allows the user to edit PSI/SI/PSIP tables manually. The user can build the tables from scratch or import tables from an input port, a file, the currently transmitted data or the currently stored static tables.

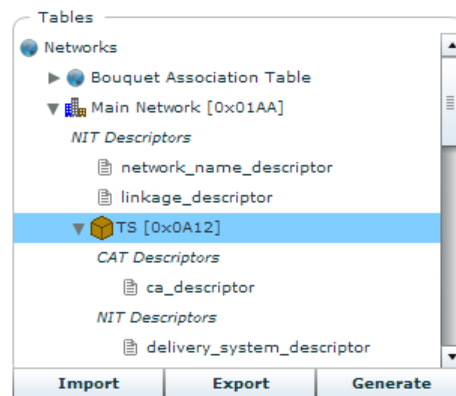


Figure 8.92 PSI/SI editor tree

After editing the tables the user can generate table sections and store them as static tables on the unit. These static tables will be played out as long as the table is configured to "Payout Static". ([Section 8.6.2.7.1](#)).

If the output is in DVB mode the PSI/SI editor will be available. If the output is in ATSC mode the PSIP editor will be available.

The PSI/SI/PSIP editor is split into two main parts. To the left is a tree showing the current structure of the PSI/SI/PSIP. Beneath the tree are three buttons that allow the user to import a configuration, export a configuration or generate PSI/SI/PSIP table sections.

When the user selects an item in the tree, configuration parameters for that item are shown to the right. Items that are displayed with italic font can not be selected, but can still be right-clicked.

Most items in the tree can be right-clicked and will then give a menu with appropriate options like adding new child items or removing the item itself.

The buttons below the tree are:

Import

Opens the "Import Tables" dialog where the user can import table data from the current ongoing data, the currently stored static tables, an input port or a file. To import data, select the radio button of the preferred source. Click the "Import" button. The imported configuration will now be shown in the text area labeled "Resulting configuration". To load this configuration, click the "Apply" button.

Export

Opens the "Export Tables" dialog where the user can copy the current configuration to the clipboard as a string or save it to a file.

Generate

This generates the table sections for the selected transport stream. If no transport stream is selected a dialog will be shown where the user can choose the transport stream to generate tables for. The transport stream configuration defines what table types to generate. The default is that all tables are generated. The "Compiled Tables" dialog is then opened. On the "Settings" tab of this dialog the user can choose whether all old static tables should be deleted. The user can also set the playout configuration of the generated tables to "Playout

Static". Tables already in this mode are greyed out. This is the same configuration as on the [Section 8.6.2.7.1](#) page.

The other tabs in this dialog show the table sections that have been generated.

To store the generated table sections as static tables, click the "Apply Tables" button. The table sections will then be played out if the tables have been configured to "Playout Static". The version number of the table sections will be updated automatically.

8.6.2.7.7 PSI/SI Editor

This page is not available when the output is in ATSC mode.

The PSI/SI editor allows the user to add, remove or edit networks, transport streams, services, components and descriptors as he sees fit.

Networks

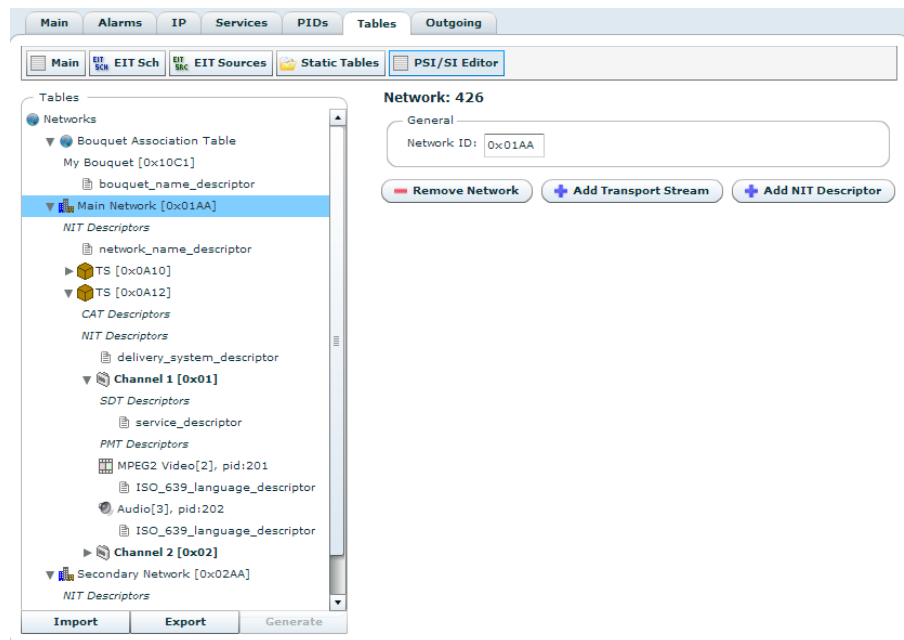


Figure 8.93 PSI/SI editor, Network item selected.

The first item in the tree is the networks node. By selecting this item or right-clicking it the user can add a new network to the system.

Selecting a network brings up a page to the right as shown in [Figure 8.93](#). Here the user can change the network ID. The user can also remove the network, add a transport stream to the network or add a NIT descriptor to the network.

The mandatory "network_name_descriptor" is added automatically and allows the user to set the name of the network.

Transport Streams

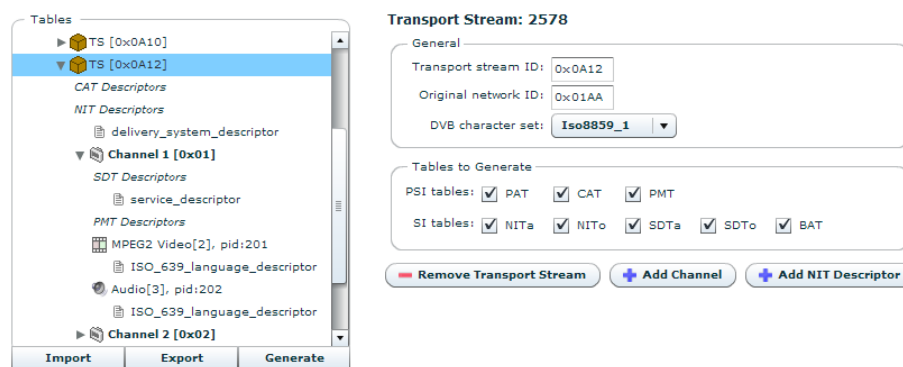


Figure 8.94 Transport Stream

Each network can have any number of transport streams belonging to it. By selecting a network or right-clicking it the user can add a new transport stream to the network.

New transport streams have the mandatory NIT descriptor "delivery_system_descriptor" added by default.

Selecting a transport stream brings up a page to the right as shown in [Figure 8.94](#).

Transport stream ID

This is a field which serves as a label to identify this Transport Stream from any other multiplex within a network. The default value is 0.

Original network ID

This field gives the label identifying the network_id of the originating delivery system. The default value is 0.

DVB character set

The character set to use for all strings belonging to this transport stream. The default value is Iso8859_1.

Tables to generate

When generating table sections for this transport stream, the selected table types will be generated. By default all the tables are selected.

Remove transport stream

Clicking this button will remove this transport stream from the network.

Add channel

By clicking this button a new channel will be added to this transport stream and then it will be selected in the tree.

Add NIT descriptor

Opens the "Add Descriptor" dialog to add a NIT descriptor to this transport stream. The "delivery_system_descriptor" is added automatically when the transport stream is created.

Add CAT descriptor

Opens the "Add Descriptor" dialog to add a CAT descriptor to this transport stream.

Channels

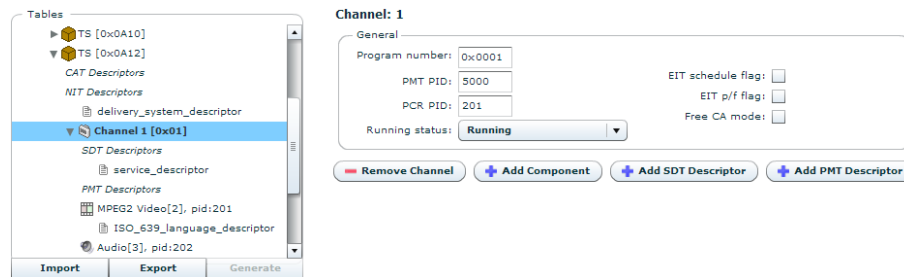


Figure 8.95 Channel

Each transport stream can have any number of channels belonging to it. By selecting a transport stream or right-clicking it the user can add a channel to the transport stream.

New channels have the mandatory SDT descriptor "service_descriptor" added by default.

Selecting a channel brings up a page to the right as shown in [Figure 8.95](#).

Program number

Program number identifies the channel within the transport stream. This field shall not take any single value more than once within one transport stream. The minimum and default value of this field is 1.

PMT PID

PMT PID specifies the PID of the Transport Stream packets which shall contain the PMT section applicable for this channel. The minimum and default value of this field is 32.

PCR PID

PCR PID indicates the PID of the Transport Stream packets which shall contain the PCR fields valid for this channel. If no PCR is associated with a channel for private streams, then this field shall take the value of 8191. This default value of this field is 8191.

Running status

This sets the current status of the service.

EIT schedule flag

If selected this field indicates that EIT schedule information for the channel is present in the current Transport stream.

EIT p/f flag

If selected this field indicates that EIT present following information for the service is present in the current TS.

Free CA mode

If this field is selected it indicates that access to one or more component streams in the channel may be controlled by a CA system.

Remove channel

Clicking this button will remove this channel from the transport stream.

Add component

By clicking this button a new component will be added to this channel and then it will be selected in the tree.

Add SDT descriptor

Opens the "Add Descriptor" dialog to add an SDT descriptor to this channel. The "service_descriptor" is added automatically when the channel is created.

Add PMT descriptor

Opens the "Add Descriptor" dialog to add an PMT descriptor to this channel.

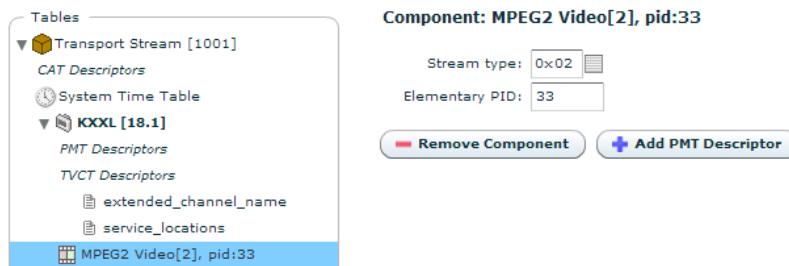
Components

Figure 8.96 Component

Each channel can have any number of components belonging to it. By selecting a channel or right-clicking it the user can add a component to the channel.

Selecting a component brings up a page to the right as shown in [Figure 8.96](#).

Stream type

This field specifies the type of program element carried within the packets with the PID whose value is specified by the Elementary PID. By clicking the icon to the right the user can select from a list of possible stream types.

Elementary PID

This field specifies the PID of the Transport Stream packets which carry this program element.

Remove component

Clicking this button will remove this component from the channel.

Add PMT descriptor

Opens the "Add Descriptor" dialog to add an PMT descriptor to this component.

Bouquets

By selecting the "Bouquet Association Table" item or right-clicking it the user can add a Bouquet to the system. A bouquet is a collection of channels, which may traverse the boundary of a network.

New bouquets have the mandatory BAT descriptor "bouquet_name_descriptor" added by default.

Selecting a bouquet brings up a page to the right as shown in [Figure 8.97](#).

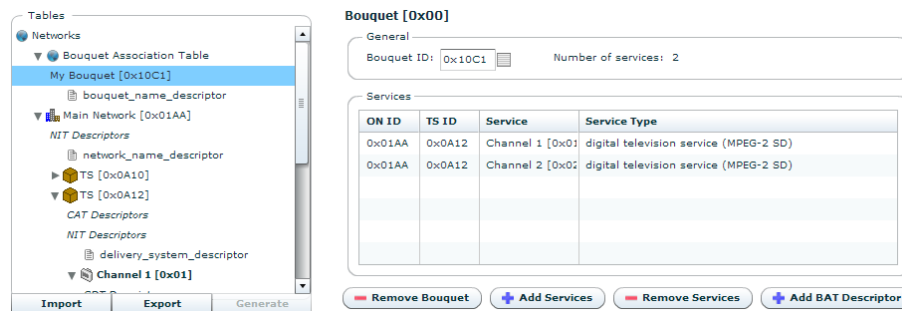


Figure 8.97 Bouquet

Bouquet ID

This field serves as a label to identify the bouquet. By clicking the icon to the right the user can select an ID from a list of possible values.

Services

This table lists the channels that are currently added to the Bouquet. It lists the Original Network ID, the Transport Stream ID, the channel name, the channel ID and the service type of the channels.

Remove bouquet

Clicking this button will remove this bouquet from the system.

Add service

Clicking this button allows the user to add one or more services to the bouquet from a list of available services.

Remove service

Removes selected channels from the bouquet.

Add BAT descriptor

Opens the "Add Descriptor" dialog to add an BAT descriptor to this bouquet. The "bouquet_name_descriptor" is added automatically when the bouquet is created.

Add Descriptor Dialog

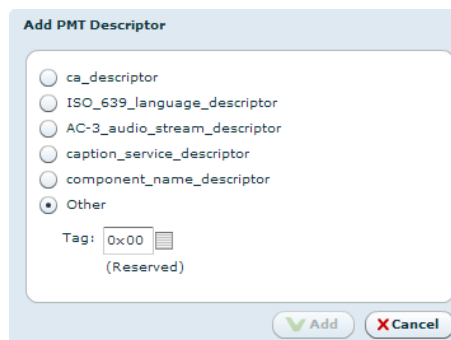


Figure 8.98 Add Descriptor Dialog

By choosing to add any type of descriptor the Add Descriptor Dialog is shown **Figure 8.98**. The dialog always gives the option to add a generic descriptor by selecting the "Other" radio button. The user can then set the descriptor tag manually or select from a list of descriptors by clicking the icon.

Some elements have predefined descriptors with custom configuration pages. These descriptors get separate radio buttons.

By clicking the add button the descriptor is added and selected in the tree. The predefined descriptors have custom configuration pages which should be self explanatory.

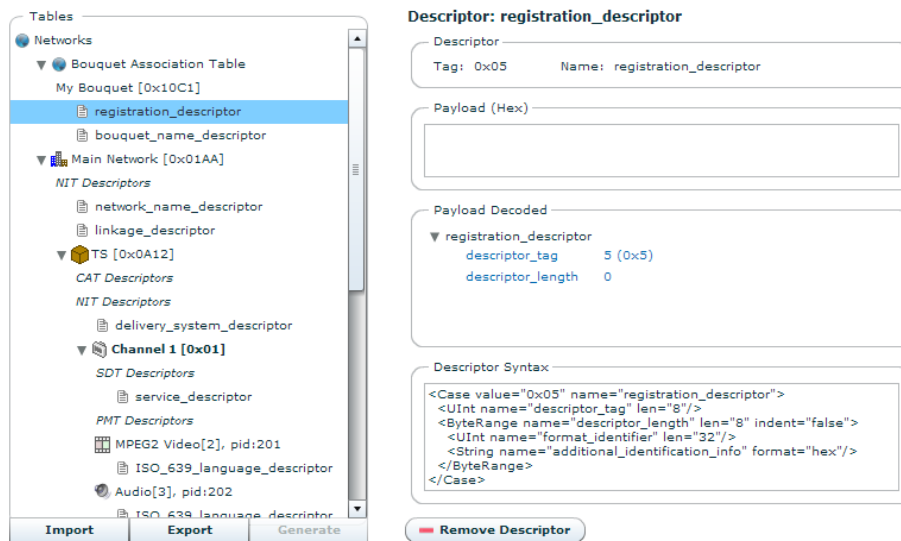


Figure 8.99 Generic Descriptor

The generic descriptor page as shown in **Figure 8.99** is build up of the following elements:

Descriptor

This box shows the descriptor tag and the descriptor name. They are not editable. To change the descriptor tag, remove the descriptor and add a new one.

Payload

This box allows the user to enter the payload of the descriptor manually as a hex string. The entered data is continuously decoded in the "Payload Decoded" box.

Payload decoded

This box shows the decoded descriptor using the currently entered payload. It will show an error if the payload is not legal.

Descriptor syntax

This box shows an xml describing the syntax of the descriptor. The structure of this xml is beyond the scope of this manual.

Remove descriptor

Clicking this button will remove the descriptor.

8.6.2.7.8 PSIP Editor

This page is only available when the output is in ATSC mode.

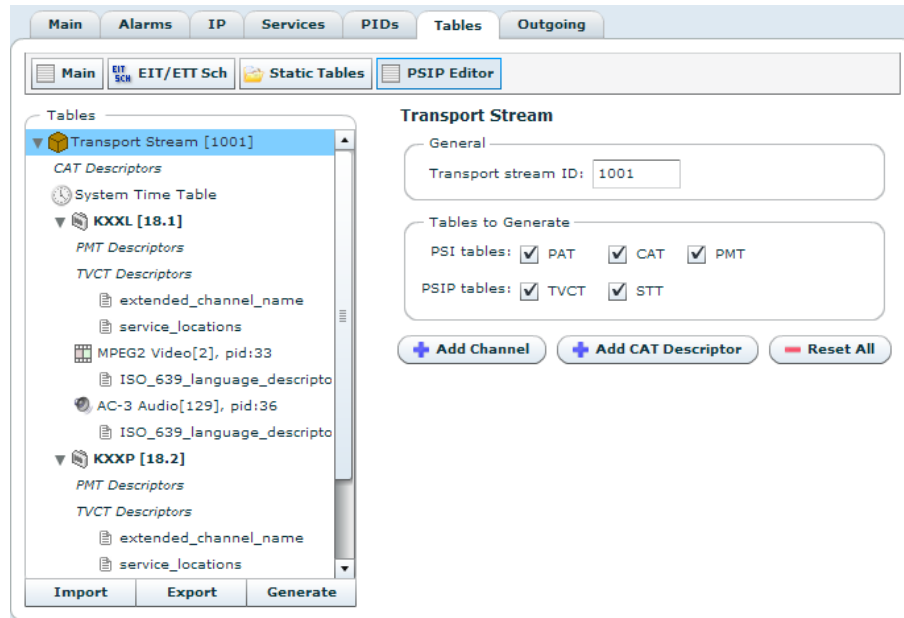


Figure 8.100 PSIP Editor, Transport Stream selected

The PSIP editor allows the user to add, remove or edit channels, components and descriptors as he sees fit.

Transport Stream

The first item in the tree is the transport stream node. By selecting this item or right-clicking it the user can add a new channel to the transport stream.

Selecting a transport stream brings up a page to the right as shown in [Figure 8.100](#).

Transport stream ID

This field serves as a label to identify this Transport Stream from any other multiplex. The default value is 0.

Tables to generate

When generating table sections for this transport stream, the selected table types will be generated. By default all the tables are selected.

Add channel

By clicking this button a new channel will be added to this transport stream and then it will be selected in the tree.

Add CAT descriptor

Opens the "Add Descriptor" dialog to add a CAT descriptor to this transport stream.

Reset All

Clicking this button will reset the PSIP editor configuration. This set all fields to their default values and remove all descriptors and channels.

System Time Table

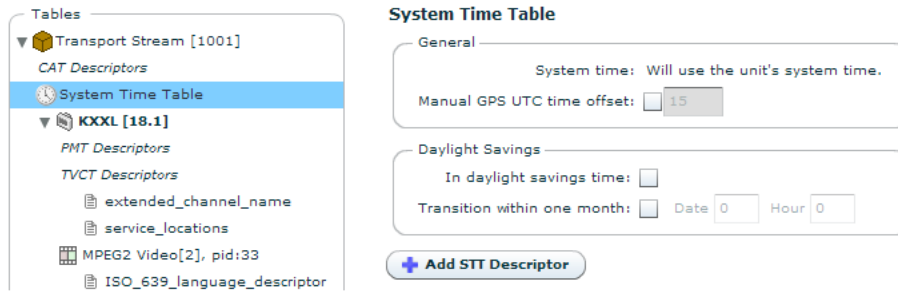


Figure 8.101 System Time Table

Selecting the "System Time Table" item in the tree brings up a page to the right as shown in **Figure 8.101**.

System time

The system time field in the STT will be set automatically by the unit to the current unit time.

Manual GPS UTC time offset

By selecting this the user can enter the offset between UTC and GPS time manually. This value should be equal to the number of leap seconds since the start of GPS time, 00:00 6th of January 1980. If the user does not tick the box, the unit will set the offset to the correct value based on the leap seconds added when the unit software was built. This field should only be overridden if there has been leap seconds since the software was built.

In daylight savings time

If this box is ticked it indicates that daylight savings time is currently in effect.

Transition within one month

If selected this indicates that the transition to or from daylight savings time is within one month. If selected, the date and hour of the transition should also be entered.

Add STT descriptor

Opens the "Add Descriptor" dialog to add an STT descriptor to the STT.

Channels

The transport stream can have any number of channels belonging to it. By selecting the transport stream or right-clicking it the user can add a channel to the transport stream.

New channels have the mandatory TVCT descriptor "service_locations" added by default. A video component and an audio component are also added to the channel by default.

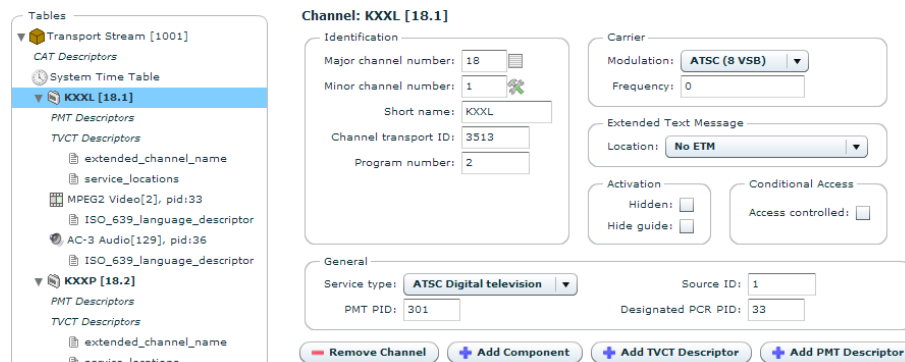


Figure 8.102 Channel

Selecting a channel brings up a page to the right as shown in [Figure 8.102](#).

Major channel number

A number that represents the "major" channel number associated with this channel. Each channel shall be associated with a major and a minor channel number. The major channel number, along with the minor channel number, act as the user's reference number for the channel. The major channel number shall be between 1 and 99. The value of major channel number shall be set such that in no case is a major channel number/ minor channel number pair duplicated.

Minor channel number

A number in the range 0 to 999 that represents the "minor" or "sub"- channel number. This field, together with major channel number, performs as a two-part channel number, where minor channel number represents the second or right-hand part of the number. Services whose service_type is ATSC digital television or ATSC audio only shall use minor numbers between 1 and 99. For other types of services, such as data broadcasting, valid minor channel numbers are between 1 and 999.

Short name

The name of the virtual channel, max seven characters.

Channel transport ID

A field that represents the MPEG-2 Transport Stream ID associated with the Transport Stream carrying the MPEG-2 program referenced by this channel. For inactive channels, channel transport ID shall represent the ID of the Transport Stream that will carry the service when it becomes active. The receiver is expected to use the channel transport ID to verify that any received Transport Stream is actually the desired multiplex. For analog channels (service_type 0x01), channel transport ID shall indicate the value of the analog TSID included in the VBI of the NTSC signal.

Program number

A number that associates this channel with the MPEG-2 PROGRAM ASSOCIATION and TS PROGRAM MAP tables. For analog services and inactive channels this field is set automatically. This number shall not be interpreted as pointing to a Program Map Table entry.

Service type

This field identifies the type of channel this is. The default value is ATSC Digital Television.

PMT PID

PMT PID specifies the PID of the Transport Stream packets which shall contain the PMT section applicable for this channel. The minimum and default value of this field is 16.

Source ID

A number that identifies the programming source associated with this channel. In this context, a source is one specific source of video, text, data, or audio programming. Source ID value zero is reserved. Source ID values in the range 0x0001 to 0x0FFF shall be unique within the Transport Stream, while values 0x1000 to 0xFFFF shall be unique at the regional level and administered by a Registration Authority designated by the ATSC.

Designated PCR PID

This field is written to the mandatory "service_locations" descriptor. It can be edited both here and directory on the descriptor page.

Modulation

A number that indicates the modulation mode for the transmitted carrier associated with this channel. This field is disregarded for inactive channels.

Frequency

The recommended value for this field is 0. Use of this field to identify carrier frequency is allowed, but is deprecated.

Location

This field specifies the existence and the location of an Extended Text Message (ETM).

Hidden

When selected, this indicates that the channel is not accessed by the user by direct entry of the channel number. Hidden channels are skipped when the user is channel surfing, and appear as if undefined, if accessed by direct channel entry. Typical applications for hidden channels are test signals and NVD services. Whether a hidden channel and its events may appear in EPG displays depends on the hide guide field.

Hide guide

Indicates, if not selected for a hidden channel, that the channel and its events may appear in EPG displays. This field shall be ignored for channels which do not have the hidden bit set, so that non-hidden channels and their events may always be included in EPG displays regardless of this field. Typical applications for hidden channels with this value selected are test signals and services accessible through application-level pointers.

Access controlled

Indicates, when selected, that the events associated with this channel may be access controlled.

Remove channel

Clicking this button will remove this channel from the transport stream.

Add component

By clicking this button a new component will be added to this channel and then it will be selected in the tree.

Add TVCT descriptor

Opens the "Add Descriptor" dialog to add an TVCT descriptor to this channel. The "service_locations" is added automatically when the channel is created.

Add PMT descriptor

Opens the "Add Descriptor" dialog to add an PMT descriptor to this channel.

Components

Works in the same way as for the PSI/SI editor, see [Section 8.6.2.7.7](#).

Add Descriptor Dialog

Works in the same way as for the PSI/SI editor, see [Section 8.6.2.7.7](#).

8.6.2.8 Pri Queue

This page is used to manage the output priority queue described in [Section 5.8.4](#) The priority queue configuration affects the sequence in which packets are transmitted on the output, and which packets that are dropped first in case of an output overflow.



Id	Queue	Rate [Mbit/s]	Shaping [Kbit/s]	Max Burst	Fill	Pkt Cnt	Lost
82	MIP	6.694	-	-		9910	-
81	Forced stuffing	7.059	-	-	Disabled	12089	-
64	PAT,CAT,PMT,TDT	0.000	213000	15	<input type="text" value="5"/>	5 111134	-
1	Audio/Video/Data 1	11.756	213000	15	<input type="text" value="5"/>	8503	57
65	NIT,SDT	0.100	213000	15	<input type="text" value="5"/>	5 111134	-
67	Data/EMM	0.300	213000	15	<input type="text" value="32"/>	32 111134	-
66	EIT	0.200	213000	15	<input type="text" value="32"/>	32 111134	-
80	Stuffing	17.613	-	-		5046	-

SI total rate: 0.400 Mbit/s (Min: 0.030 Mbit/s , Max: 1.000 Mbit/s)
 SI total packet count: 133455555

Figure 8.103 Basic output priority queue - default config.

The priority queue is presented in a data grid with the highest prioritised queue at the top, lowest priority at the bottom.

Figure [8.103](#) shows this view for the basic priority queue variant with default configuration.



Note: Remark that the PSI player queue (ID 64) is placed at higher priority than the Audio/Video queue to assure that PSI tables is delivered even on an overload.

The grid has these columns

Id

Queue identifier. This number is used to identify the queue in the user interface. The output PID list refers to this number.

Queue

Name of the queue.

Group C queues (see definition in table 5.4) can be assigned a name by the user for later reference where PIDs/Services are assigned to a queue.

Rate

The average output bitrate measured on the queue. Minimum and maximum values measured are shown on tool-tip. For groups, the average rate of all queues in the group is shown in the grid, while the individual queue rates are shown on the tool tip.

Shaping

Bandwidth limit for a queue (or group of queues) specified in kbit/s. “Shaping” plus “Max Burst” sets the constraints on packet transmission from a queue. A value of 213000kbit/s completely disables the shaper. Please see [Section 5.8.5](#) for a description of the bitrate shaping algorithm.

Max burst

Max number of packets allowed back-to-back on the ASI output bitrate. (see [Section 5.8.5](#)).

Fill

Graphical indicator of the buffer filling for the category D queues. Shows average, min and max fill since last reset of statistics. The number to the right of the diagram shows the max number of packets that can be buffered in this queue.

This column also shows status info for the forced stuffing packet source.

Pkt Cnt

Number packets transmitted on this queue.

Lost

Number of overflows detected on a queue. This number is not the same as the number of TS packets lost on the queue.

Min/max rates and packet counters are cleared by pressing the “Reset Statistics” button.

To edit writable fields in the grid, click the grid cell, type the new value and press enter. Edited fields are shown in yellow. Press the apply button to commit any changes.

To change the priority of a queue select the queue and use the up and down arrow button to the left of the grid to move the queue row up or down in the table. Changes are indicated in yellow. Press apply to commit all changes or refresh to cancel.

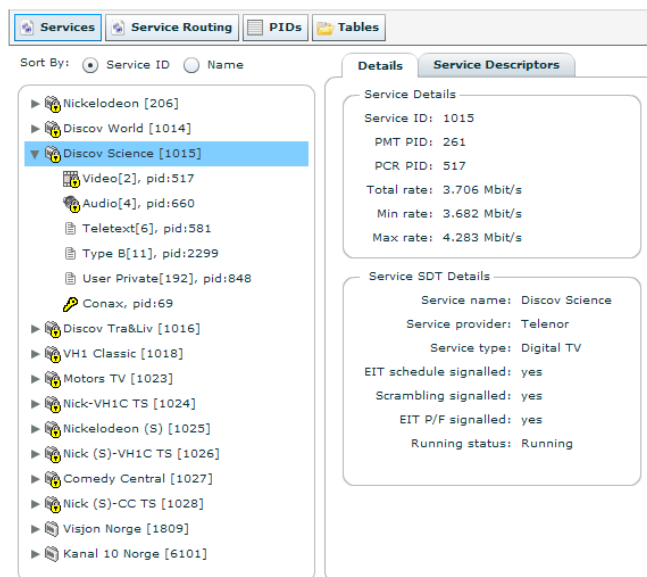
8.6.2.9 Outgoing

The Outgoing page shows PIDs and services that are currently being transmitted on the output. It has four sub-pages:

- Services
- Service Routing
- PIDs
- Tables

8.6.2.9.1 Services

This page shows the service composition of the output, [Figure 8.104](#). Refer to [Section 8.5.2.4](#) for a description of the page contents, since it is similar to the user interface description of each input.



The screenshot shows the 'Services' page with a tree view on the left and a details panel on the right. The tree view lists various services, with 'Discov Science [1015]' selected. The details panel shows the following information:

Service Details	
Service ID:	1015
PMT PID:	261
PCR PID:	517
Total rate:	3.706 Mbit/s
Min rate:	3.682 Mbit/s
Max rate:	4.283 Mbit/s

Service SDT Details	
Service name:	Discov Science
Service provider:	Telenor
Service type:	Digital TV
EIT schedule signalled:	yes
Scrambling signalled:	yes
EIT P/F signalled:	yes
Running status:	Running

Figure 8.104 Outgoing Services



Note: If PAT and/or PMT are forwarded to the output by PID routing, the content displayed on the page may not be displayed correctly.

8.6.2.9.2 Service Routing

Input Port	Input Service ID	Input Service Name	Output Service ID	Output Service Name
Switch 1	202	CNN International	202	CNN International

Figure 8.105 Outgoing Services Routing

The page has a table showing the services that are currently being transmitted on the output, with reference to the input port of the service. The table has the following columns:

Input port

The input port of the service.

Input Service ID

The Service ID (program number) of the service on the input port.

Input Service Name

The name of the service as described in the "Service Description Table" (DVB-SDT) or "Virtual Channel Table" (ATSC-VCT).

Output Service ID

The Service ID of the output service.

Output Service Name

Name on the service of the output, as described in SDTa or VCT.

8.6.2.9.3 PIDs

Info	PID	Bitrate	Min Rate	Max Rate	CC Err Cnt	Priority	Pri Queue	Count
	0	0.014 Mbit/s	0.014 Mbit/s	0.029 Mbit/s	0	2	64	12385
	1	0.002 Mbit/s	0.002 Mbit/s	0.011 Mbit/s	0	2	64	2479
	17	0.000 Mbit/s	0.000 Mbit/s	0.017 Mbit/s	0	18	65	2388
	18	0.194 Mbit/s	0.000 Mbit/s	0.738 Mbit/s	2	19	66	114162
	20	0.000 Mbit/s	0.000 Mbit/s	0.005 Mbit/s	0	3	1	166
	48	0.371 Mbit/s	0.000 Mbit/s	0.642 Mbit/s	0	3	1	247368
	68	0.014 Mbit/s	0.011 Mbit/s	0.026 Mbit/s	0	6	4	12378
	69	0.014 Mbit/s	0.011 Mbit/s	0.023 Mbit/s	0	6	4	12381
	70	0.014 Mbit/s	0.011 Mbit/s	0.026 Mbit/s	0	6	4	12383
	100	0.011 Mbit/s	0.011 Mbit/s	0.023 Mbit/s	0	2	64	12378
	110	7.675 Mbit/s	3.019 Mbit/s	7.687 Mbit/s	225	9	7	4739013
	120	0.269 Mbit/s	0.000 Mbit/s	0.308 Mbit/s	88	10	8	216620
	121	0.134 Mbit/s	0.000 Mbit/s	0.155 Mbit/s	40	10	8	109518
	125	0.460 Mbit/s	0.000 Mbit/s	0.463 Mbit/s	116	11	9	365279
	130	0.263 Mbit/s	0.000 Mbit/s	0.268 Mbit/s	106	11	9	208728
	131	0.005 Mbit/s	0.000 Mbit/s	0.005 Mbit/s	0	11	9	3741
	192	0.005 Mbit/s	0.002 Mbit/s	0.008 Mbit/s	0	3	1	3872

Figure 8.106 Outgoing PIDs List

The Outgoing PIDs page shows a table of all PIDs that are currently being transmitted on the output. The table has the following columns:

Info

This column shows the same icons as in figure 8.58, explained in Section 8.5.2.5, except that the PCR detection is not available on the output.

PID

The Packet Id.

Type

The PID type. Unsignalled PIDs do not have a type.

Bitrate

The current bitrate of the PID in Mbit/s.

Min Rate/Max rate

The minimum and maximum recorded rates of the PID since the last rate reset, in Mbit/s.

CCErr Cnt

This counter shows the number of CC errors on this PID since the last CC error count reset.

Pri

The priority of the PID.

Priority Queue

The transmission queue number of this PID. This number is the same as the Id column in the priority queue data grid. The tool-tip for this column shows the queue name for the given queue number.

Ref. by service

A comma separated list of services referencing the PID. If there are too many services to show in the cell, a tool tip showing all the services will appear when holding the mouse over the cell.

ECM PID(s)

A comma separated list of ECM PIDs containing PID descrambling information.

Count

Gives a count of the number of TS packets sent for this PID.

Input Port

Reference to the input port this PID is routed from. If internally generated, thus played out by the PSI/SI/PSIP player, the column shows a dash.

Input PID

The original PID value on the input port.

Beneath the table are three buttons. The Reset CC error counts button resets the CC error counters of all PIDs. The Reset min/max rates button resets the measured minimum and

maximum rates of all PIDs. The Reset packet counts button resets the packet counters of all PIDs.

8.6.2.9.4 Tables

This page shows the content of the PSI/SI/PSIP playout database [Figure 8.107](#).

Table [pid]	TID	Primary	Secondary	Tertiary	Ver	Age
PAT [0]	0	10	-	-	22	0d, 00h:22m:38s
CAT [1]	1	-	-	-	15	0d, 00h:22m:38s
PMT [256]	2	206	-	-	4	0d, 00h:22m:38s
PMT [259]	2	1013	-	-	5	0d, 00h:22m:38s
PMT [260]	2	1014	-	-	4	0d, 00h:22m:38s
PMT [261]	2	1015	-	-	6	0d, 00h:22m:38s
PMT [268]	2	1016	-	-	4	0d, 00h:22m:38s
PMT [262]	2	1018	-	-	3	0d, 00h:22m:38s
PMT [297]	2	1021	-	-	2	0d, 00h:22m:38s
PMT [299]	2	1022	-	-	1	0d, 00h:22m:38s
PMT [292]	2	1023	-	-	4	0d, 00h:22m:38s
PMT [258]	2	1024	-	-	5	0d, 00h:22m:38s
PMT [263]	2	1025	-	-	9	0d, 00h:22m:38s

Figure 8.107 Outgoing tables list

PSI/SI/PSIP tables that are not handled in a "Playout" mode will not appear here. Please refer to [Section 8.5.2.7](#) for a detailed description of the page.

8.6.3 Output copies

Clicking on one of the ASI or ASI/310M entries (according to set-up) in the Outputs tab navigator opens a page that provides a quick way to re-allocate this output to be used as an input, [Figure 8.108](#). If the button is disabled, it means your are not allowed to switch direction on this port.



Figure 8.108 Re-allocate output

Click the Change to ASI input button and confirm with Apply.

Clicking on one of the IP interface entries opens the page that allows setting all relevant parameters for that IP output.

8.6.4 TS-OUT -> IP Destination

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

8.6.4.1 Main

This page is shown in [Figure 8.109](#).

Figure 8.109 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 5.5.2](#) 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.

TS packets per frame

Enter the number of 188 byte MPEG-2 transport stream packets to map into each UDP frame. Valid values are between 1 and 7. Normally 7 is the best choice to reduce overhead and Ethernet frame rate. For very low bitrate streams, less than 7 packets per frame may be used to advantage reducing the delay through the unit.

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.

8.6.4.2 FEC

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

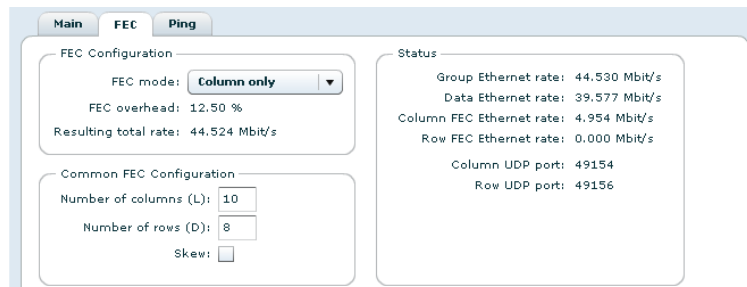


Figure 8.110 IP output FEC page

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.

8.6.4.3 Ping

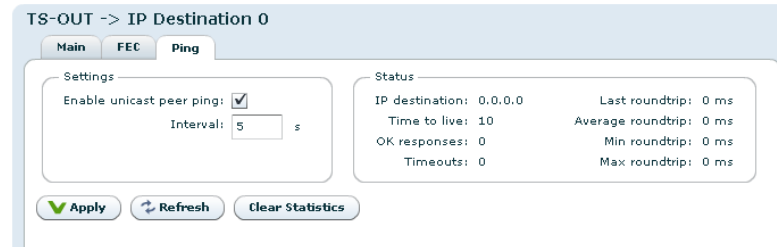


Figure 8.111 Ping page

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 ping 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.

8.7 Redundancy

8.7.1 Redundancy Controller

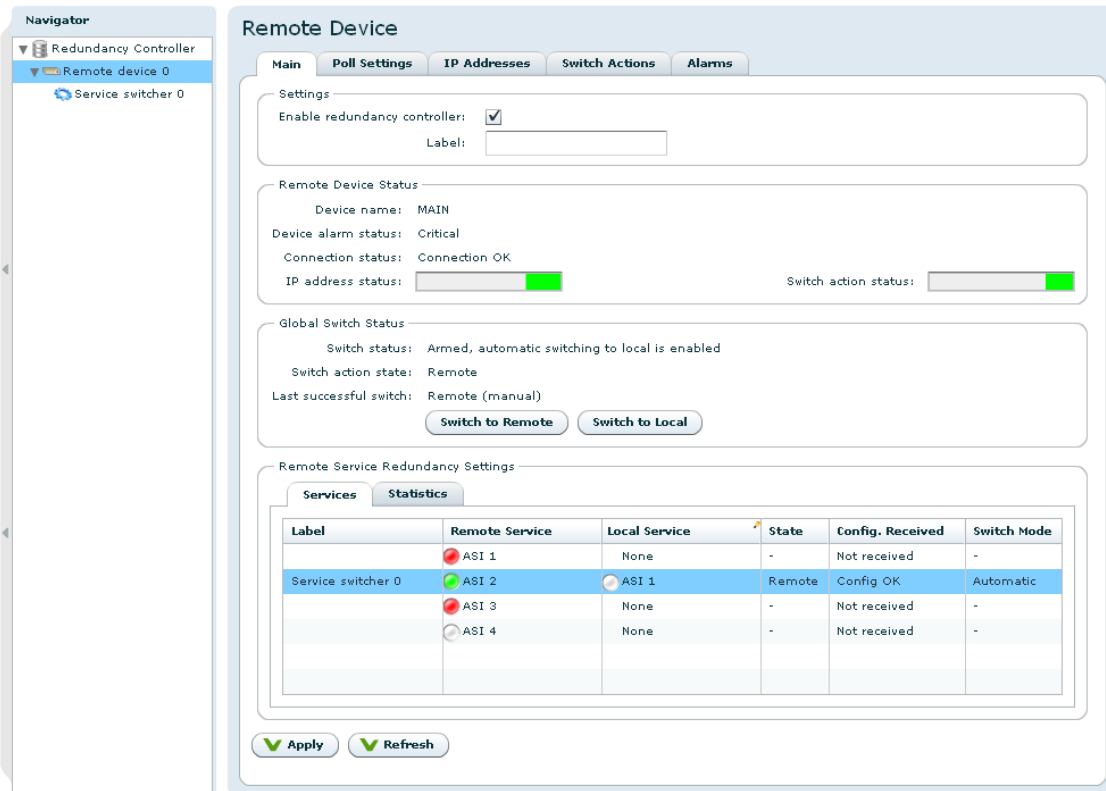


Figure 8.112 The user interface

Figure 8.112 shows the user interface. The page is divided into four sections: Settings, Remote Device Status, Global Switch Status and Remote Service Redundancy Settings.

Settings

allows the user to label this specific redundancy controller and also to enable or disable it.

Remote Device Status

shows the remote device name and alarm status. It also shows the status of the connection to the remote device. Additionally two status bars show the status of the last poll towards each configured IP Address and Switch action. The status bar is divided into a number of parts according to the number of IP addresses or Switch actions. For instance if three IP addresses are configured and their status is no contact, disabled and contact ok, then the bar is divided into three equally sized parts with the colours red, gray and green.

Global Switch Status

shows the status of the global redundancy controller. The information shown in this

section changes when a global switch is performed, either by an automatic switch to local or a manual switch. The Switch Action State attribute reflects the combined state of the configured switch actions. If all switch actions are configured to remote value the Switch Action State is Remote. If all switch actions are configured to local value the Switch Action State is Local. Otherwise the Switch Action State is Unknown.

Remote Service Redundancy Settings

This section shows a table of the remote and local services. For each remote service the user can configure a local replacement by using the select box on each row in the Local service column. When a local replacement is configured a service switcher is added to the redundancy controller. The service switcher parameters state, Configuration received and mode is shown in the table. Refer to [Section 8.7.2](#) for detailed information on service switchers.

8.7.1.1 Global redundancy controller switching

A global switch can be performed either manually or automatically. Figures [8.113](#) and [8.114](#) show redundancy controller state diagrams when switching to local or remote services respectively.

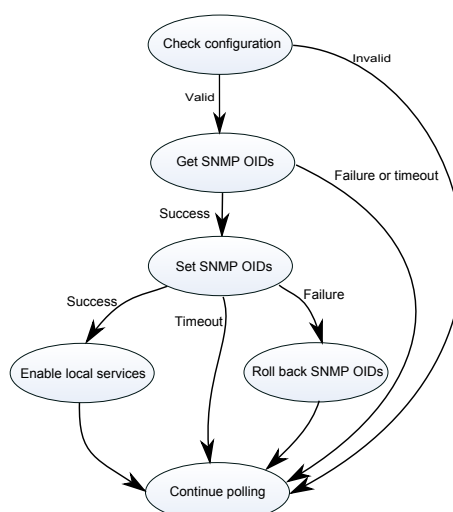


Figure 8.113 The actions performed when the redundancy controller loses contact with the remote device.

8.7.1.2 Poll settings

The remote device is polled through a set of IP addresses. Loss of contact towards any of these addresses causes an alarm.

During normal operation the redundancy controller alternates between two states, poll and sleep. When entering the poll state a series of polls are made towards the configured IP addresses and SNMP OIDs. When all poll responses are received the redundancy controller

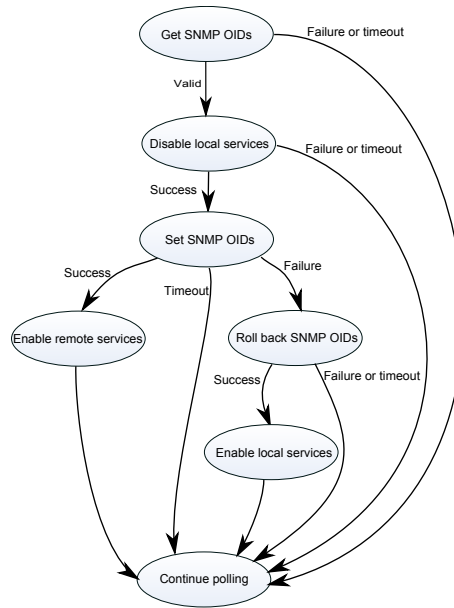


Figure 8.114 The actions performed when a manual redundancy controller switch to remote services is forced.

switches to sleep state. If not all responses are received before the poll state timeout the remaining IP addresses and OIDs will be flagged as no contact before switching to sleep. The redundancy controller will wait a number of seconds in sleep before doing a new poll. The sleep state timeout is configurable for both link up (contact with remote) and link down (no contact with remote) scenarios.

If an authorization error towards any address occurs the redundancy controller cannot resolve the state of the remote device. In this case the redundancy controller assumes the remote device is healthy and will not switch to local.

All IP addresses should be to the same device, otherwise a configuration alarm will be raised.

If no contact can be made to any of the IP addresses configured for a device, each service switcher will be informed that the remote device is down. In addition, a set of SNMP actions will be performed.

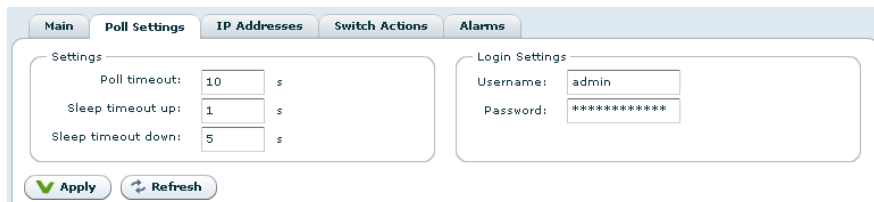


Figure 8.115 The poll settings page

Figure 8.115 shows the poll settings of the redundancy controller. The timeouts used in the sleep and poll states are configured here. The username and password to use when logging in on the remote device is also configurable.

8.7.1.3 Remote device IP addresses

Enable	IP Address	Timeout [s]	Polls OK	Polls Failed	RTT [s]	Max RTT [s]	Status	Device
<input checked="" type="checkbox"/>	10.105.99.101	8	3045	6	0.060...	2.33	Contact ok	20

Figure 8.116 The IP Addresses to the remote (main) device

Figure 8.116 shows the IP address configuration. Basic poll statistics are provided to measure the round trip time between the remote and local unit. Both the maximum and the current round trip time (RTT) is measured. The maximum RTT can be cleared by clicking on the “Reset polling stats” button. The individual poll timeout per address should not be higher than the poll state timeout **and** not be lower than the maximum measured round trip time.

8.7.1.4 SNMP switch actions

#	Enabled	IP Address	Poll OID	Read Value	State	RTT [s]	Max RTT [s]	Polls OK	Polls Failed	Status
0	no	0.0.0.0	1.3.6.1		Unknown	0		0	0	

SNMP Action #0

Switch Action Settings

Enable:

IP address: 0.0.0.0

UDP port: 161

Value to set when switching to remote:

Value to set when switching to local:

OID type: Integer32

Set OID: 1.3.6.1

Poll mode: GET

Other read OID: 1.3.6.1

Read community string: public

Write community string: private

Figure 8.117 The SNMP switch actions

Figure 8.117 shows the SNMP switch action configuration. Note that these OIDs are only set after a loss of contact with the remote device or when manually switching the entire redundancy controller between remote and local services, i.e. during a global switch. The OIDs are not set when switching a single service switcher between remote and local.

Basic poll statistics are provided to measure the round trip time between the remote and local unit. Both the maximum and the current round trip time (RTT) is measured. The maximum RTT can be cleared by clicking on the “Reset polling stats” button.

The SNMP OIDs are polled during normal operation to discover potential problems as soon as possible. Three modes are available for this poll: set oid, get oid or get other oid request.

The set oid sets the oid to remote value if the link to the remote device is up and local value if the link is down. The get oid mode just reads the oid. The get other oid reads the Other read OID.

8.7.2 Service switchers

A service switcher is assigned to each pair of remote and local services. As long as the Redundancy Controller has contact with the remote device, the service switcher will acquire the current status and configuration.

The service switcher does not perform a switchover unless it has received a valid configuration.

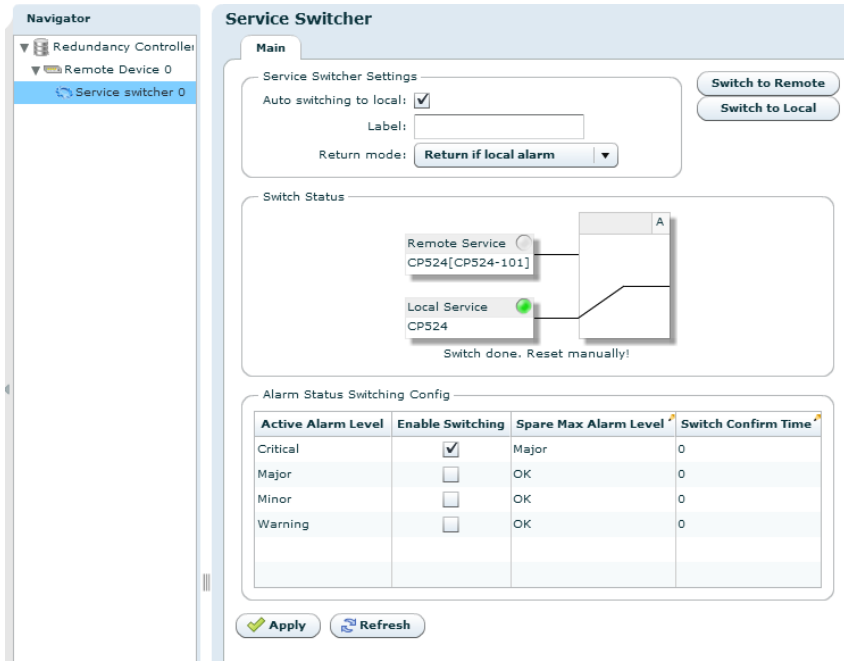


Figure 8.118 The service switcher configuration page

The service switcher page shows the current state of this service pair. The label and the alarm status is shown in the graphical representation in addition to the current switch state.

The service switcher controller only relates to alarm levels for the two corresponding services. It is up to the user to configure appropriate alarm levels for each of the alarms a service is able to generate. The switching criteria are configured as follows:

For each alarm level (starting with the highest, most severe level), the following configuration is done:

- Enable/disable switching for this level
- Required alarm level of the other (spare) input to allow switching
- The confirm time for this level (how long to wait before doing a switch)

The required level of the other input needs to be lower than the configured level, e.g. when configuring the switch criteria for “Critical (6)” main level, the spare input must be on level “Major (5)” or lower.

Example: A very simple configuration may be to *only* switch on “Critical (6)” level and require “OK (1)” level on the spare input.

In “auto” state, the switch controller is “armed” and continuously listens to change in the alarm status for each service. For each change event, the controller evaluates the levels and checks if the switching criteria is met. If the answer is “yes”, the controller jumps to a `wait_confirm` state to actually confirm that the switch criteria still is met after the configured time. If the criteria is still met, the controller performs a switch. If the criteria is no longer met, the controller does no switching and jumps back to the auto state.

The Embedded Redundancy Controller also offers automatic switch back to remote. After a switch to the local unit has been performed, the local unit continue to poll the remote device. When the remote device has recovered it is possible to perform an automatic switch back. The automatic switch back scheme is seperated into three different options, “Return if OK”, “Return if local alarm”, “No return”.

Return if OK

This option will return automatically to the remote device, when the remote device has recovered and is OK.

Return if local alarm

This option will return automatically to the remote device if the remote device has recovered **and** the local unit is in an erroneous state.

No return

The no return option will disable automatically switch back. However, it is still possible to do a manually switch back to remote.

9 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.

9.1 SNMP agent characteristics

The SNMP agent supports the SNMPv2c (Community based SNMPv2) protocol. All custom MIBs are written in SMIV2 format. The SNMP agent 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.

9.2 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.

9.3 MIB overview

This section describes the different MIBs. Detailed description of MIBs is included later on in this document.

9.3.1 Supported standard MIBs

RFC1213-MIB

MIB-II according to RFC1213.

9.3.2 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

9.4 SNMP related configuration settings

The SNMP related configuration parameters are located on the Device Info/SNMP settings page in the GUI.

9.4.1 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.

9.4.2 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.

9.4.3 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 9.5](#).

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.

9.5 Alarm/status related SNMP TRAPs

All TRAP messages are defined in VIGW-UNIT-MIB. This section describes each trap message.

9.5.1 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 9.1](#).

Table 9.1 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> .

9.5.2 Severity indications

All alarm event traps (i.e. all traps defined in [Table 9.1](#) except `unitAlarmStatusChanged`) contain a severity field which is encoded according to the definition below:

Severity	Description
1	Cleared
2	Indeterminate
3	Warning
4	Minor
5	Major
6	Critical

9.5.3 Alarm event fields

A description of the fields in the alarm event traps is presented in [Table 9.2](#). Most of the fields are entries from the `unitEventHistoryTable`. The instance identifier for each variable binding corresponds to the index in this table. This index is of kind `CircularLog` and will wrap around at 2^{32} .

Table 9.2 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.

9.5.4 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.

9.5.5 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 9.3](#).

Table 9.3 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.

10 Examples of Use

10.1 Intro

This chapter offers a small selection of different practical examples of use of the CP524, with corresponding recommended configuration steps, pointing to section in [Chapter 8](#) where the relevant configuration pages are described.

10.2 Installation in a system

When installing the device in a new environment, there are a few parameters that typically need to be configured. These steps are the same for all the cases studied below.

1. Set the IP address as described in [Section 7.3](#)
2. Assign a name for the device. See [Section 8.4.1](#).
3. If you are unsure of the state of the device, set it back to factory default configuration as described in [Section 8.4.8.1](#).
4. Configure a time zone and a source for the real time clock, to assure alarm log entries get correct time stamping. See [Section 8.4.4](#).
5. Enable the input ports to use and disable the ones that will not be used (see [Section 8.5.1](#)).
6. Enable the output and configure the wanted output bitrate. Refer to [Section 8.6.2.1](#).

10.3 Raw PID multiplexing

The most basic way of using the CP524 is to work strictly on a PID stream level, multiplexing streams by manually mapping a number of PIDs through the device.

In this mode you will not depend on the PSI/SI/PSIP signalling on the input signal.

1. For all the inputs in use, disable parsing of all tables, as described in [Section 8.5.2.8](#). Doing this, makes all PIDs to be treated as unsignalled PIDs, since the unit will not know about the PMT on the input.
2. Under Tables on the Outputs tab, configure all PSI/SI/PSIP tables to "Stopped" mode.
3. On the PIDs page ([Section 8.6.2.6](#)) you can now chose the PIDs that shall be transmitted.



Note: If you leave analysis on PAT, PMT and SDT actual in step 1 above, you can see the service relations and type decoding of PIDs and, still do manual PID mappings, but you would have to add the PID mapping with the flag "Transmit always".

10.4 Simple local insertion of a program

This example shows how to set up the following case:

You want to add a locally encoded service to a national multiplex.

1. Put the national feed on port 1.
2. Put the locally encoded feed on port 2.
3. Connect output cable to one of the output ports.
4. On Outputs->Tables configure PAT, CAT, PMT and SDTa to "Payout Regenerated".
5. On the Outputs->Services select "Transmit services by default" from ASI1 to transmit all services from the national feed. See [Section 8.6.2.4](#).
6. On the same page select the local service from ASI2 and click the "Transmit selected service" button to add it to the output.
7. Set up additional SI/PSIP on the Outputs -> Tables page. See [Section 8.6.2.7](#).

NIT

Set NITa/NITo to "Passthrough PID" or "Payout Unchanged" from optional source, or have NIT on the output.

SDT other and BAT

Set SDTo and BAT to "Payout Unchanged" from optional source. Since you're regenerating SDT actual, you cannot choose a passthrough mode on "SDT other" or BAT (same PID).

EITpfa and EITsa

If you have EIT actual on both the national and local feeds, you can set EITpfa and/or EITsa to "Payout Regenerated" to include EIT p/f for the local service. If the local feed doesn't have EIT, you may just as well set EITpfa and EITsa to "Payout Unchanged" or "Passthrough PID" from ASI1.

EITpfo and EITso

Set EITpfo to "Payout Unchanged" from ASI1 to play out the other information from the national feed.

TDT and TOT

Set to "Passthrough PID" from ASI1 to forward TDT and TOT from national feed.

10.5 Sharing of service component

Having the case above, you also need to add signalling of a data component that is signalled on one or more of the national services, to the locally generated channel. This is illustrated in figure [10.1](#).

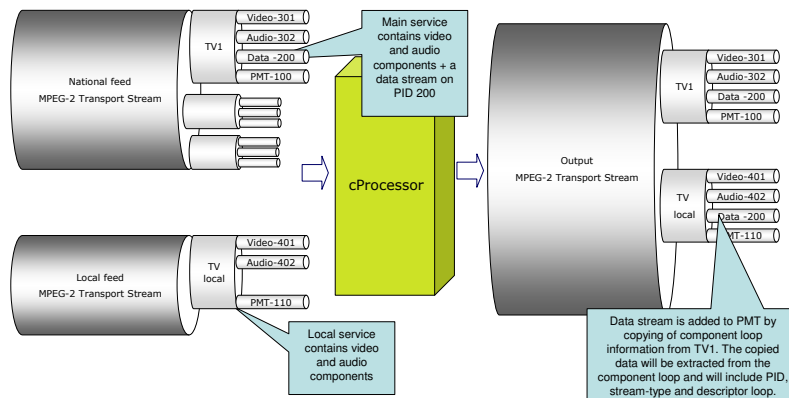


Figure 10.1 “Sharing of component”

1. On the Services tab click edit service on the service on which you want to add the component, i.e the local service.
2. On the components tab (see [Section 8.6.2.5.3](#)) in the service edit dialogue click Add to add a component. In the dialogue that appears select the port of the service that signals the wanted component. Then select the wanted service from the drop-down list and finally the PID in that service in the next drop-down. Apply changes.

10.6 Adding an unsignalled component (Ghost PID)

The CP524 supports insertion of unsignalled PIDs (ghost PIDs) from any input into any service(s). This functionality is often termed Ghost PID insertion. A ghost PID component may be added to several services.

1. Adding the ghost PID is done by editing the outgoing service you want to add the component for. How to edit a service is shown in [Section 8.6.2.4](#).
2. Navigate to the Components tab from the service edit dialogue as shown in [Section 8.6.2.5.3](#).
3. Press Add, which brings up a new dialogue as shown in [Section 8.6.2.5.3](#).
4. Select Custom. This changes the layout to [Figure 10.2](#). In this dialogue you may select previously created components, or you may create new component configurations.
5. Press New to add the new component. This brings up a new dialogue as shown in [Figure 10.3](#).
6. In this view you must select the input port for the unsignalled PIDs. When the input port is selected you may press the icon next to the "Input PID" field to list all unsignalled PIDs of that input. When the PID value is defined you must also specify the type for the component, and also add descriptors for the new component, if desired.
7. Press Apply for all open dialogues. The Components view from [Section 8.6.2.5.3](#) should now show a new component with a + sign next to it. If the new component is present in the configuration, you should be able to see the new component signalled in the PMT for your service by looking at the "Outgoing services" as shown in [Section 8.6.2.9.1](#).

Add Component

From input
 Custom

My Ghost PID ▼ Edit Delete New

Input port: IP 1
 Input PID: 100
 Type: 17
 Scrambling mode: Service default
 Scrambling group: Default
 Scrambling signalling: Service default

Tag	Length	Payload
0x03	1	0x11

Out PID [Global]: 32
 Out PID [Local]: 32
 Priority: Default ▼

Figure 10.2 Custom components

Edit Custom Component

Label: My Ghost PID
 Input port: IP 1
 Input PID: 100
 Type: 17

Scrambling mode: Service default
 Scrambling group: Default
 Signalling: Service default

Tag	Length	Payload
0x03	1	0x11

Figure 10.3 New ghost PID component

11 Preventive Maintenance and Fault-finding

This chapter provides the schedules and instructions, where applicable, for routine inspection, cleaning and maintenance of the CP524, 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 CP524 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 CP524 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 CP524 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 CP524. 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 CP524 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 CP524.
 - Name and address of the owner
 - Model number
 - Serial number
 - Description of service required or failure indication.
2. Package the CP524.
 - 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 SMPTE 310M port

Table B.6 SMPTE 310M Port Specification

Type	SMPTE 310M, Coaxial cable
Connector type	BNC 75 Ω socket
Signal	Compliant with SMPTE 310M-2004
Data rate	19,392658 Mbit/s
Packet length	188 bytes
Max cable length (Belden 8281 type)	300 m typical

B.4.3 Ethernet management port

Table B.7 Ethernet Management Port Specification

Type	10/100Base-T
Connector type	RJ45

B.4.4 Ethernet data port

Table B.8 Ethernet Data Port Specification

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

Table B.9 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.4.5 Serial USB interface

Table B.10 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.11 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.12 Alarm Relay and Reset Port Pin Out

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

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.13](#).

Table B.13 Safety requirements met.

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

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 lose 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.

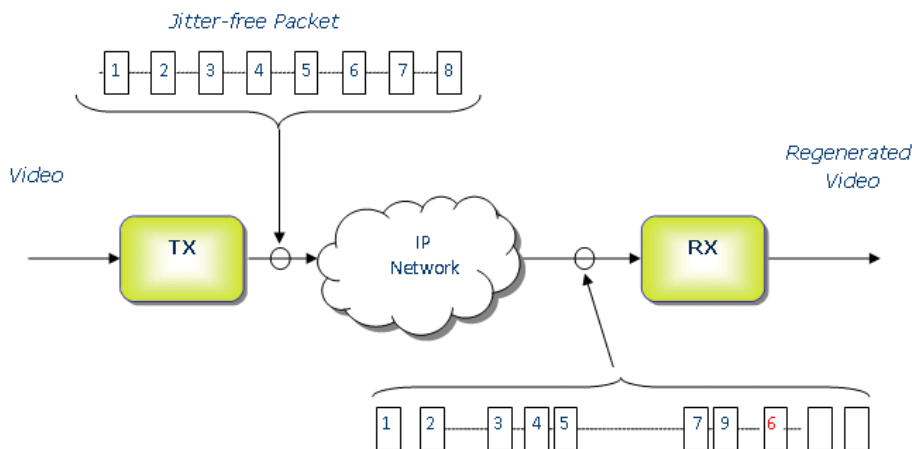


Figure C.1 Impairments of an IP packet stream

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.

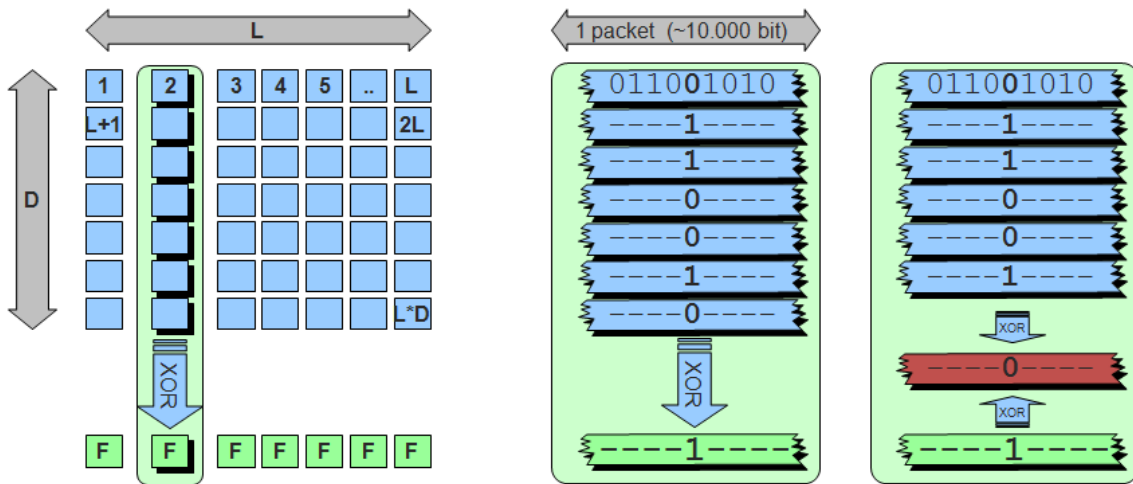


Figure C.2 IP packet FEC calculation matrix

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.

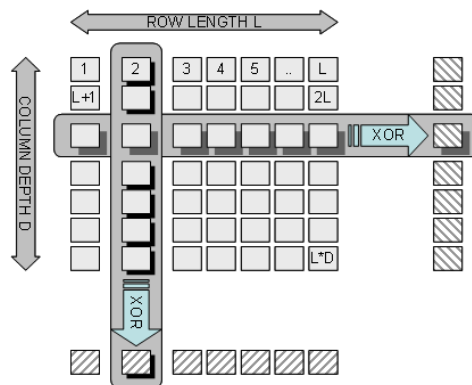


Figure C.3 Two-dimensional FEC calculation matrix

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.

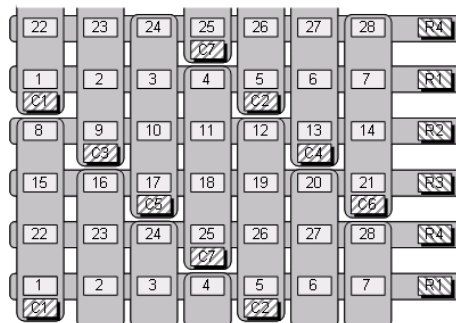


Figure C.4 FEC matrix with column offset

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.

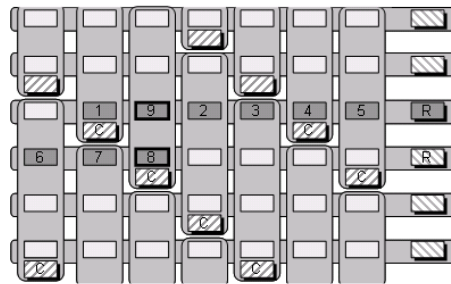


Figure C.5 Offset FEC matrix with missing packets

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.

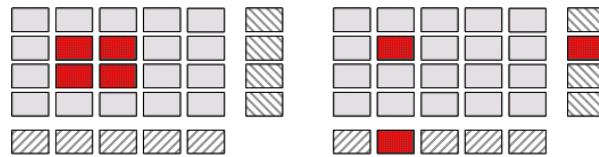


Figure C.6 Uncorrectable error patterns

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.

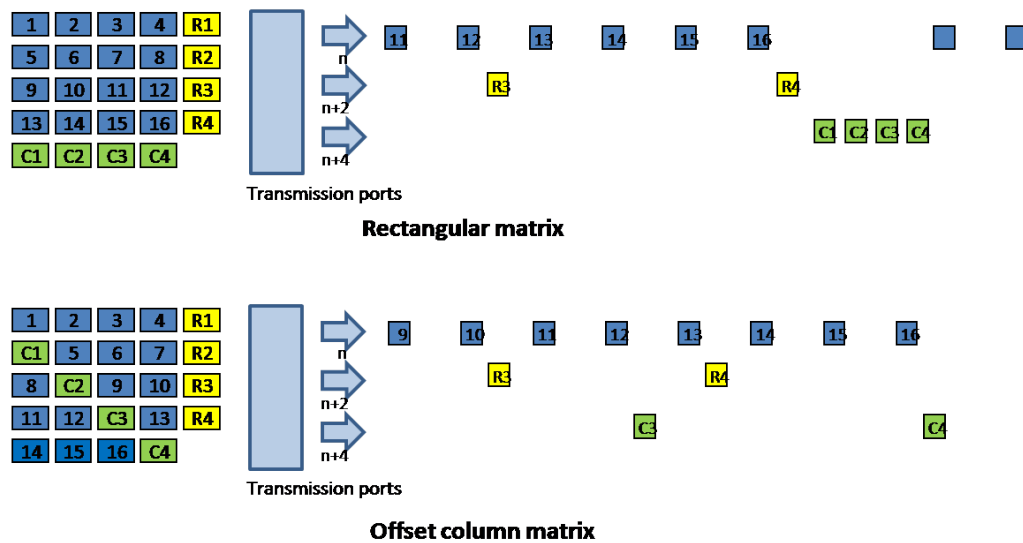


Figure C.7 FEC data transmission

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.

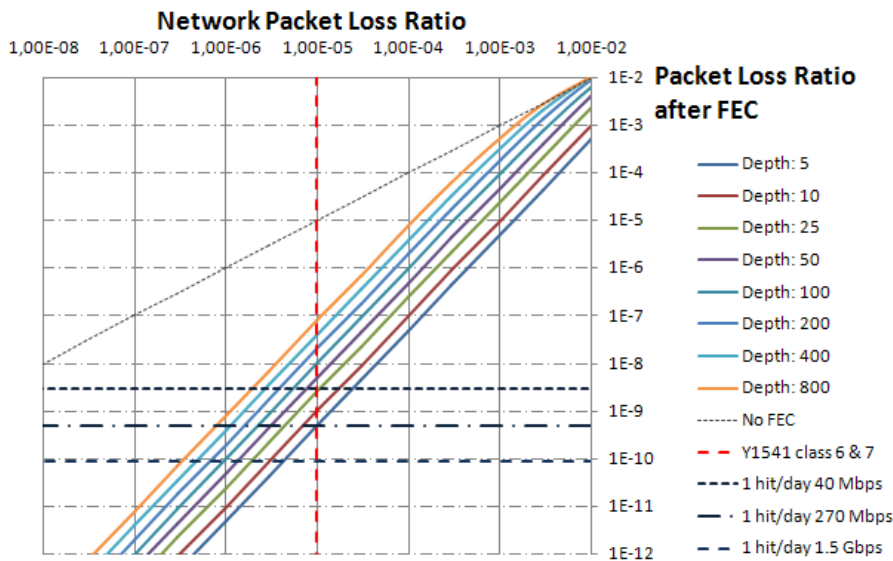


Figure C.9 Error improvement using column FEC only

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.

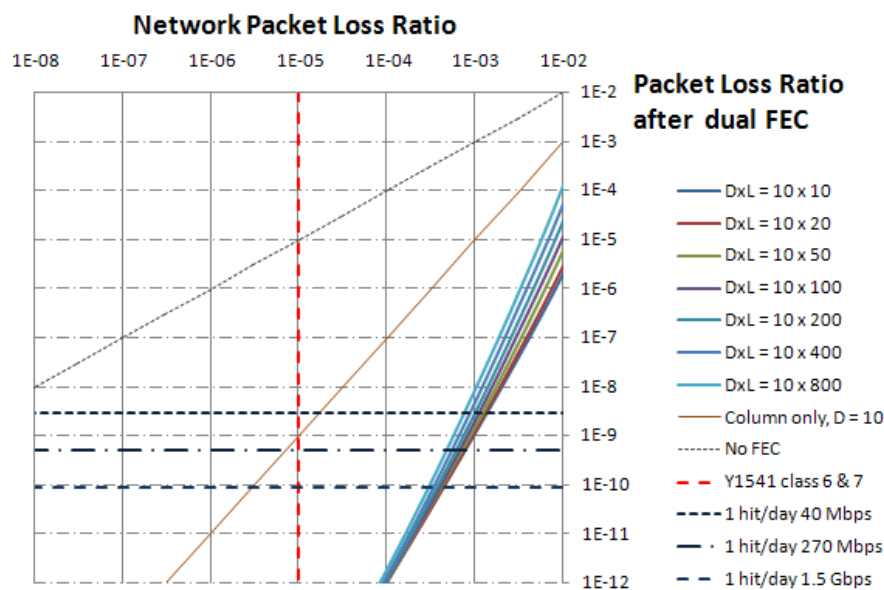


Figure C.10 Error improvement using two-dimensional FEC

[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.

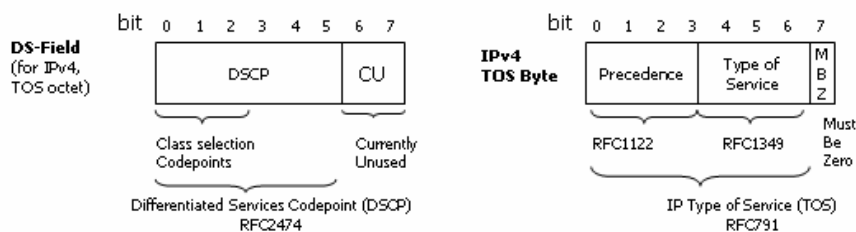


Figure D.1 Differentiated services (Diff-serve) and precedence bits (TOS)

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 CP524 configuration

The number entered into the Type of service (TOS) field in CP524 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 CP524 configuration

The COS priority is entered in the VLAN configuration page in the CP524 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 CP524 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 CP524. 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>
133	Generic SFP alarm	Critical	<p><i>Description:</i> Generic SFP alarm for Mipot and SFF-8472 based modules.</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>
134	Ethernet link problem	Critical	<p><i>Description:</i> Problem on the ethernet link</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>

Table E.3.b Alarms

Alarm ID	Text	Def. severity	Details
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>
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>
159	Unsynchronized diversity source	Warning	<p><i>Description:</i> Data received on diversity sources cannot be used for merging of streams.</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>

Table E.3.c Alarms

Alarm ID	Text	Def. severity	Details
166	Time source switch	Notification	<i>Description:</i> Device started using a new time source. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> No
167	Time adjusted	Notification	<i>Description:</i> The real time clock of the device was adjusted significantly. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> No
168	Power failed	Warning	<i>Description:</i> One or more power supplies have failed, or are out of regulation. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes <i>Subid3:</i> Power supply ID
169	Virtual alarm relay activated	Notification	<i>Description:</i> A virtual alarm relay has been activated. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes <i>Subid3:</i> Relay ID
200	No GPS 1PPS ref. signal	Critical	<i>Description:</i> The 1PPS reference signal is lost (The regulator has however not lost synchronization). <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes
201	Lost GPS 1PPS sync.	Critical	<i>Description:</i> The clock synchronization mechanism has been resynchronized due to too large phase error. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes
210	Emergency switch active	Notification	<i>Description:</i> A user has activated the remote emergency switch. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes
211	Emergency switch unreachable	Warning	<i>Description:</i> The device is not able to communicate with the remote emergency switch. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes
212	Emergency switch rule config error	Warning	<i>Description:</i> An error has been detected in the configuration of the emergency switch. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> Yes
501	User logged in	Notification	<i>Description:</i> This event is generated when a user logs on to the system. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> No
502	User logged out	Notification	<i>Description:</i> This event is generated when a user logs out from the system. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> No
503	System started	Notification	<i>Description:</i> The system has booted. <i>Type:</i> System (Type ID = 13) <i>Clear event:</i> No

Table E.3.d Alarms

Alarm ID	Text	Def. severity	Details
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>
509	Switch done	Notification	<p><i>Description:</i> A switch has been performed.</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> No</p> <p><i>Subid3:</i> Source</p>
510	Auto switch performed	Filtered	<p><i>Description:</i> An automatic switch has been performed.</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>
511	Unable to switch	Warning	<p><i>Description:</i> Switch criteria met but non-active input has too high alarm status.</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>
512	Auto switch ctrl. disabled	Warning	<p><i>Description:</i> Switch is in manual mode.</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>
513	Spare is active	Warning	<p><i>Description:</i> Spare input is active</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>

Table E.3.e Alarms

Alarm ID	Text	Def. severity	Details
514	Missing main service	Warning	<p><i>Description:</i> Main input is missing.</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>
515	Missing spare service	Warning	<p><i>Description:</i> Spare input is missing</p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>
516	Switcher configuration alarm	Warning	<p><i>Description:</i></p> <p><i>Type:</i> Switcher (<i>Type ID</i> = 14)</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Source</p>
517	Alarm log cleared	Notification	<p><i>Description:</i> Alarm log was cleared, user in details</p> <p><i>Type:</i> System (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 13)</p> <p><i>Clear event:</i> No</p>

Table E.3.f Alarms

Alarm ID	Text	Def. severity	Details
1100	Sync unstable	Major	<i>Description:</i> Two separate sync-losses in 10s. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1101	TS unstable	Minor	<i>Description:</i> Lots of PIDs appearing/disappearing or CC errors. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
1110	No sync	Critical	<i>Description:</i> No valid ASI stream detected. <i>Type:</i> Port (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier

Table E.3.g Alarms

Alarm ID	Text	Def. severity	Details
1152	PMT scrambled	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>
1153	PMT missing	Warning	<p><i>Description:</i> PMT not found in transport stream.</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>
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>
1510	Output overflow	Critical	<p><i>Description:</i> The total bit rate of the ASI input stream is too high.</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>
1511	PID conflict	Warning	<p><i>Description:</i> The unit has detected a PID conflict on the output.</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>
1512	Service ID conflict	Warning	<p><i>Description:</i> The MUX has detected a service ID conflict on the regenerated output.</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>
1520	Pri 1 tables delayed	Warning	<p><i>Description:</i> SI playout module not able to maintain configured repetition intervals for priority 1 tables (PAT, CAT, PMT).</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>
1521	Pri 2 tables delayed	Warning	<p><i>Description:</i> SI playout module not able to maintain configured repetition intervals for priority 2 tables (NITa, SDTa, EITpfa).</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.h Alarms

Alarm ID	Text	Def. severity	Details
1522	Pri 3 tables delayed	Warning	<p><i>Description:</i> SI playout module not able to maintain configured repetition intervals for priority 3 tables (NITo, SDTo, BAT, EITpfo, EITsch a+o).</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>
1540	MIP resync	Notification	<p><i>Description:</i> This alarm is raised when the MIP insertion process is resynchronised.</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>
1541	MIP enabled when no 1PPS lock configured	Warning	<p><i>Description:</i> MIP insertion is enabled, but the unit is not locked to an external 1PPS source.</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>
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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<i>Type ID</i> = 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 (<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>
1803	PID rate too low	Filtered	<p><i>Description:</i> PID 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> <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>

Table E.3.i Alarms

Alarm ID	Text	Def. severity	Details
1813	TS rate too low	Filtered	<i>Description:</i> TS bitrate is lower than set limit. <i>Type:</i> Port (<i>Type ID</i> = 9) <i>Clear event:</i> Yes <i>Subid2:</i> Port identifier
2001	No SI download client	Warning	<i>Description:</i> No contact with SI download client. <i>Type:</i> System (<i>Type ID</i> = 13) <i>Clear event:</i> Yes
2002	No PSIP download client	Warning	<i>Description:</i> No contact with PSIP download client. <i>Type:</i> System (<i>Type ID</i> = 13) <i>Clear event:</i> Yes
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

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