TVG425
MPEG-2 Transport Stream Gateway
User's Manual

Revision: 3.4 (4208)

2013-09-30

Valid for SW version 3.4.0 and newer

Contents

1 History 9

2 Introduction 11

2.1 Scope 11
2.2 Warnings, cautions and notes 11
2.3 Heed warnings 12
2.4 Contact information 12

3 Short Product Description 13

3.1 Summary of features 13
3.2 Options 14
3.2.1 Hardware options 14
3.2.2 Software options 15

4 Getting Started 17

4.1 Configure the management interface 17
4.2 Configure device name and time settings 18
4.3 Configure operation 18
4.3.1 ASI Stream source 18
4.3.2 IP Stream source 19
4.3.3 Stream to ASI output for monitoring. 19
4.3.4 Stream IP encapsulation and transmission. 20

5 Installing the Equipment 21

5.1 Inspect the package content 21
5.2 Installation Environment 21
5.3 Equipment installation 22
5.4 Ventilation 22
5.5 Power supply 23
5.5.1 AC power supply 23
5.5.1.1 AC power cable 23
5.5.1.2 Protective Earth/technical Earth 24
5.5.1.3 Connecting to the AC power supply 24
5.5.2 DC power supply 25
5.5.2.1 DC power cable 25
5.5.3 Powering up/down 25

6 Functional Description 27

6.1 IP transmit mode 27
6.2 IP receive mode 27

6.3 Hitless switching 28
6.4 Management sub-system 29
6.4.1 Graphical user interface 29
6.4.2 Configuration database 29
6.4.3 Alarm manager 30
6.5 Time synchronisation 31
6.6 Video over IP 31
6.6.1 Protocol mapping 31
6.6.1.1 UDP mode 32
6.7 Forward Error Correction (FEC) 32
6.8 The SFP module 33
6.9 Redundancy controller 34
6.9.1 Operation 35

7 Physical Description 37

7.1 ASI ports 37
7.1.1 ASI input ports 38
7.1.2 ASI output ports 38
7.2 1 PPS Input 38
7.3 Ethernet data ports 39
7.4 Ethernet management port 39
7.5 Power supply 40
7.6 Technical earth 40
7.6.1 Alarm/Reset connector 40
7.6.2 Serial USB interface 41

8 Operating the Equipment 43

8.1 Accessing the graphical user interface 43
8.2 Password protection 43
8.2.1 Resetting the password list 44
8.3 Changing the IP address of the unit 44
8.3.1 Changing IP address via the Web GUI 44
8.3.2 Changing the management port IP address via terminal interface 45
8.3.3 Configuring automatic IP address assignment 46
8.3.4 Detecting the management port IP address 47
8.3.4.1 USB Interface 47
8.3.4.2 Nevion Detect 47

9 WEB Interface 49

9.1 Login 49
9.2 Status header 50
9.3 Status 51
9.3.1 Current Status 51
9.3.2 Alarm log 54

9.4 Device Info 55
- 9.4.1 Product info 55
- 9.4.2 Alarms 58
  - 9.4.2.1 Device alarms 58
  - 9.4.2.2 Global configuration 59
  - 9.4.2.3 Relays and LED 60
  - 9.4.2.4 Alarm log settings 62
- 9.4.3 Time Settings 63
- 9.4.4 Network 65
  - 9.4.4.1 Interfaces 67
  - 9.4.4.1.1 Main 67
  - 9.4.4.1.2 Interface Settings 67
  - 9.4.4.1.3 DHCP Settings 68
  - 9.4.4.1.4 DHCP Status 68
  - 9.4.4.1.5 Manual IP Settings 70
  - 9.4.4.1.6 Interface Status 70
  - 9.4.4.1.7 Detect Settings 70
  - 9.4.4.1.8 Alarms 70
  - 9.4.4.1.9 Advanced 71
  - 9.4.4.1.10 Status 71
  - 9.4.4.1.11 VLAN 73
  - 9.4.4.1.12 Main Settings 74
  - 9.4.4.1.13 Manual IP Settings 74
  - 9.4.4.1.14 Advanced Settings 74
  - 9.4.4.1.15 DHCP settings and status 75
  - 9.4.4.1.16 SFP 75
  - 9.4.4.2 DNS Settings 83
  - 9.4.4.3 IP Routing 83
  - 9.4.4.4 TXP Settings 84
  - 9.4.4.5 SNMP Settings 85
  - 9.4.4.6 Tools 87
  - 9.4.4.6.1 Ping 87
  - 9.4.4.6.2 Traceroute 88
- 9.4.5 Clock Regulator 90
  - 9.4.5.1 Main 90
  - 9.4.5.2 Alarms 91
- 9.4.6 Save/Load Config 91
  - 9.4.6.1 Save/Load Configs 91
  - 9.4.6.1.1 Save Configuration 91
  - 9.4.6.1.2 Load Configuration From file 92
  - 9.4.6.1.3 Load Configuration from Remote Device 93
  - 9.4.6.1.4 Load options 93
  - 9.4.6.2 Boot Log 94
  - 9.4.6.3 Stored Configs 94
- 9.4.7 Maintenance 96
  - 9.4.7.1 General 96
  - 9.4.7.2 Software Upgrade 98
  - 9.4.7.3 Feature Upgrade 99

9.4.8 Users 100
9.4.9 GUI Preferences 100
9.5 Inputs 101
9.5.1 Inputs Overview 101
9.5.1.1 IP Inputs 103
9.5.1.2 Switch Inputs 104
9.5.2 Input 105
9.5.2.1 Main 106
9.5.2.2 Alarms 109
9.5.2.3 IP 113
9.5.2.3.1 RTP/IP Diversity Reception 116
9.5.2.3.2 FEC 119
9.5.2.3.3 Ping 120
9.5.2.3.4 Regulator 121
9.5.2.4 Services 124
9.5.2.5 PIDs 127
9.5.2.6 Tables 130
9.5.2.7 Tables 130
9.5.2.8 Settings 131
9.5.3 Switch Inputs 133
9.5.3.1 Main 133
9.6 Streams 135
9.6.1 Streams overview 135
9.6.2 Stream 136
9.6.3 Main 136
9.6.4 Alarms 140
9.6.5 Stream to IP destination 140
9.6.5.1 Main 140
9.6.5.2 FEC 143
9.6.5.3 Ping 145
9.6.6 RIP-2 146
9.7 Redundancy 148
9.7.1 Redundancy Controller 148
9.7.1.1 Device redundancy controller switching 149
9.7.1.2 Communication 151
9.7.1.3 SNMP Switch Actions 153
9.7.2 Service switchers 153
10 SNMP 157
10.1 SNMP agent characteristics 157
10.2 MIB naming conventions 157
10.3 MIB overview 157
10.3.1 Supported standard MIBs 157
10.3.2 Custom MIBs 157
10.4 SNMP related configuration settings 159
10.4.1 Community strings 160

10.4.2 Trap destination table 160
10.4.3 Trap configuration 160
10.5 Alarm/status related SNMP TRAPs 161
10.5.1 The main trap messages 161
10.5.2 Severity indications 161
10.5.3 Alarm event fields 162
10.5.4 Matching of on/off traps 163
10.5.5 Legacy trap messages 163
10.6 Using net-snmp to access MIB information 164
10.6.1 Reading a parameter with snmpget 164
10.6.2 Writing a parameter with snmpset 164

11 Preventive Maintenance and Fault-finding 167

11.1 Preventive maintenance 167
11.1.1 Routine inspection 167
11.1.2 Cleaning 167
11.1.3 Servicing 167
11.1.4 Warranty 168
11.2 Fault-finding 168
11.2.1 Preliminary checks 168
11.2.2 PSU LED not lit / power supply problem 169
11.2.3 Fan(s) not working / unit overheating 170
11.3 Disposing of this equipment 170
11.4 Returning the unit 170

A Glossary 171

B Technical Specification 177

B.1 Physical details 177
B.1.1 Half-width version 177
B.2 Environmental conditions 177
B.3 Power 177
B.3.1 AC Mains supply 177
B.3.2 DC supply 178
B.4 Input/output ports 178
B.4.1 DVB ASI port 178
B.4.2 Ethernet management port 178
B.4.3 Ethernet data port 179
B.4.4 Serial USB interface 179
B.5 Alarm ports 179
B.5.1 Alarm relay/reset port specification 179
B.6 External reference 180
B.6.1 10MHz/1 PPS input 180
B.7 Compliance 180
B.7.1 Safety 180

B.7.2 Electromagnetic compatibility - EMC 180
B.7.3 CE marking 181
B.7.4 Interface to “public telecommunication system” 181

C Forward Error Correction in IP Networks 183

C.1 IP stream distortion 183
C.2 Standardisation 184
C.3 FEC matrix 184
C.4 Transmission aspects 187
C.5 Quality of service and packet loss in IP networks 188
C.6 Error improvement 189
C.7 Latency and overhead 190

D Quality of Service, Setting Packet Priority 193

D.1 MPLS 193
D.2 Layer 3 routing 193
D.2.1 TVG425 configuration 194
D.3 Layer 2 priority 194
D.3.1 TVG425 configuration 194

E Alarms 195

F References 209

1 History

Revision	Date	SW version	Comments
3.4	Sep 2013	3.4.0	Added description of RIPv2 functionality. Added description of new SSRC Mode parameter on output. Included small section on how the Detect application can be used to configure the IP address. Update to the time sources configuration page description Description of new MTU option on Ping tools. Description of new tool Trace route available from GUI Added VIGW-PLAT-TS-INPUTSWICHING-MIB to the list of custom MIBs Alarm table updated with latest changes. Added comment on DHCP option in **Section 8.3: Changing the IP address of the unit**
3.2	Apr 2013	3.2.x	Added description of Embedded Redundancy feature. Added description DHCP and DNS. Updated figures for new Nevion layout.
3.0	Feb 2013	3.0.x	Updated for Nevion Added description of new functions - IP/RTP diversity reception feature (hitless switching). - manual bitrate option. - New fast coarse IP source syncing mode for non-PCR streams - Cover-up time feature - Bitrate limiting feature on ASI inputs. - Configuration of 204 byte TS packets on IP layer. - Option to set ASI outputs in DC or Idle when no data to sent. - Dual A/C power hardware option - Configuration ID parameter - Load configuration from remote device - Generate system report - Licences that can be upgraded without reboot (hot upgradable)
2.0	June 2011	2.0.x	Updated with FEC and new options list. Minor overall improvement to layout.
1.4	December 2010	1.4.22	Initial release

2 Introduction

2.1 Scope

This manual is written for operators and users of the TVG425 Transport Stream Gateway and provides necessary information for installation, operation and day-to-day maintenance of the unit. The manual covers the functionality of the software version 3.4.0 or later, and continues to be relevant to subsequent software versions where the functionality of the equipment has not been changed. When a new software version changes the functionality of the product, an updated version of this manual will be provided.

The manual covers the following topics:

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

2.2 Warnings, cautions and notes

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

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

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

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

2.3 Heed warnings

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

2.4 Contact information

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

Please contact us at:

Telephone	+47 22 88 97 50
Fax	+47 22 88 97 51
E-mail	support@nevion.com
WEB	http://www.nevion.com
Mail and visiting address	Nevion Nils Hansens vei 2 NO-0667 Oslo Norway

3 Short Product Description

The TVG425 Transport Stream Gateway is a member of the Nevion Video Gateway suite; a line of compact, powerful and cost-effective products designed for real-time contribution and distribution of broadcast quality video over IP networks.

The TVG425 provides gateway functionality to encapsulate MPEG-2 transports streams to be transported over IP networks, and to extract MPEG-2 streams from IP encapsulation. It will also redirect MPEG-2 transport streams from an input to multiple outputs. The input transport streams may arrive via one of up to 8 ASI ports using coaxial cable, and/or through either of two independent IP Network connections. Received transport streams may likewise be output as individual transport streams on one or more ASI ports, and/or as one or more IP streams through the IP network interfaces.

The TVG425 has functionality to perform detailed analysis of each received transport stream, which enables close monitoring of transport stream integrity. In addition it contains logic to perform redundancy switching of input streams, as specified by the operator.

Up to 24 individual MPEG-2 transport streams may be handled simultaneously, depending on the licence installed (Number of input ports activated), refer to chapter **Section 9.4.7.1**

The TVG425 is housed in a 1RU hight rack-mounted enclosure containing a DSP module (Master Module) and 1 or 2 ASI I/O boards. Optical Gigabit or a second electrical Gigabit port is provided by an optional SFP (Small Form-Factor Pluggable) slot.

3.1 Summary of features

Features of the TVG425 include:

- Transmission and reception of MPEG2 Transport Streams over Gigabit Ethernet
  - MPTS / SPTS capable
  - Up to 8 bi-directional DVB-ASI inputs/outputs
  - Input/Output direction switching without reset
  - Fast and accurate locking to Transport Stream
  - Supports both CBR and VBR Transport Streams
  - VLAN support
- End-to-end Quality of Service
  - Forward Error Correction for increased robustness against network packet loss
  - TOS/COS field support for traffic prioritisation

- Compact, cost-effective solutions
  - Complete transmitter / receiver in 1RU
  - User configurable as transmitter, receiver or bi-directional
- User-friendly configuration and control
  - WEB/XML based remote control
  - SNMPv2c and SNMPv1 agent for easy integration with NMS systems
  - Integrated with Nevion Connect
- 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
- 1 PPS timing reference input
- Redundancy switching

3.2 Options

The TVG425 is modular and may be equipped according to user requirements. Available hardware and software options are described below.

3.2.1 Hardware options

SFP Module

The TVG425 is equipped with an SFP socket. Different types of SFP modules may optionally be delivered to provide optical Gigabit transportation.

Dual power supplies

The TVG425 may optionally be delivered with dual internal wide-ranging AC power supplies. In this case the size of the cabinet is always full-width 1RU. The power supplies cover the voltage range 100-240 VAC, 50/60 Hz.

3.2.2 Software options

The TVG425 functionality depends on the sofware licences installed. The following table describes the features available as software options. Please refer to **Section 9.4.7.3** for more information how to obtain and enable feature upgrades.

Table 3.1 Functionality enabled through software licences

Functionality	Max value	Description
SFP module	-	Enables operation of the Small form-factor pluggable (SFP) transceiver slot.
SFP configuration	-	Enables configuration interface and parameter storage for some specifically supported SFP modules.
Input switching	-	Enables creation of input switching groups.
Forward Error Correction	-	Controls availability of the FEC feature for IP outputs and IP inputs.
RTP/IP diversity reception	-	Enables configuration of IP diversity reception input pairs.
SFN Rate Lock	-	Controls whether the device can use DVB-T MIP timestamps to lock outgoing rate when in IP to ASI mode.
Output Streams	8	Controls the number of Transport Stream outputs that can be active at the same time.
Connect control	-	Enables supervision of the unit through the Connect Software.
Embedded redundancy controller	-	Availability of on-unit redundancy controller service.

4 Getting Started

This section provides a short description of the minimum steps that must be taken in order to start operating the TVG425.

If you are an experienced user of Nevion equipment or similar types of MPEG-2 processing equipment the following description should enable you to quickly install the TVG425 Transport Stream Gateway and start operation. If this is your first time to install such equipment you are strongly adviced to read the full installation procedure. To gain full benefit of the product functionality and capabilities refer to the user interface description.

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

4.1 Configure the management interface

Since the TVG425 is all Web controlled the first step is to set up the IP address for the management interface.

Changing the default IP address using the Web interface requires that your management computer may be configured with a static IP address. If a static IP address cannot be configured on your computer the IP address may be configured via the terminal interface. The procedure is described in the user manual, refer to section 8.3.2.

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

1. Connect an Ethernet cable directly between the PC and the Ethernet Control port of the TVG425. The default IP address of the TVG425 is **10.0.0.10/255.255.255.0**. Configure the PC to be on the same subnet as the TVG425.

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

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

4. The connection with your management PC will now be lost. To re-connect to the TVG425 connect both the “Control” port of the unit and the management PC to the network. The IP settings of the management PC must now be set to agree with the network used.

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

4.2 Configure device name and time settings

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

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

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

4.3 Configure operation

The basic entity to consider in theTVG425 is the internal Stream to which input source and output(s) are allocated. A Stream may be sourced from an ASI or IP input, respectively, and may be routed to one or several ASI and/or IP outputs, as required. Transport streams received on IP are de-encapsulated into the internal Stream. Conversely a Stream is appropriately encapsulated before being sent to an IP output interface. The TVG425 operation does not distinguish between single program and multi program transport streams.

4.3.1 ASI Stream source

The following describes the procedure to prepare a transport stream arriving on an ASI input port to source a TVG425 Stream.

1. Select the ASI input port to receive the transport stream. Browse to Inputs and click on the ASI port you want to activate, designated ASI #.

2. In the Main page, Transport Stream Details field, tick the Enable input check box and type an identifying name, e.g. the service name, in the Input label box. Select DVB or ATSC, as appropriate, in the TS mode pull-down menu. Click Apply to activate.

3. If a transport stream is applied to the ASI input connector the Transport Stream Details field will now indicate its presence and properties. The Pids Present and Services Present fields will show the composition of the transport stream.

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

4.3.2 IP Stream source

This procedure enables an IP input to source a TVG425 Stream.

1. Browse to Inputs > Inputs Overview > IP Inputs. At the bottom of the page, click the Add IP Input button. Click Apply. An entry for the new input appears in the table, with default values for all parameters.

2. Open the IP input configuration page by clicking on the table entry.

3. In the Main page, IP RX Configuration field, tick the Enable input check box and type an identifying name, e.g. the service name, in the Input label box. Specify the UDP receive port. If the signal to receive is an IP multicast click the Join multicast check box and enter the multicast address in the adjacent field.

4. Select the Ethernet interface from the alternatives in the Source interface pull-down list. Click Apply to activate.

5. In the Transport Stream Details field select DVB or ATSC in the TS mode pull-down menu, according to the incoming transport stream format. Click Apply to activate.

6. The IP RX Status field will indicate if the attached network cable carries a valid signal and the remaining status fields will report the properties and contents of the incoming transport stream.

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

4.3.3 Stream to ASI output for monitoring.

The below procedure enables routing a TVG425 Stream to an ASI output.

1. Browse to Outputs and select Stream 1 in the navigator list.

2. In the Main page, Stream Configuration field, tick the Enable output check box and enter an identifying name in the Output label field. Click on the icon next to the Source input field and select the ASI input activated previously.

3. In the ASI Outputs Configuration field adjust the ASI output characteristics by clicking on the appropriate radio buttons.

4. In the ASI ports field click on Add as Output in the line of the desired ASI output port.

5. Click Apply to commit the changes.

Returning to the Status page, the block diagram now reflects the TVG425 behaviour, showing the input and output connections to Stream 1.

4.3.4 Stream IP encapsulation and transmission.

This procedure enables IP encapsulation of a TVG425 Stream.

1. Go to the Output > Stream 1 > Main page and click on the Add IP destination button at the bottom of the page.

2. Having confirmed the addition of an IP destination, the IP outputs field changes to allow specifying IP destination parameters.

3. In the IP Output Basic Configuration field tick the Enable box and enter the appropriate destination address in the field provided. Select RTP or UDP protocol and enter the UDP destination port number in the box provided.

4. Click Apply to commit the changes.

5. The IP Output status field indicates the default physical interface used. This may be changed by clicking the Manual destination interface in the IP Output Basic Configuration field and selecting the desired interface from the pull-down list.

The IP status field also indicates when the destination has been reached (Resolved = Yes) and the bit rate of the IP encapsulated transport stream. Several additional IP parameters may be set in the Outputs > Stream > IP destination > Main page. See section 9.6.5.1 for details.

5 Installing the Equipment

Caution: The TVG425 must be handled carefully to prevent safety hazards and equipment damage. Ensure that the personnel designated to install the unit have the required skill and knowledge. Follow the instructions for installation and use only installation accessories recommended by the manufacturers.

5.1 Inspect the package content

- Inspect the shipping container for damage. Keep the shipping container and cushioning material until you have inspected the contents of the shipment for completeness and have checked that the TVG425 is mechanically and electrically in order.
- Verify that you received the following items:
  - TVG425 with correct power supply option
  - Power cord(s)
  - CD-ROM containing documentation and Flash Player installation files
  - Any optional accessories you have ordered

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

5.2 Installation Environment

As with any electronic device, the TVG425 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 TVG425.
- 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 TVG425 has been subject to a lightning strike or a power surge which has stopped it working, disconnect the power immediately. Do not re-apply power until it has been checked for safety. If in doubt contact Nevion.

5.3 Equipment installation

The TVG425 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 TVG425 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 TVG425.

5.4 Ventilation

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

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

- This product should never be placed near or over a radiator or heat register. Do not place in a built-in installation (e.g. a rack) unless proper ventilation is provided in accordance with the device airflow design as depicted in Figure 5.1.
- The TVG425 may be vertically stacked in 19" racks without intermediate ventilation panels. In systems with stacked units forced-air cooling may be required to reduce the operating ambient temperature.

  Figure 5.1 shows the air path through the unit, where cool air is taken from the left hand side, seen from the front.

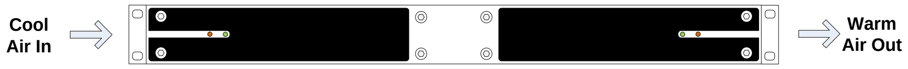


Figure 5.1 Air path through the unit

5.5 Power supply

The TVG425 may be delivered rated for AC or DC operation, respectively.

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

5.5.1 AC power supply

The TVG425 has a wide-range power supply accepting the voltage range 100-240 VAC, 50/60 Hz. Please refer to **Appendix B** for a detailed specification of the AC power supply.

5.5.1.1 AC power cable

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

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

The unit is supplied with a two meter detachable mains supply cable equipped with a moulded plug suitable for Europe, UK or USA, as appropriate. The wires in the mains cable are coloured in accordance with the wire colour code shown in **Table 5.1**.

Table 5.1 Supply cable wiring colours

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

5.5.1.2 Protective Earth/technical Earth

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

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

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

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

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

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

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

5.5.1.3 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 TVG425 mains input connector(s) and then to the local mains supply.

5.5.2 DC power supply

The TVG425 can be delivered with a 48 VDC power supply for use in environments where this is required. The DC power supply accepts an input voltage range of 36-72 VDC. Please refer to **Appendix B** for detailed specification of the power supply.

5.5.2.1 DC power cable

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

Table 5.2 DC power connector pin assignment

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

To connect the unit to the local DC power supply:

1. Use an electronics soldering iron or a hot air workstation to attach the supplied female D-SUB power connector to suitable power leads.
2. Connect the power leads to your local power supply.
3. Connect the DC power connector, with attached power leads, to the TVG425 power input connector.

5.5.3 Powering up/down

Before powering-up the unit, please ensure that:

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

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

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

6 Functional Description

This chapter provides a high-level functional description of the TVG425 and an overview of transmission of MPEG-2 data over IP networks.

The TVG425 is capable of receiving multiple MPEG-2 transports treams, in ASI format or as IP streams, and re-direct received streams to a number of output interfaces. A stream received on one ASI interface may be sent out over one or several different ASI interfaces, as needed. At the same time the stream may be encapsulated and sent out over one or several IP interfaces. Similarly, a stream received over one IP interface may be re-directed and sent out over one or several different IP interfaces, while at the same time being extracted and sent out over one or more ASI interfaces.

Internally, MPEG-2 transport streams are referred to as Streams to which one input and one or several outputs are allocated. Two or more input signals may be applied to a redundancy switch, which in turn can be used to source an internal Stream.

In the IP transmit mode, the TVG425 encapsulates a Stream (MPEG-2 transport stream format) into an IP stream. The stream is sent via an Ethernet interface onto the IP network.

In IP receive mode, the TVG425 receives and extracts one or more MPEG2 transport streams from the IP network to provide inputs to one or more internal Streams, or to a redundancy switch, as required.

6.1 IP transmit mode

In the IP transmit mode the MPEG-2 transport streams to encapsulate are sourced by the internal Stream. The TVG425 has a feature to auto detect of 188/204 byte packets on ASI inputs and sends 188 byte packets over the IP network by default. It is possible to configure the unit to keep 204 byte packets if required. The MPEG-2 transport stream packets are encapsulated as described in section 6.6.1. The user configures the IP address of the Ethernet data port. For each transport stream to be sent over the IP network the IP destination address and UDP port must be configured. The TVG425 handles both unicast and multicast transmissions.

The IP packets from one internal Stream are then merged with the IP packets from the other internal Streams, if applicable. The combined IP stream is then passed to the physical interface.

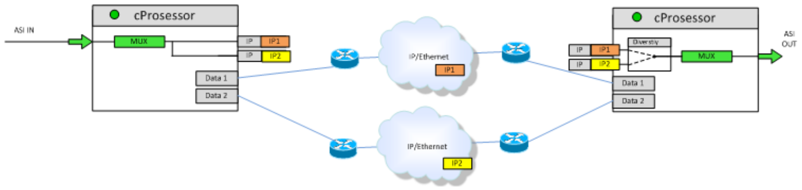
6.2 IP receive mode

In IP receive mode the TVG425 receives IP packets from the physical data interface. The TVG425 will receive streams from multiple IP sources. In the case of unicast, the TVG425 will parse the IP stream and send the transport stream to the internal Stream set up to listen to the appropriate UDP port. In case of multicast, the TVG425 will send a join message to join the configured multicast. When reception is disabled, the TVG425 will send a leave message to the network. The reassembled packets of each MPEG-2 transport stream are held in a buffer. The function of this buffer is to handle re-ordering of packets, compensate network jitter and support the adaptive rate recovery.

6.3 Hitless switching

The TVG425 enables hitless switching by combining smallcast on the transmitter side with RTP/IP diversity reception on the receiver sider. 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 TVG425 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 TVG425 or at the first sebsequent 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 SSRCs, 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.

6.4 Management sub-system

The management subsystem is a set of modules that handles all the interfaces to monitor and control the operation of the TVG425.

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

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

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

6.4.1 Graphical user interface

Operators monitor and control the TVG425 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 TVG425 can be controlled from the web GUI.

6.4.2 Configuration database

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

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

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

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

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

6.4.3 Alarm manager

The TVG425 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 TVG425 supports so-called *Virtual Alarm Relays*. These are highly programmable items that can be customised to react to virtually any given alarm event or combination of alarm events. The status of each virtual alarm relay can be viewed in the GUI and can also be exported using SNMP. Details on configuring the virtual alarm relays can be found in the WEB interface section.

6.5 Time synchronisation

The TVG425 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 TOT/TDT on selectable ASI ports
- From NTP servers using SNTP protocol. Up to four NTP servers can be configured for NTP server redundancy.

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

6.6 Video over IP

One of the core functions of the TVG425 is IP encapsulation of MPEG-2 transport streams. The task is basically to encapsulate video packets into IP frames using the appropriate headers.

6.6.1 Protocol mapping

Figure 6.1 shows the layering of the transport protocols used.

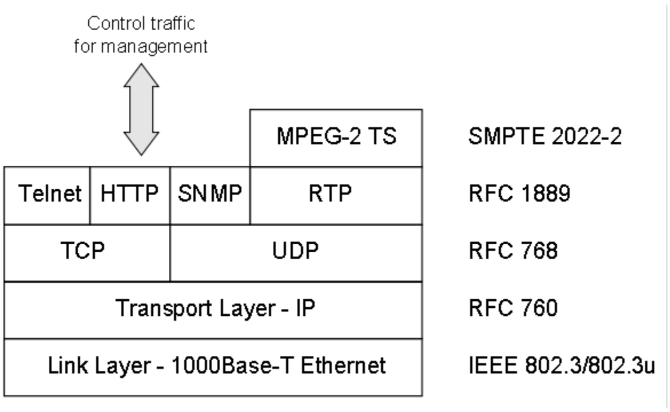


Figure 6.1 Protocol mapping

The MPEG-2 TS layer is specified in ISO/IEC 13818-1.

The TVG425 is able to handle both Multi-Program Transport Streams (MPTS) and Single-Program Transport Streams (SPTS). In the current version, the TVG425 operates in transparent mode, i.e. the unit will encapsulate and extract complete transport streams without changing the streams. This means that no insertion or removal of NULL packets is performed and PCR is sent transparently through the unit.

Control data are handled differently from transport stream data on the next layer. RTP as defined in RFC1889 is applied for the MPEG-2 transport stream data. Three types of protocols are used for control data. HTTP is used when the unit is configured and monitored via the internal WEB server. SNMP is used for alarm traps and simple status polling. Telnet is used for development purposes.

The transport stream data are handled according to RFC768 on the UDP layer. The operator can configure destination port for the MPEG-2 transports stream. The 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.

TCP is used for control data.

6.6.1.1 UDP mode

To allow interoperability with legacy equipment, the TVG425 can stream video over IP without using the RTP protocol encapsulation. This is also called UDP mode or UDP only. UDP mode is manually configured in the transmitting TVG425 unit, and automatically detected by the receiving TVG425.

> **Note:** FEC relies on information in the RTP protocol, and will not be available in UDP mode. FEC is explained in section 6.7.

6.7 Forward Error Correction (FEC)

In real networks data streams may experience packet loss that may seriously degrade the service. In order to cope with packet loss, the TVG425 may provide forward error correction according to Pro-MPEG Code of Practice #3 rev. 2. Pro-MPEG FEC is carried out on RTP packets. The mechanism is based on the insertion of additional data containing the result of an XOR (exclusive OR)-operation of packets over a time window.

The generation of FEC packets is based on the use of a matrix. The matrix size is defined by the number of columns (L) and the number of rows (D). The FEC packets are calculated as an XOR operation over the packets in a column and the packets in a row. Figure 6.2 shows an example of the FEC scheme. In this illustration three missing (corrupt) packets are corrected.

One missing packet per row or column can be calculated by XOR'ing the FEC packet with the other packets in that row or column. Iterative operations makes it possible to correct more than one missing packet per column or row. Please note the restrictions $4 \le L \le 32$, $4 \le D \le 32$ and $L+D \le 32$ and that the maximum matrix size is 256(L*D). When using column FEC only, L is allowed to be in the range $1 \le L \le 32$. The size of the matrix is a trade between latency, transmission overhead and error protection.

'Column FEC' provides correction of consecutive lost packets up to L packets. The FEC packets are generated per column within the matrix allowing loss of any single media packet within a column, or a burst of errored packets within a row to be corrected through the FEC packet. Column FEC is used to correct burst errors and random errors.

'Row FEC' provides correction of non-consecutive packet loss and can correct any single packet loss within a row of media packets. The FEC packets are generated per row allowing loss of any single packet to be recovered. Row FEC is ideal for correcting random packet errors.

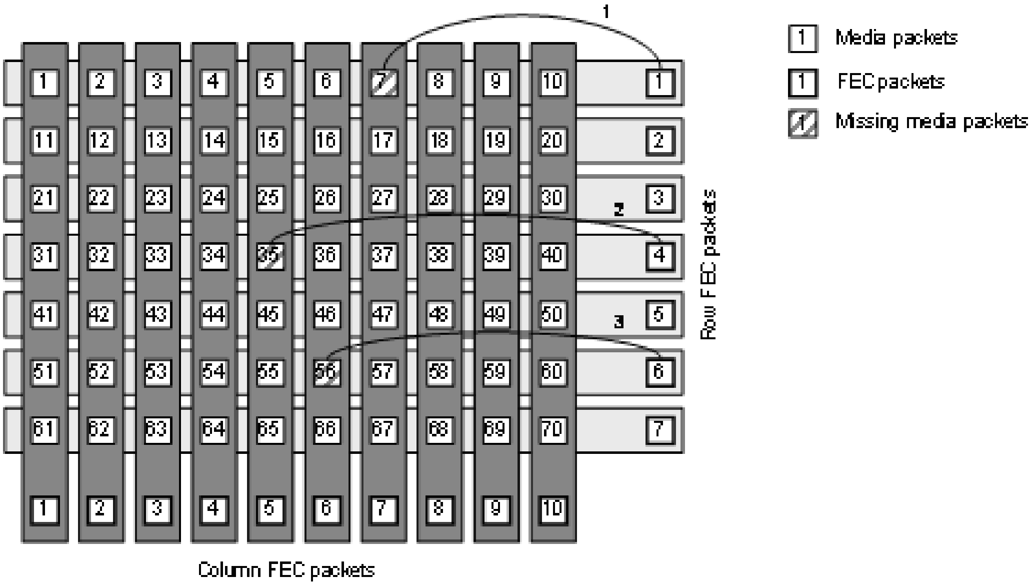


Figure 6.2 Illustration of two-dimensional FEC, where packet 7, 35 and 56 are lost and corrected.

Once the FEC packets have been computed they are transmitted with the media packets to the receiver site. FEC column packets are transmitted on UDP port n+2 and FEC row packets are transmitted on UDP port n+4 where n is the UDP port of the media data. This is in accordance with Pro-MPEG CoP 3.

6.8 The SFP module

The SFP module (SFP = small form-factor pluggable) is a third-party product providing an extra, optional interface to the TVG425. 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 6.3 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 TVG425 WEB interface. Control information is passed to and from the SFP module using the I^{2}C 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 TVG425 provides a slot to accommodate an SFP module. Access to the SFP interface is possible if the SFP software is installed and the feature key has been licensed (see section **Section 9.4.7**).

The SFP interface must be expressly enabled from the TVG425 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.

6.9 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 may be configured to switch back to the main device automatically if the main device recovers.

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 both main and spare devices.

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

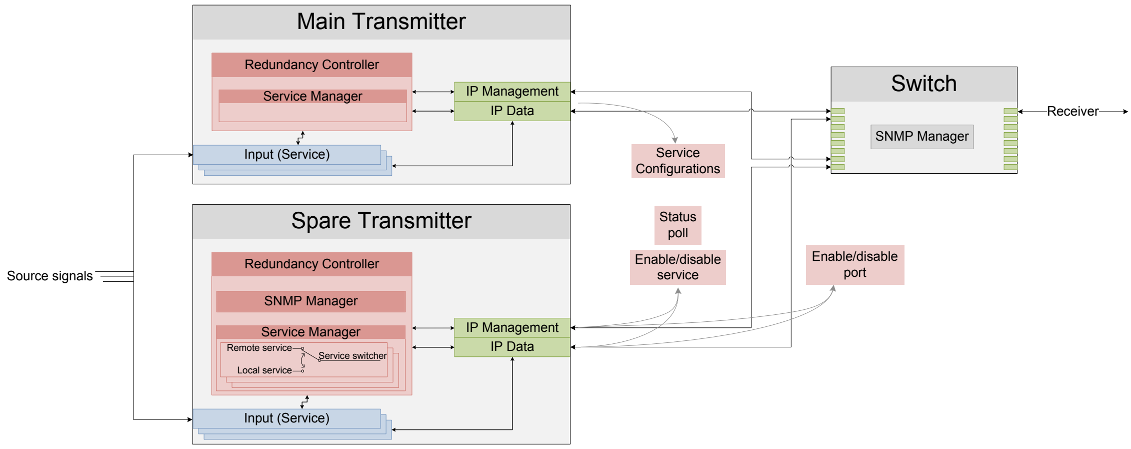


Figure 6.4 An overview of the embedded redundancy controller

6.9.1 Operation

All redundancy control enabled Nevion devices advertise a set of services. A service might be an IP transmitter port, ASI port, SDI port etc. Any service on a Nevion device with redundancy control can be a spare for any compatible service on another Nevion device licenced for 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 6.1.

Table 6.1 Typical states of the redundancy controller

State	Main	Spare
Normal operation	Output enabled	Output disabled
Main service has alarm	Output disabled	Output enabled
No contact with main device	Unknown, typically port on switch disabled	Output enabled

Normal Operation

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

Main service has alarm

When the main 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 main service. This includes disabling the main service before applying the main service configuration to the spare service and finally enabling output of the spare service.

No contact with main device

When the spare device loses contact with the main device all service switchers will switch to spare 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 main device to stop the data transmission from it.

The Embedded Redundancy Controller also offers automatic switch back to main. After a switch to the spare unit has been performed, the spare unit continue to poll the main device. When the main 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 spare alarm”, “No return”.

Return if OK

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

Return if spare alarm

This option will return automatically to the main device if the main device has recovered **and** the spare 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 main.

7 Physical Description

The TVG425 Transport Stream Gateway consists of a main board and one or two ASI boards mounted horizontally in a screened, self-ventilated cabinet. The unit is 1RU high and two units can be mounted side-by-side behind a common front panel in a 19 inch rack. All inputs and outputs are located on the rear panel and there are no front panel keypad or display.

The front panel provides four LEDs per TVG425. The meaning of each LED indicator is shown in table 7.1.

Table 7.1 Front panel LED descriptions

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

These LEDs are replicated on the rear panel, figure 7.1.

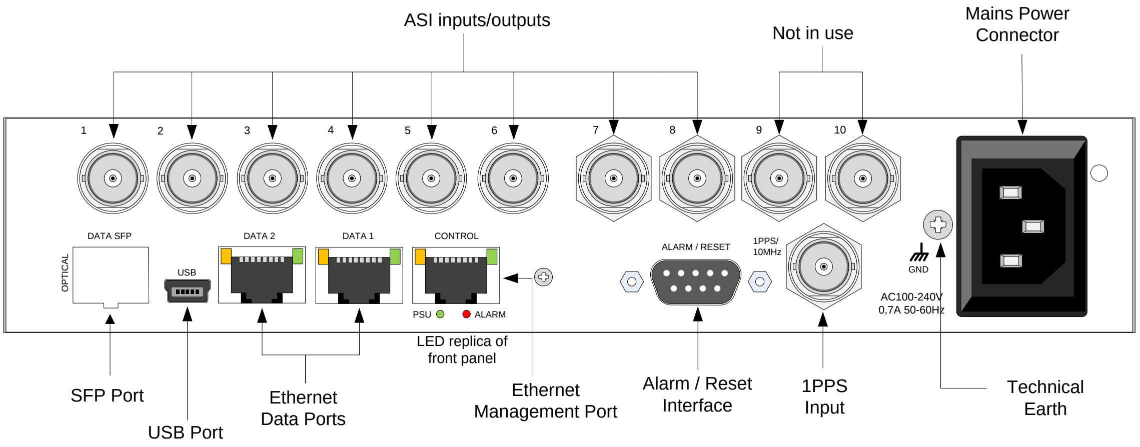


Figure 7.1 Rear panel

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

7.1 ASI ports

The TVG425 ASI ports can be configured as inputs or outputs. The number of available ports depends on the hardware installed and the software licence, and may be between 1 and 10. Enabled ports start at number 1 up to the number of ports ordered. When the number of ports available is 8 or less, each port may be freely programmed as an input or output. So far the ports 9 and 10 aer not in use in the actual software version of the TVG425.

For physical specification of the ASI ports, please refer to **Appendix B: Technical Specification**.

7.1.1 ASI input ports

Inputs signals connected to the ASI ports should DVB or ATSC compliant transport streams, depending on the selected setting (see **Chapter 9**).

On the unit delivered with 8 ASI ports, each ASI input port has two LEDs associated with it. The yellow LED indicates active input and the green LED indicates that sync is detected. Note that these LEDs aer not present on the 10 ASI variant

Table 7.2 ASI Input LED description for the 8 ASI port variant

LED	Colour	Description
Upper	yellow	Lit when input is enabled, unlit otherwise.
Lower	green	Lit when input is in sync, unlit if not in sync.

7.1.2 ASI output ports

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

On the 8 units with 8 ASI ports, one LED is used for each ASI output port: A green LED is lit whenever the output is enabled.

Table 7.3 ASI Output LED description

LED	Colour	Description
Lower	green	Lit when output is enabled, unlit otherwise.
Upper		Not in use for outputs

7.2 1 PPS Input

In order to achieve exact output bitrate control the TVG425 may be externally synchronised. An optional interface module provides an input connector for a 1 PPS synchronisation signal for the internal system clock. The typical application is in an SFN (Single Frequency Network) system, where a transport stream received over IP at several locations may be sent out on ASI connectors in each location at the exact same rate, determined by a common external synchronising signal.

The signal is:

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

For physical parameters of the 1 PPS port, see appendix **B.6.1**.

7.3 Ethernet data ports

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

For flexibility, the TVG425 provides an optional SFP (Small Form-Factor Pluggable) slot to accommodate a copper or optical interface SFP, allowing customers to use different SFPs for special distance, cost, existing infrastructure and future expansion requirements. The TVG425 is prepared for electrical (1000Base-T) or optical 1000BASE-SX and 1000BASE-LX SFP transceivers. When the SFP module is in use Ethernet port Data2 is no longer available.

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

Table 7.4 Ethernet data port LEDs

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

Note: The TVG425 interface to the SFP slot is always Gigabit Ethernet. Other bitrates are not supported.

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

7.4 Ethernet management port

The TVG425 provides one Ethernet port for control and management. The default port setting is Auto sense, 10 or 100 Mbit/s. Connect the management port to the management network. The LEDs for the management port indicate as follows:

Table 7.5 Ethernet management port LEDs

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

7.5 Power supply

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

7.6 Technical earth

Connect the Technical earth to a suitable earth point.

7.6.1 Alarm/Reset connector

The unit is equipped with a 9-pin male DSub connector to provide alarm information.

Two programmable relays are provided. The first relay is always activated on a critical alarm or when the unit is not powered. Please refer to section 9.4.2.3 for a description how to program the relays.

The pin-out of the connector is shown in table 7.6.

Table 7.6 Alarm/Reset connector pin out

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

When there is a *critical* (level 6) alarm in the unit, if the unit is not powered or if any other programmed condition for relay 1 is satisfied there will be a connection between pin 6 and pin 7. When the above conditions are not present there will be a connection between pin 7 and pin 8.

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

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

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

7.6.2 Serial USB interface

The TVG425 provides a USB interface intended for initial IP address setup. The interface conforms to the USB 1.1 specification through a Mini USB connector.

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

8 Operating the Equipment

The TVG425 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 TVG425. As a general rule it is recommended to always use the latest official release of Flash Player (version 10 or newer). If the Flash Player is not installed on the adminstrator PC, a copy is provided on the CD delivered with the device. Alternatively, the latest Adobe Flash Player can be downloaded free of charge from http://www.adobe.com.

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

8.1 Accessing the graphical user interface

The default IP address of the TVG425 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 TVG425 offers two options to alter the user interface IP address; through an Ethernet connection or using a USB terminal interface. If your management computer allows setting a fixed IP address, change the IP address using the Ethernet option described in **Section 8.3.1**.

If a static address cannot be configured on your management computer, **Section 8.3.2** gives the procedure to initially configure device network parameters (IP, netmask, etc...) using the USB terminal interface.

Configuring the device functionality according to operational needs is done using the Web interface, see **Chapter 9**.

8.2 Password protection

Remote access to the device is controlled by password protection. If you access the TVG425 using the USB terminal interface a password is not required.

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

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

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

8.2.1 Resetting the password list

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

```
userdb factory_defaults
```

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

8.3 Changing the IP address of the unit

The TVG425 is supplied with a dedicated management Ethernet port, labeled Control. The default IP configuration (IP address and netmask) of the port is **10.0.0.10/255.255.255.0**.

8.3.1 Changing IP address via the Web GUI

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

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

1. Connect an Ethernet cable directly between the PC and the Ethernet control port of the TVG425. Configure the PC to be on the same sub net as the TVG425. See **Figure 8.2**.

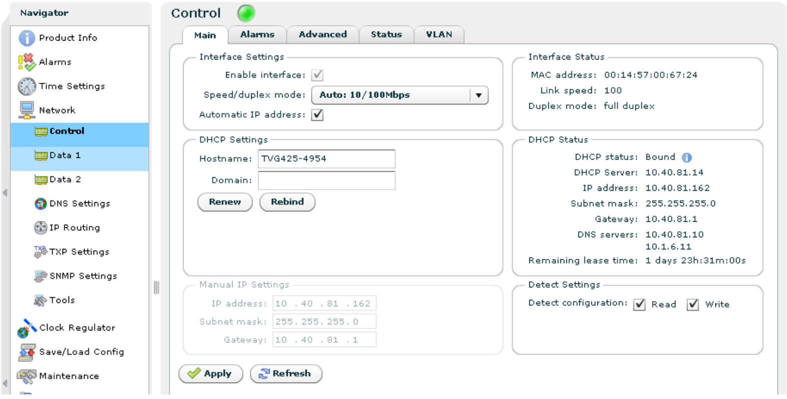
2. Open your web browser and type http://10.0.0.10 in the address field of the browser. Log into the GUI with username **admin** and password **salvador**.

3. Browse to Device Info -> Network -> Control in the GUI, and set the correct IP address settings. Click apply to activate the new parameters. **Figure 8.1** shows this GUI screen.

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

Windows XP example

The screen-shot in **Figure 8.2** shows how to configure the network interface in Windows XP to communicate with the TVG425 with factory default settings. The IP address/netmask is set



Interface Settings

Enable interface: ☑

Speed/duplex mode: Auto: 10/100Mbps

Automatic IP address: ☑

Interface Status

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

Link speed: 100

Duplex mode: full duplex

DHCP Settings

Hostname: TVG425-4954

Domain:

DHCP Status

DHCP status: Bound

DHCP Server: 10.40.81.14

IP address: 10.40.81.162

Subnet mask: 255.255.255.0

Gateway: 10.40.81.1

DNS servers: 10.40.81.10
10.1.6.11

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

Manual IP Settings

IP address: 10 . 40 . 81 . 162

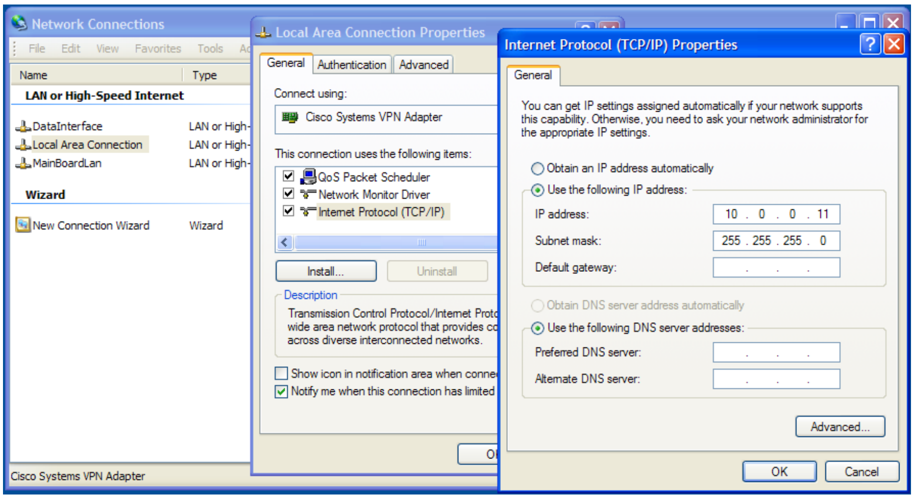
Subnet mask: 255 . 255 . 255 . 0

Gateway: 10 . 40 . 81 . 1

Detect Settings

Detect configuration: ☑ Read ☑ Write

Figure 8.1 Configuring network settings via the Web GUI



Connect using:

Cisco Systems VPN Adapter

This connection uses the following items:

☑ QoS Packet Scheduler

☑ Network Monitor Driver

☑ Internet Protocol (TCP/IP)

Description

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

☐ Show icon in notification area when conne

☑ Notify me when this connection has limited

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 8.2 Setting static IP address 10.0.0.11 in Windows XP

to 10.0.0.11/255.255.255.0 which is on the same sub net as the TVG425, and does not conflict with the IP address of the device.

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

8.3.2 Changing the management port IP address via terminal interface

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

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

2. Connect your computer USB port to the TVG425 USB port using a suitable cable.
3. Access the terminal interface using a suitable terminal program, emulating an ANSI terminal, on your PC (e.g. HyperTerminal). The USB will appear as a virtual COM port on your PC. No specific serial port settings are required. Assure "scroll lock" is not on. Type <enter> and see that you have a prompt (app>).
4. Test that the connection is successful by hitting the <Enter> key. If successfull an >app prompt should be shown.
5. In the terminal, type the following command and press <Enter>:

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

Example:

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

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

Note: The product CD shipped with the TVG425 contains a USB driver to use for serial communication with the device on the USB port. The MS Windows driver installation script is configured to give a one-to-one relationship between the physical USB port number on the PC and the COM port number to use on the PC. Drivers retrieved from http://www.ftdichip.com will also work, but these may not have the same COM port number mapping.

8.3.3 Configuring automatic IP address assignment

The TVG425 can be configured to obtain an IP address automatically from a DHCP server on the network. See section 8.3.1 for how to connect, and section 9.4.4.1.1.1 for how to configure this from the GUI. Alternatively, configure it in the terminal by connecting as in 8.3.2 and issuing the following command:

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

Example:

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

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

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

To disable automatic IP assignment, use the command

```
ipconfig --dhcp 0
```

Note: Hostname registration is only done via the DHCP server, so if DHCP is not enabled the hostname is not registered. The default hostname used is on the format TVG425-`<serial-no>`-`<interface-no>`

8.3.4 Detecting the management port IP address

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

8.3.4.1 USB Interface

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

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

```
app>net ipconfig
```

8.3.4.2 Nevion Detect

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

The Nevion Detect software detects devices by sending broadcast messages that the TVG425 and other Nevion devices will recognize and reply to with some essential information. The PC running Nevion Detect may be on a totally different subnet than the TVG425, such that the device will be discovered regardless of IP addresses and IP submasks.

Warning: Some Ethernet equipment might block broadcast traffic. Connect your PC directly to the TVG425 to avoid this.

Note: It is possible to avoid that the TVG425 is detected by the Nevion Detect software. See **Section 9.4.4.1.1** for details on how to do this.

9 WEB Interface

The TVG425 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 TVG425 and get status information.

9.1 Login

Access the TVG425 by entering its IP address in the address field of your favourite browser. When accessing the TVG425 the first time, the progress bar (**Figure 9.1**) should appear while the Flash application is loading from the device.

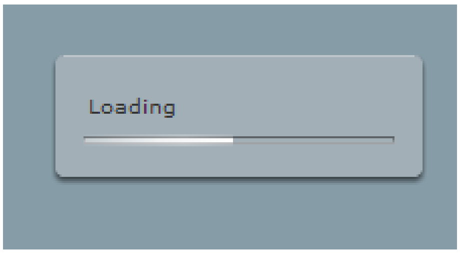
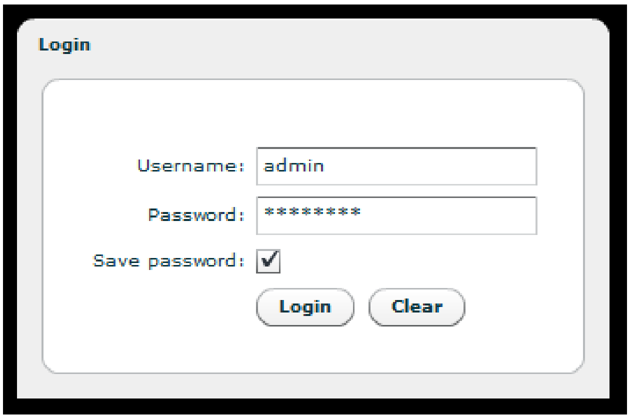


Figure 9.1 Flash application loading

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



Login

Username: admin

Password: ********

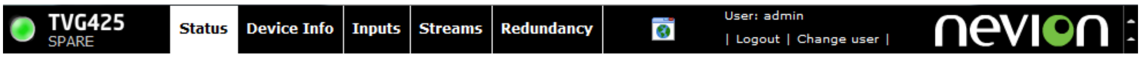
Save password: ☑

Figure 9.2 GUI login window

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

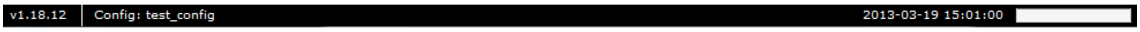
9.2 Status header

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



User: admin

Figure 9.3 The status header


v1.18.12

Config: test_config

2013-03-19 15:01:00

Figure 9.4 The status footer

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

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

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

- A Globe symbol. Clicking this symbol brings up a smaller version of the Status diagram (see **Section 9.3.1**) at the right hand side of the page. This may be un-docked from its location (click the "Pin" symbol) and positioned anywhere on the WEB page. It remains visible until cancelled by clicking the top right-hand **X** or clicking again on the Globe symbol.
- A text showing the current user name.
- A button to log out from the GUI.
- A button to switch current user level.
- The Nevion logo.
- A button for minimising the header. Using this hides a lot of the header information and gives more space for the rest of the page.

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

- The current software version
- The name of the current configuration, if any. See **Section 9.4.1** for details on how to configure this.
- The local device time.
- An activity indicator.

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

A tab bar is located beneath the status header. The exact number of tabs and tab labelling depends on the units operational mode and licences. Clicking a tab will open the corresponding page with a navigation pane to the left as shown in **Figure 9.5**. This pane is used to navigate between sub-pages of the tab.

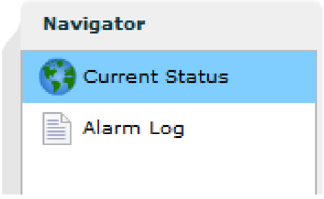


Figure 9.5 Status navigator

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

9.3 Status

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

There are two sub-pages within the status page.

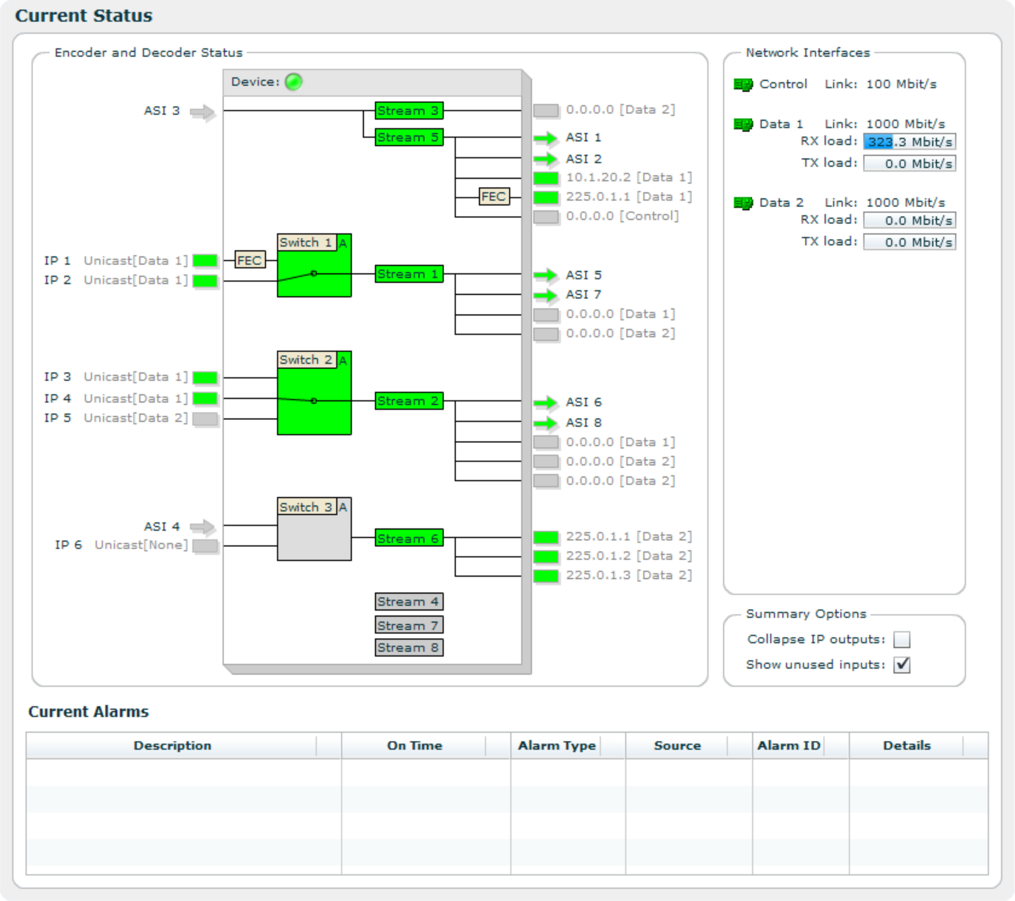
Current Status
: Indicates the running status of the device.

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

9.3.1 Current Status

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

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



Description	On Time	Alarm Type	Source	Alarm ID	Details

Figure 9.6 Current status

- 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.

The precise lay-out of the block diagram depends on the device configuration; partly as a function of the installed options and partly depending on the user's selections. The block diagram shown represents a test set-up to demonstrate a range of configuration possibilities.

The main item in focus in the TVG425 is a Stream, which represents an MPEG2 transport stream. The block diagram shows the input and output channels of the streams and the TVG425 internal routing. As the figure suggests one input transport stream may represent more than one TVG425 Stream. A Stream may be re-directed to different outputs; whether it be ASI or IP interfaces.

If an input switch is defined, it is shown in the status diagram as a box inside the device block in front of a Stream 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.

The *Network Interfaces* field gives an overview of the active network interfaces and indicates dynamically the transmit and receive loads on these interfaces.

The *Summary Options* field provides options to modify the appearance of the block diagram.

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 TVG425.

Subid2

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

Alarm ID

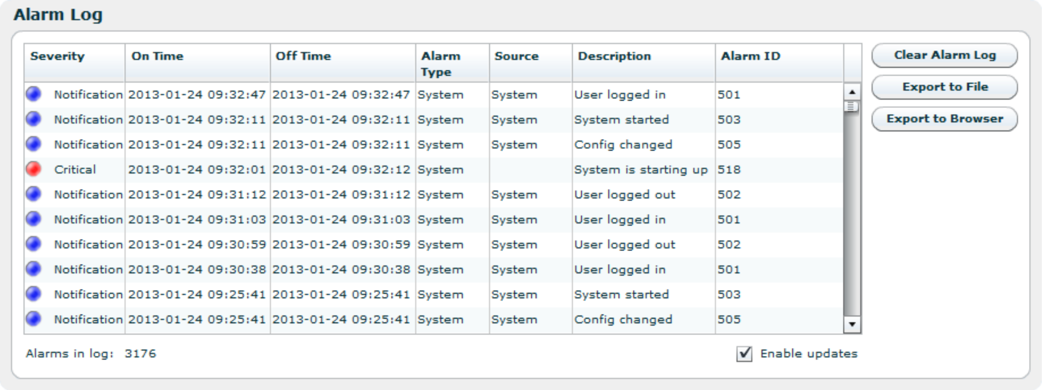
Each alarm condition has an associated numerical alarm ID.

Details

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

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

9.3.2 Alarm log



Alarm Log

Severity	On Time	Off Time	Alarm Type	Source	Description	Alarm ID
● Notification	2013-01-24 09:32:47	2013-01-24 09:32:47	System	System	User logged in	501
● Notification	2013-01-24 09:32:11	2013-01-24 09:32:11	System	System	System started	503
● Notification	2013-01-24 09:32:11	2013-01-24 09:32:11	System	System	Config changed	505
● Critical	2013-01-24 09:32:01	2013-01-24 09:32:12	System		System is starting up	518
● Notification	2013-01-24 09:31:12	2013-01-24 09:31:12	System	System	User logged out	502
● Notification	2013-01-24 09:31:03	2013-01-24 09:31:03	System	System	User logged in	501
● Notification	2013-01-24 09:30:59	2013-01-24 09:30:59	System	System	User logged out	502
● Notification	2013-01-24 09:30:38	2013-01-24 09:30:38	System	System	User logged in	501
● Notification	2013-01-24 09:25:41	2013-01-24 09:25:41	System	System	System started	503
● Notification	2013-01-24 09:25:41	2013-01-24 09:25:41	System	System	Config changed	505

Alarms in log: 3176

☑ Enable updates

Figure 9.7 Alarm log

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

The table consists of the same columns as the Current Alarms table, but does not show details by default. You can change which columns to show, including the details column, in **Section 9.4.2.4**. Additionally a column named Off Time shows the time the alarm condition was cleared. Rows will not have the Off Time set if the alarm is still active.

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

Sequence #

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

SubID 1

The primary numerical index of the alarm instance. This index is reserved for future use and is always set to 1 in the TVG425.

SubID 2

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

SubID 3

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

Details

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

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

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

Clear Alarm Log

Clears all alarms from the alarm log.

Export to File

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

Export to Browser

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

Enable updates

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

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

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

9.4 Device Info

The device info page contains all the information and settings that are not related to a single input or output port. It is divided into multiple sub pages accessed via the navigation list to the left. In the list of physical interfaces in the navigation list, the currently active interface is shown in bold. See **Figure 9.8**.

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

9.4.1 Product info

The product info page contains general device information.

Name

Configures the current user defined name of the unit. This parameter, together with the management network parameters are used as device identifiers and remain untouched if the unit configuration is changed by loading a different configuration file. See **Section 9.4.6**.

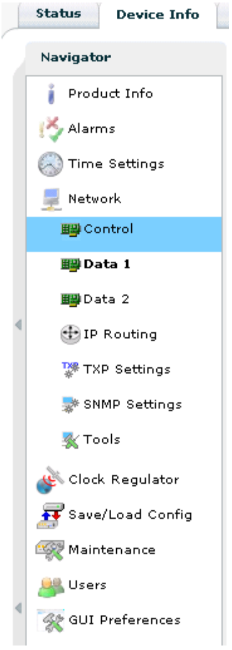
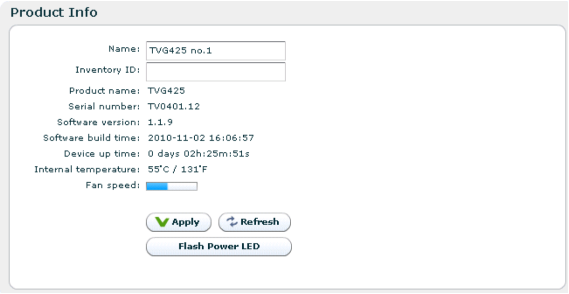


Figure 9.8 Device Info navigator


Product Info

Name:	TVG425 no.1
Inventory ID:	
Product name:	TVG425
Serial number:	TV0401.12
Software version:	1.1.9
Software build time:	2010-11-02 16:06:57
Device up time:	0 days 02h:25m:51s
Internal temperature:	55°C / 131°F
Fan speed:	

Figure 9.9 Product Information

The device name is shown in the web GUI status header (see **Section 9.3.1**), and in the web browser title bar to facilitate identification of each device.

Inventory ID

Configures the current user defined inventory ID of the unit. This parameter, together with the management network parameters are used as device identifiers and remain untouched if the unit configuration is modified. It is only intended as a label/tag and will not affect the operation of the unit.

Configuration ID

Configure a user defined name for the current configuration of the unit. This name will, if given, be diplayed in brackets after the unit name in the status header as shown in **Figure 9.3**. The Configuration ID does not, as opposed to the Name and Inventory ID fields, remain untouched when loading a new unit configuration. Loading a new unit configuration will change the Configuration ID. See **Section 9.4.6** on how to load a new configuration.

Product name

Displays the name of the product as designated by Nevion.

Serial number

The serial number of the device.

Software version

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

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

The convention for the SW version numbering is as follows:

major_version

Incremented for significant SW changes.

minor_version

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

patch_version

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

Software build time

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

Device up time

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

Internal temperature

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

Fan speed

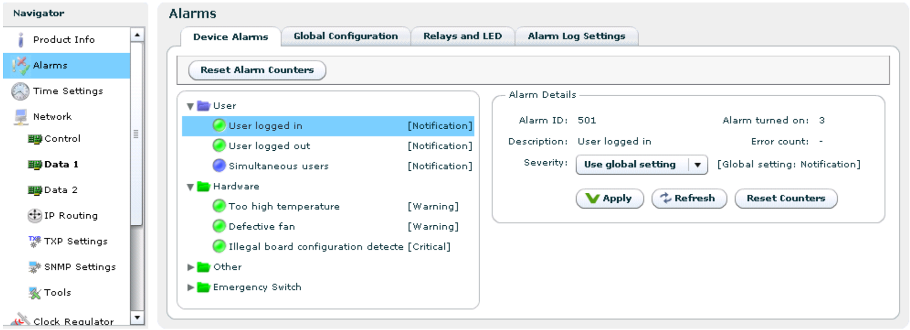
This bar chart shows the current speed of the device fans relative to full speed.

Flash Power LED button

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

9.4.2 Alarms

The Alarms page is shown in **Figure 9.10**:



```
▼ User
    User logged in                      [Notification]
    User logged out                     [Notification]
    Simultaneous users                  [Notification]
▼ Hardware
    Too high temperature                [Warning]
    Defective fan                       [Warning]
    Illegal board configuration detecte [Critical]
▶ Other
▶ Emergency Switch
```

Alarm Details

Alarm ID: 501 Alarm turned on: 3

Description: User logged in Error count: -

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

Figure 9.10 Alarm configuration

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

It gives access to the following sub pages:

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

9.4.2.1 Device alarms

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

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

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

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

Description
: Brief description of the alarm.

Severity
: A configurable option defining the severity of the alarm. Options in the pull-down box range between Filtered (meaning ignored) to Critical. The text in brackets represents the default setting.

Alarm turned on

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

Error count

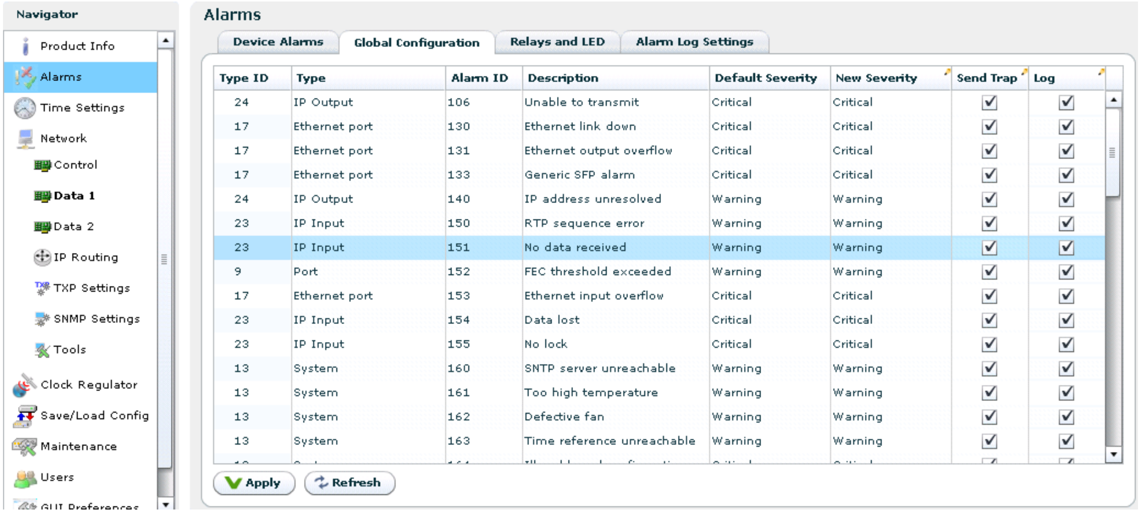
Not used.

'Reset Counters' button

When clicked, clears the alarm counters for the current alarm.

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

9.4.2.2 Global configuration



Type ID	Type	Alarm ID	Description	Default Severity	New Severity	Send Trap	Log
24	IP Output	106	Unable to transmit	Critical	Critical	☑	☑
17	Ethernet port	130	Ethernet link down	Critical	Critical	☑	☑
17	Ethernet port	131	Ethernet output overflow	Critical	Critical	☑	☑
17	Ethernet port	133	Generic SFP alarm	Critical	Critical	☑	☑
24	IP Output	140	IP address unresolved	Warning	Warning	☑	☑
23	IP Input	150	RTP sequence error	Warning	Warning	☑	☑
23	IP Input	151	No data received	Warning	Warning	☑	☑
9	Port	152	FEC threshold exceeded	Warning	Warning	☑	☑
17	Ethernet port	153	Ethernet input overflow	Critical	Critical	☑	☑
23	IP Input	154	Data lost	Critical	Critical	☑	☑
23	IP Input	155	No lock	Critical	Critical	☑	☑
13	System	160	SNTP server unreachable	Warning	Warning	☑	☑
13	System	161	Too high temperature	Warning	Warning	☑	☑
13	System	162	Defective fan	Warning	Warning	☑	☑
13	System	163	Time reference unreachable	Warning	Warning	☑	☑

Figure 9.11 Global alarm configuration

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

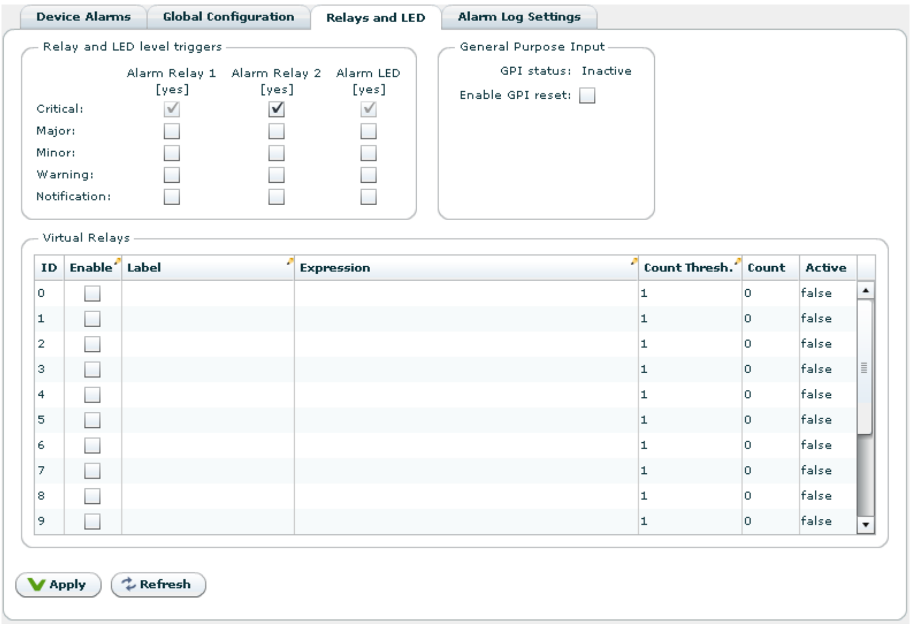
For each alarm a custom severity level can be configured. In addition the alarms can be omitted from the alarm log and trap transmission.

Edited rows are highlighted until changes have been applied.

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

9.4.2.3 Relays and LED

This page lets the user configure the alarm severity level that shall turn the 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.



Relay and LED level triggers

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

General Purpose Input

GPI status: Inactive

Enable GPI reset: □

Virtual Relays

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

Figure 9.12 Relays and LED configuration

The General purpose input field allows the user to enable pin 9 of the alarm D-SUB connector as a remote reset input. See **Section 7.6.1**. GPI status indicates if the input signal is active.

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

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

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

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

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

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

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

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

Table 9.1 Legal field values to use in expressions

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

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

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

Table 9.2.a Legal operators to use in expressions

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

Table 9.2.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 9.3.

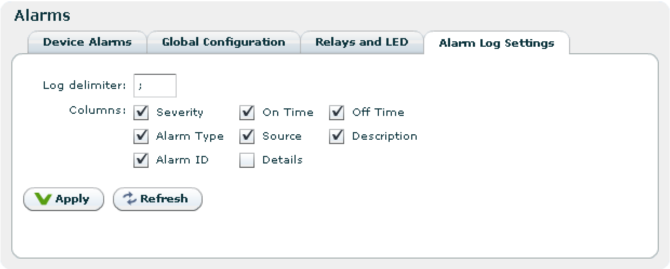
Table 9.3 Expression examples

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

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

9.4.2.4 Alarm log settings

This page is used to set alarm log properties.



Log delimiter: ;

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

Figure 9.13 Configuring the alarm log

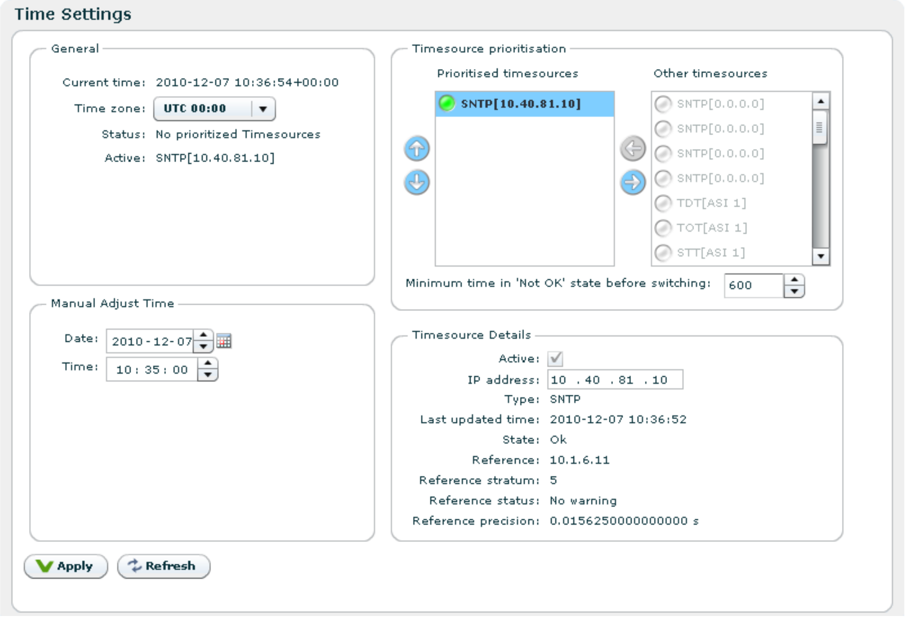
Log delimiter

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

Columns

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

9.4.3 Time Settings



Time Settings

General

Current time: 2010-12-07 10:36:54+00:00

Time zone: UTC 00:00

Status: No prioritized Timesources

Active: SNTP[10.40.81.10]

Timesource prioritisation

Prioritised timesources

● SNTP[10.40.81.10]

Other timesources

○ SNTP[0.0.0.0]
○ SNTP[0.0.0.0]
○ SNTP[0.0.0.0]
○ SNTP[0.0.0.0]
○ TDT[ASI 1]
○ TOT[ASI 1]
○ STT[ASI 1]

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

Manual Adjust Time

Date: 2010 - 12 - 07

Time: 10 : 35 : 00

Timesource Details

Active: ☑

IP address: 10 . 40 . 81 . 10

Type: SNTP

Last updated time: 2010-12-07 10:36:52

State: Ok

Reference: 10.1.6.11

Reference stratum: 5

Reference status: No warning

Reference precision: 0.0156250000000000 s

Figure 9.14 Time Settings

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

The page consists of 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

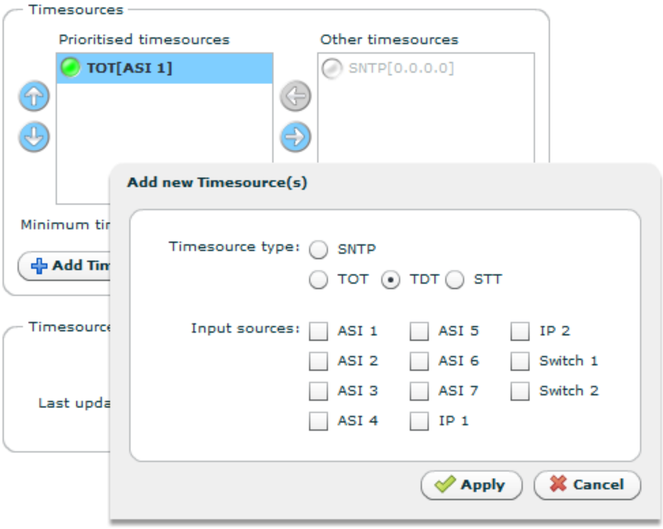
The status of the time synchroniser.

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



Timesource type: ○ SNTP ○ TOT ● TDT ○ STT

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

Figure 9.15 Time Settings - Add time source

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

Timesource type

SNTP
: Time source retrieving time from an SNTP server.

Server address
: Specify the server IP address here.

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

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

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

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

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

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

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

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

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

State
: The current state of the time source.

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

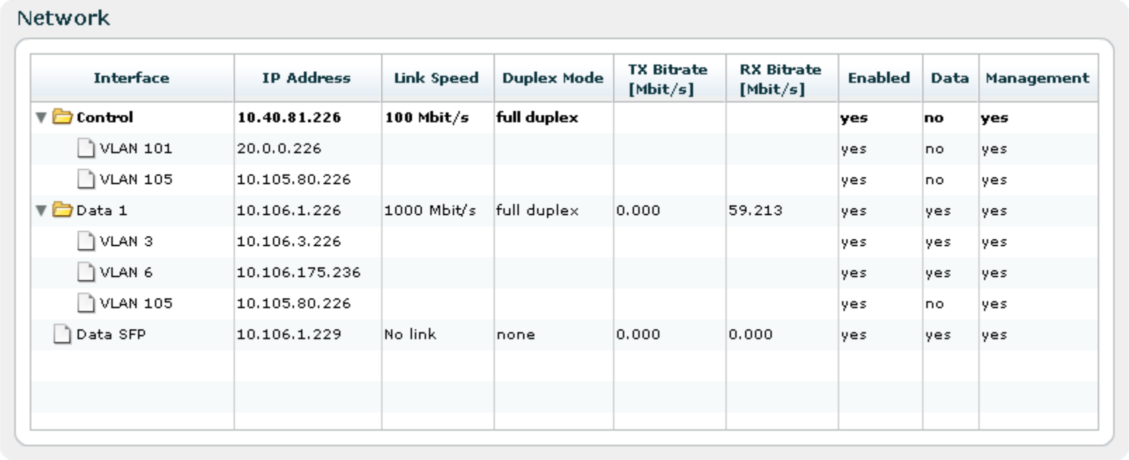
Reference stratum
: Indicates the hierarchy level of the current time source. The master reference is at stratum 0 (highest).

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

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

9.4.4 Network

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.



Network

Interface	IP Address	Link Speed	Duplex Mode	TX Bitrate [Mbit/s]	RX Bitrate [Mbit/s]	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	0.000	59.213	yes	yes	yes
VLAN 3	10.106.3.226					yes	yes	yes
VLAN 6	10.106.175.236					yes	yes	yes
VLAN 105	10.105.80.226					yes	no	yes
Data SFP	10.106.1.229	No link	none	0.000	0.000	yes	yes	yes

Figure 9.16 Network status

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

IP Address
: The IP address configured for this interface.

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

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

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

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

Enabled
: Shows whether the interface is currently enabled.

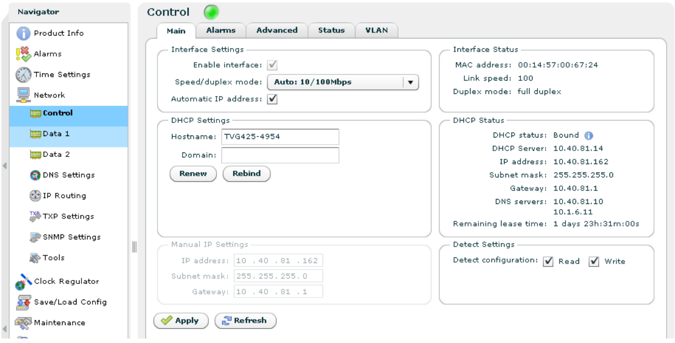
Data
: Shows whether data traffic is currently enabled for this interface.

Management
: Shows whether management traffic is currently enabled for this interface.

9.4.4.1 Interfaces

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

9.4.4.1.1 Main



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

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

DHCP Settings
Hostname: TVG425-4954
Domain:

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

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

Detect Settings
Detect configuration: ☑ Read ☑ Write

Figure 9.17 Main IP settings

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

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

9.4.4.1.2 Interface Settings

Enable interface

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

Speed/duplex mode

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

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

Automatic IP address

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

9.4.4.1.3 DHCP Settings

Hostname

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

Domain

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

Renew button

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

Rebind button

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

9.4.4.1.4 DHCP Status

DHCP status

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

Possible values are:

Disabled

DHCP is not turned on.

Selecting

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

Bound

Client has received IP settings and is ready for use.

Renewing

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

Rebinding

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

Checking

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

Backing off
Client received a nack from the server.

DHCP server
The IP of the selected server.

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

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

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

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

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

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

DHCP status info icon

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

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

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

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

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

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

Last transmission ID
ID used on last DHCP message transmitted.

9.4.4.1.5 Manual IP Settings

IP address
: IP address of the interface.

Subnet mask
: The subnet mask of the interface.

Gateway
: The default gateway address for the interface.

9.4.4.1.6 Interface Status

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

Link speed
: Speed of current connection.

Duplex mode
: Shows duplex of current connection.

9.4.4.1.7 Detect Settings

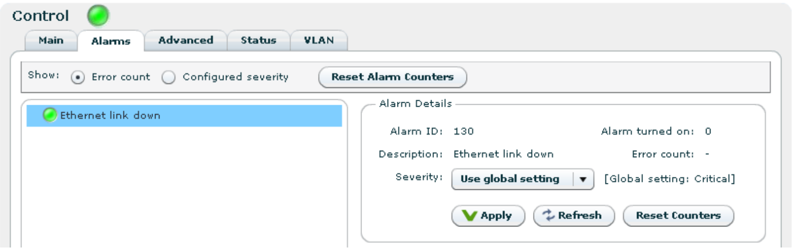
Detect configuration
: Applies to the Control interface, only.

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

Enabling the Read option makes the TVG425 visible for the Nevion Detect on the LAN. If the Write option is enabled the IP address of the TVG425 may be configured using the Nevion Detect. These options do not affect the operation of the device from the management application Nevion Connect.

9.4.4.1.8 Alarms

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



Show: ● Error count ○ Configured severity

Ethernet link down

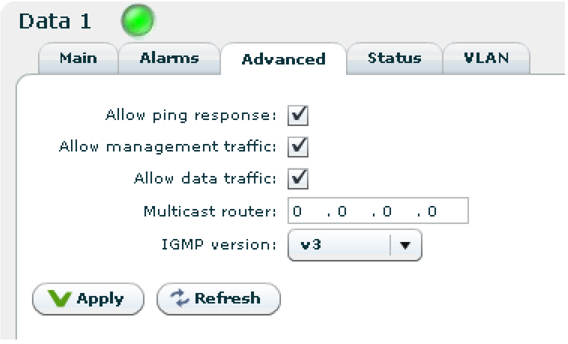
Alarm ID: 130
Alarm turned on: 0
Description: Ethernet link down
Error count: -
Severity: Use global setting ▾ [Global setting: Critical]

Figure 9.18 Network interface alarms

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

9.4.4.1.9 Advanced

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



Allow ping response: ☑
Allow management traffic: ☑
Allow data traffic: ☑
Multicast router: 0 . 0 . 0 . 0
IGMP version: v3

Figure 9.19 Advanced IP settings

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

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

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

Multicast router
: *This parameter is not shown in the management interface page.*

The IP address of the multicast router. The address here is used in conjunction with the Use multicast router option in the "IP Output" page, **Section 9.6.5.1**.

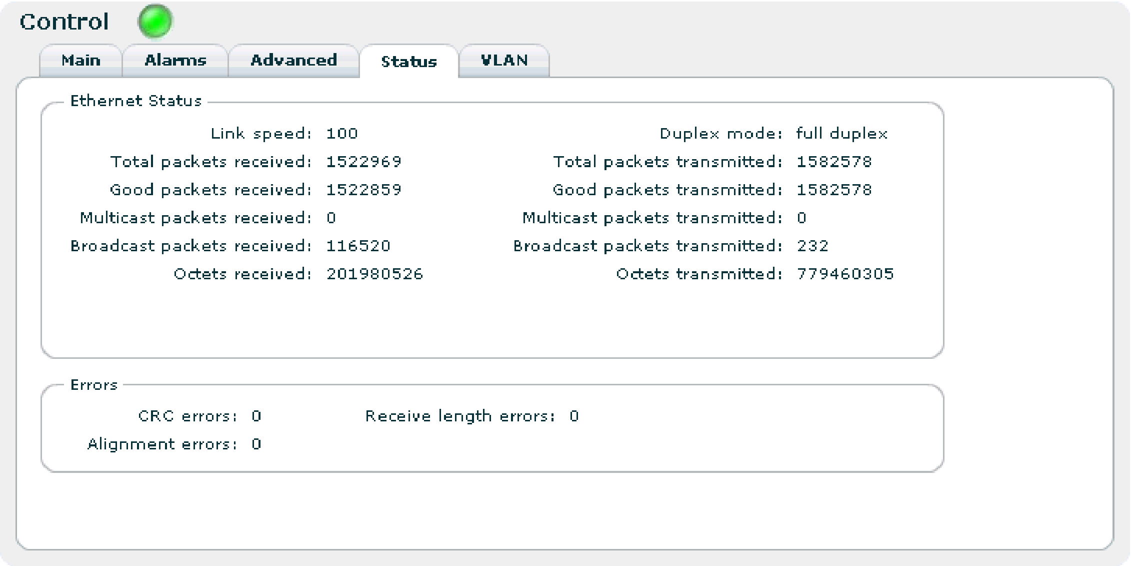
IGMP version
: *This parameter is not shown in the management interface page.*

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

9.4.4.1.10 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:



Ethernet Status

Link speed:	100	Duplex mode:	full duplex
Total packets received:	1522969	Total packets transmitted:	1582578
Good packets received:	1522859	Good packets transmitted:	1582578
Multicast packets received:	0	Multicast packets transmitted:	0
Broadcast packets received:	116520	Broadcast packets transmitted:	232
Octets received:	201980526	Octets transmitted:	779460305

Errors

CRC errors:	0	Receive length errors:	0
Alignment errors:	0		

Figure 9.20 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.

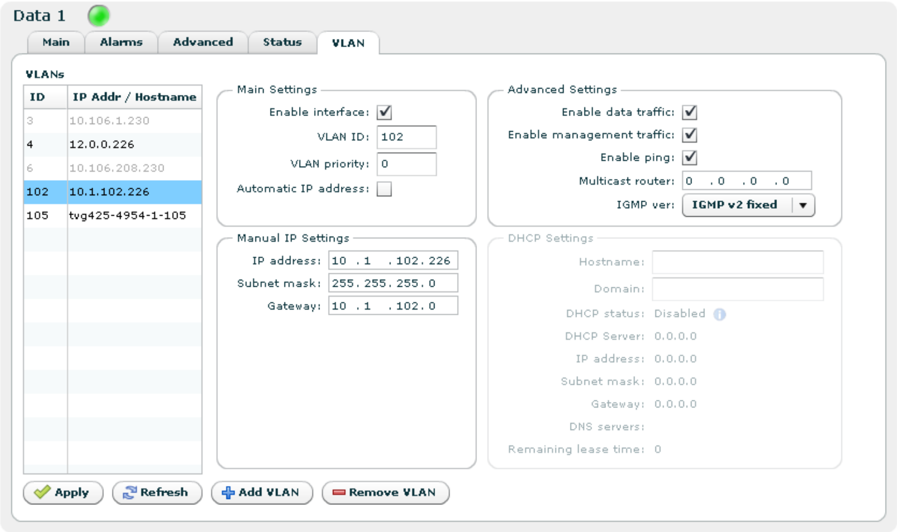
Alignment errors
Number of packets detected with alignment errors (non-integer number of bytes).

Receive errors
Number of erroneous packets received.

Missed packets
Number of packets missed.

Receive length errors
Number of packets with invalid size.

9.4.4.1.11 VLAN



VLANs

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

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

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

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

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

Figure 9.21 VLAN configuration

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

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

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

9.4.4.1.12 Main Settings

Enable interface
Enable/disable the virtual interface.

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

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

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

9.4.4.1.13 Manual IP Settings

IP address
The IP address of the virtual interface.

Subnet mask
The subnet mask of the virtual interface.

Gateway
The gateway address to use for the virtual interface.

9.4.4.1.14 Advanced Settings

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

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

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

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

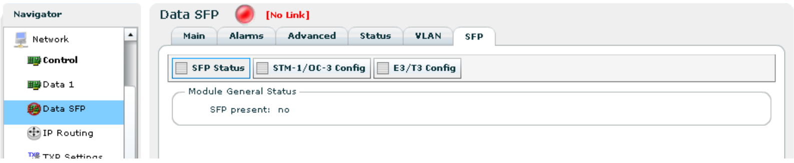
IGMP ver
Provides selection of the IGMP version to use. *Not applicable to the "Control" interface.*

9.4.4.1.15 DHCP settings and status

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

9.4.4.1.16 SFP

The SFP tab is visible for the second network interface if this interface is set to use SFP. How to enable the SFP is described in section 9.4.7.1 , provided the appropriate licence has been installed .



SFP present: no

Figure 9.22 The Device Info > Network > SFP tab

The SFP tab gives access to three sub-pages: SFP Status, STM-1/OC-3 Config and E3/T3 Config. The two configuration sub-pages reflect that separate configuration files are used to configure the different SFP module types. For each module type the TVG425 stores a configuration file that can be edited “off-line”. These pages are visible only if SFP configuration has been licensed. The settings will not be committed to the module until writing of the file is expressly initiated.

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

The Module General Status field displays the status of the module as seen by the TVG425.

SFP Present
: Indicates that the module has been detected by the TVG425.

Vendor
: Shows the vendor name.

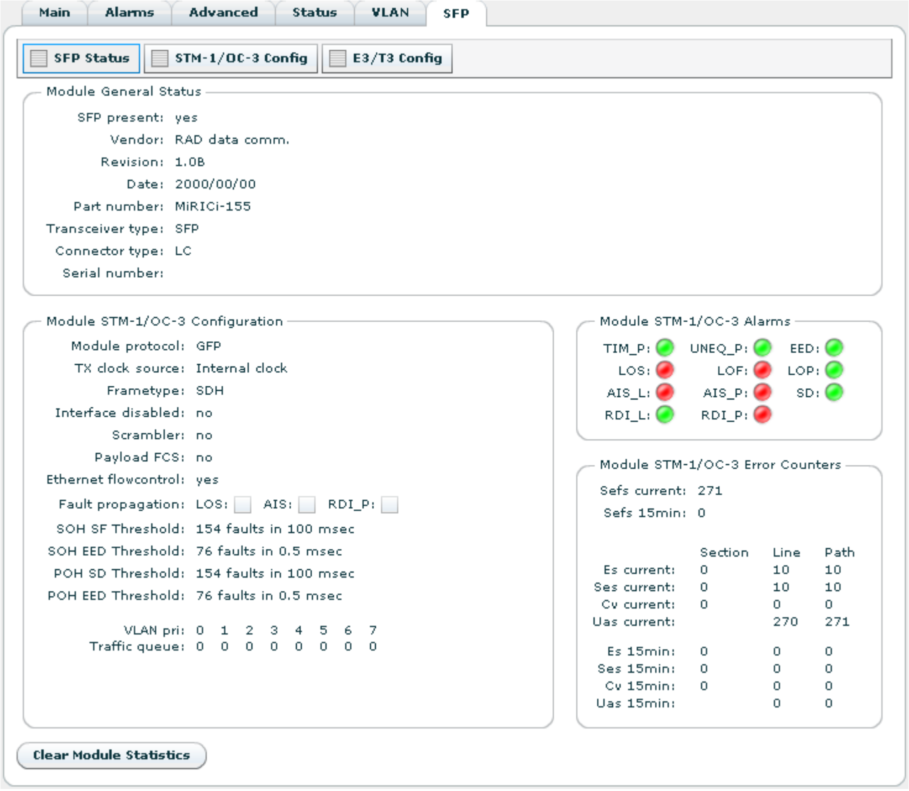
Revision
: Indicates the module revision.

Date
: Indicates the revison date.

Part number
: The module part number.

Transceiver type
: The type of transceiver inside the SFP module. Only a limited range of transceivers is compatible with the TVG425.

Connector type
: Indicates the network connector type.



Module General Status

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

Module STM-1/OC-3 Configuration

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

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

Module STM-1/OC-3 Alarms

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

Module STM-1/OC-3 Error Counters

Sefs current: 271
Sefs 15min: 0

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

Figure 9.23 The SFP status page

Serial number
: The serial number of the SFP module.

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

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

TIM-P
: Trace ID Mismatch (Path)

LOS
: Loss of Signal

AIS_L
: Alarm Indication Signal (Line)

RDI_L
: Remote Defect Indication (Line)

UNEQ_P
: Payload Label Mismatch (Path)

LOF
: Loss of Frame

AIS_P
: Alarm Indication (Path)

RDI_P
: Remote Defect Indication (Path)

EED
: Excessive Error Defect

LOP
: Loss of Point

SD
: Signal Degrade

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

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

BV
: Bipolar Violation

LCV
: Line Coding Violation

LOS
: Loss of Signal

RDI
: Remote Detection Indication

WLD
: WAN Loop Detected

EZ
: Excessive Zeroes

PCV
: P-bit Coding Violation

OOF
: Out of Frame

LLD
: Lan Loop Detected

LOL
: LIU Out of Lock

CCV
: C-bit Coding Violation

AIS
: Alarm Indication Signal

SS
: System Status.

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

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

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

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

  Section
  : "Section" related error counts

  Line
  : "Line" related error counts

  Path
  : "Path" related error counts

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

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

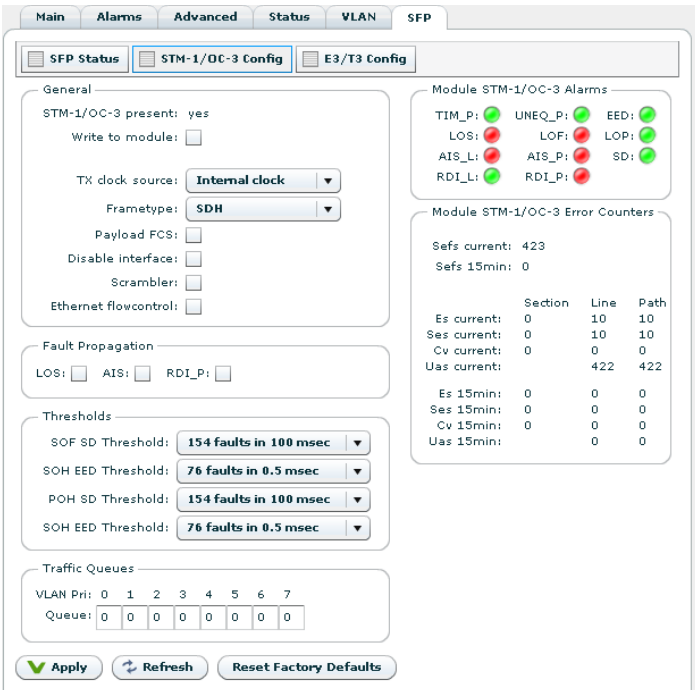
The STM-1/OC-3 module provides an optical interface for high speed data communications in SDH or SONET networks. This page provides access to change the configuration settings of the module. As shown in figure **Figure 9.24** the page contains four fields to set operational parameters. The Alarms and Error counters fields are identical to those described for the SFP Status sub-page. Editing the configuration settings will alter the SFP configuration file stored in the TVG425, 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 TVG425.

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.



General

STM-1/OC-3 present: yes

Write to module: □

TX clock source: Internal clock

Frametype: SDH

Payload FCS: □

Disable interface: □

Scrambler: □

Ethernet flowcontrol: □

Fault Propagation

LOS: □ AIS: □ RDI_P: □

Thresholds

SOF SD Threshold: 154 faults in 100 msec

SOH EED Threshold: 76 faults in 0.5 msec

POH SD Threshold: 154 faults in 100 msec

SOH EED Threshold: 76 faults in 0.5 msec

Traffic Queues

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

Module STM-1/OC-3 Alarms

TIM_P: 🟢 UNEQ_P: 🟢 EED: 🟢

LOS: 🔴 LOF: 🔴 LOP: 🟢

AIS_L: 🔴 AIS_P: 🔴 SD: 🟢

RDI_L: 🟢 RDI_P: 🔴

Module STM-1/OC-3 Error Counters

Sefs current: 423

Sefs 15min: 0

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

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

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

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

Disable interface
: Not available.

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

Ethernet flow control
: A tick enables flow control of Ethernet data from the TVG425 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 Taffic Queues field allows mapping of network traffic queues to VLAN priorities. For information on VLAN priority usage refer to [7].

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

At the bottom of the page are three buttons:

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

Refresh
: Cancels changes that have been entered.

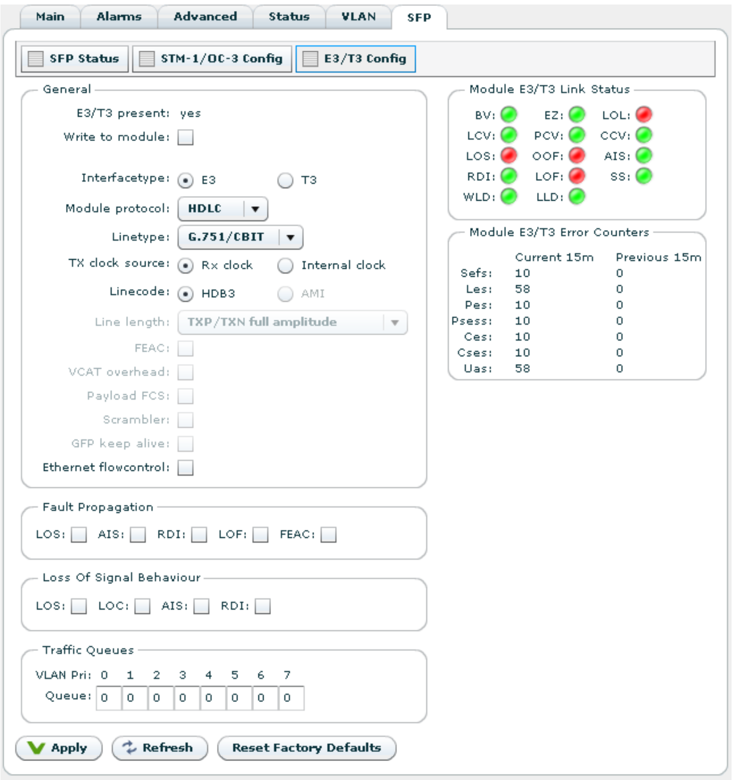
Reset Factory Defaults
: Only active if the Write to module box has not been ticked. Clicking this button returns the module to factory default settings but will not affect the settings of the configuration page. The status of the SFP module is at all times displayed in the SFP Status sub-page.

The **E3/T3 Config** page.

The E3T3 module provides an electrical interface for high speed data communications in E3 or T3 networks. This page provides access to change the configuration settings of the module. As shown in figure **Figure 9.25** the page contains four fields to set operational parameters. Editing the configuration settings will alter the SFP configuration file stored in the TVG425, only.

E3/T3 present
: Indicates if the module has been detected by the TVG425.

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



General

E3/T3 present: yes
Write to module: □

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

Module E3/T3 Link Status

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

Module E3/T3 Error Counters

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

Fault Propagation

LOS: □ AIS: □ RDI: □ LOF: □ FEAC: □

Loss Of Signal Behaviour

LOS: □ LOC: □ AIS: □ RDI: □

Traffic Queues

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

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

the box is checked the configuration file is written to the module every time the Apply button is clicked.

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

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

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

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

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

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

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

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

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

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

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

Ethernet flow control
: A tick enables flow control of Ethernet data from the TVG425 to the SFP module. Flow control prevents data overflow in the SFP module buffer. Buffer overflow leads to data loss that would go unnoticed until attempting to decode the data at the receiving end.

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

LOS
: Loss of signal

AIS
: Alarm indication signal

RDI
: Remote defect indication

LOF
: Loss of frame

FEAC
: Far end alarm and control

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

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

LOS
: Loss of signal

LOC
: Receive loss of lock

AIS
: Alarm indication signal

RDI
: Remote defect indication

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

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

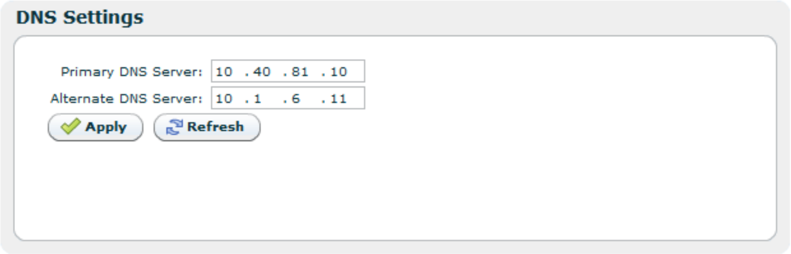
At the bottom of the page are three buttons:

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

Refresh
: Cancels changes that have been entered.

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

9.4.4.2 DNS Settings



DNS Settings

Primary DNS Server: 10 .40 .81 .10

Alternate DNS Server: 10 .1 .6 .11

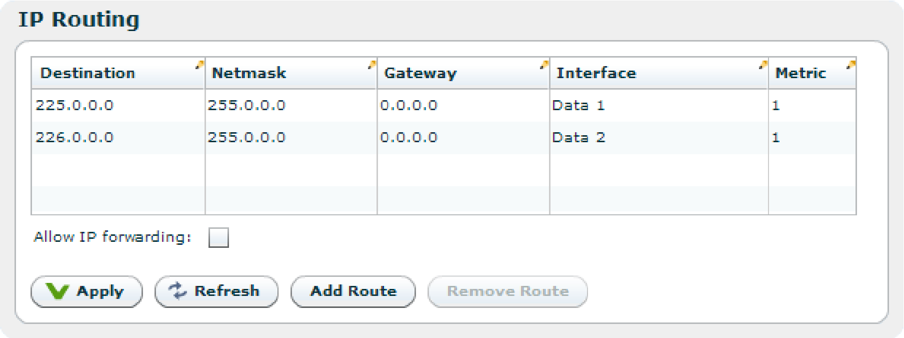
Figure 9.26 DNS settings

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

9.4.4.3 IP Routing

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.



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

Allow IP forwarding: □

Figure 9.27 IP Routing

Netmask

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

Gateway

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

Interface

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

Metric

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

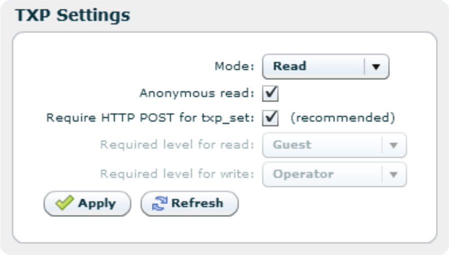
When an IP packet is sent from the unit the destination address of the packet is matched against the configured routing rules. If the destination address matches one or more rules the rule with the lowest metric will be used. The packet will then be forwarded to the interface determined by this rule.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

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

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

9.4.4.4 TXP Settings

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



TXP Settings

Mode: Read

Anonymous read: ☑

Require HTTP POST for txp_set: ☑ (recommended)

Required level for read: Guest

Required level for write: Operator

Figure 9.28 TXP Settings

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

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

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

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

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

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

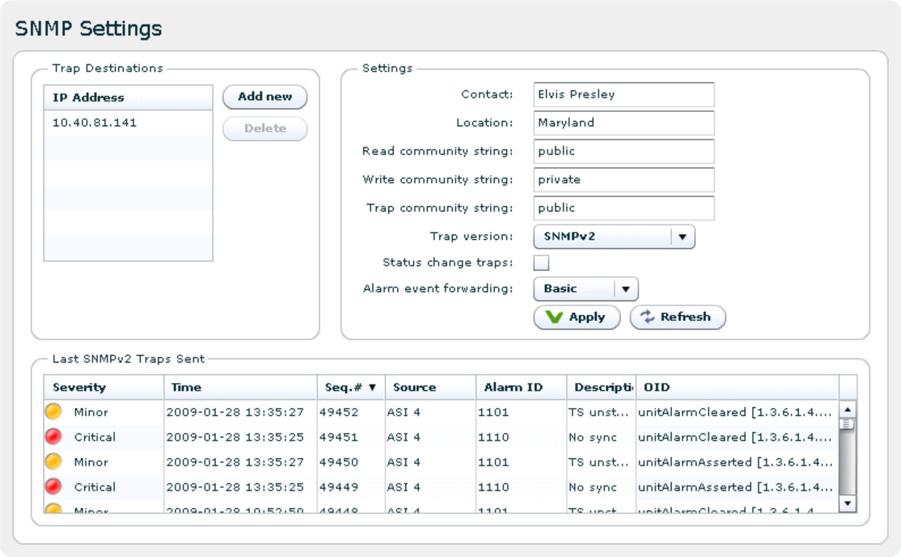
Below follows a simple example of how to get the units uptime.

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

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

9.4.4.5 SNMP Settings

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



SNMP Settings

Trap Destinations

IP Address
10.40.81.141

Settings

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

Last SNMPv2 Traps Sent

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

Figure 9.29 SNMP Settings

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

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

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

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

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

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

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

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

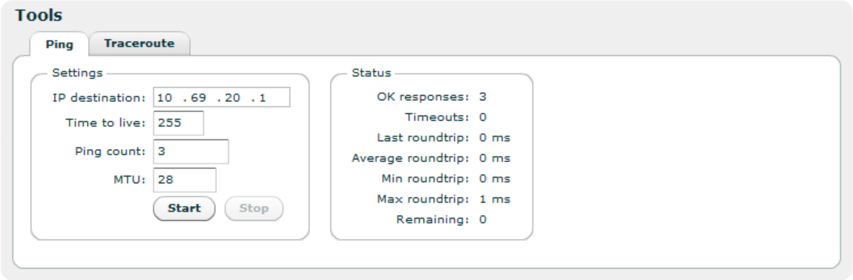
For more information about the configuration settings for SNMP, please refer to **Section 10.4** in **Chapter 10: SNMP**.

9.4.4.6 Tools

The tools menu contains helpfull tools for network debugging.

9.4.4.6.1 Ping

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



Settings

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

Status

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

Figure 9.30 The Ping tool

IP destination

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

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

TTL (Time To Live)

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

Ping count

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

MTU

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

Start

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

OK responses

The number of ping responses received.

Timeouts

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

Last roundtrip

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

Average roundtrip

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

Min roundtrip

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

Max roundtrip

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

Remaining

The number of remaining ping requests in this session.

9.4.4.6.2 Traceroute

The traceroute tool can be used to debug the network connectivity with a given host by tracking the router hops between the TVG425 and the host. Traceroute uses ICMP ping messages with increasing TTL to track the router hops.

Settings

IP Destination

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

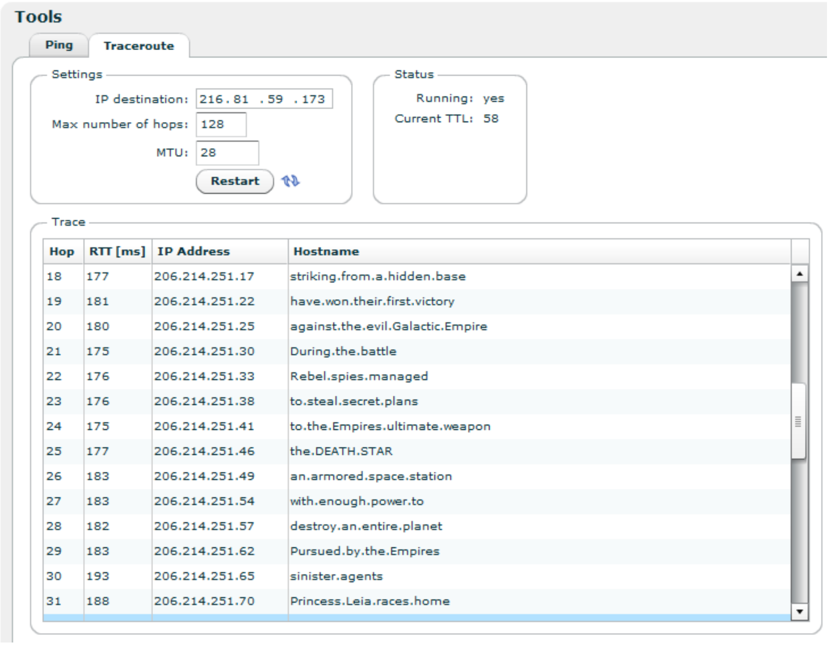
Number of hops

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

MTU

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

Status



Settings

IP destination: 216 . 81 . 59 . 173
Max number of hops: 128
MTU: 28

Status

Running: yes
Current TTL: 58

Trace

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

Figure 9.31 The Traceroute tool

Running
: State of tracer.

Current TTL
: Increasing for each new hop traced.

Trace
: Grid showing routers encountered.

Hop
: Hop number.

RTT[ms]
: Round trip time measured in milliseconds for message returned from router at this point in chain.

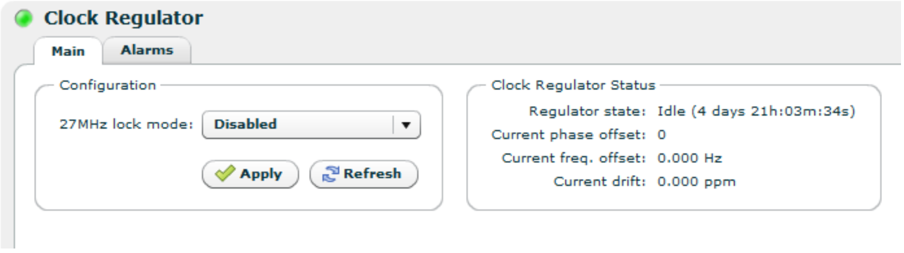
IP Address
: IP address of router at this point.

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

9.4.5 Clock Regulator

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

9.4.5.1 Main



Configuration

27MHz lock mode: Disabled

Clock Regulator Status

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

Figure 9.32 Clock regulator

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

The Configuration field:

27 MHz lock mode

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

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

The Clock Regulator Status field:

Regulator state

Idle
: External reference signal is disabled.

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

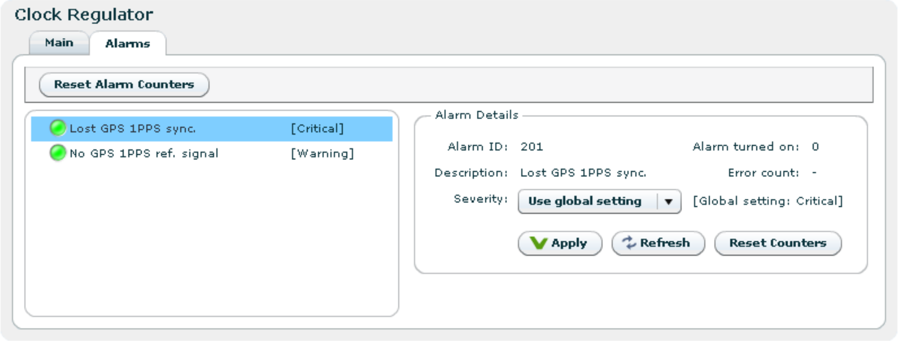
Fine tune
: External Reference signal is enabled, and the internal clock has obtained lock to the reference.

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

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

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

9.4.5.2 Alarms



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

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

Figure 9.33 Clock regulator Alarms

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

9.4.6 Save/Load Config

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

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

9.4.6.1 Save/Load Configs

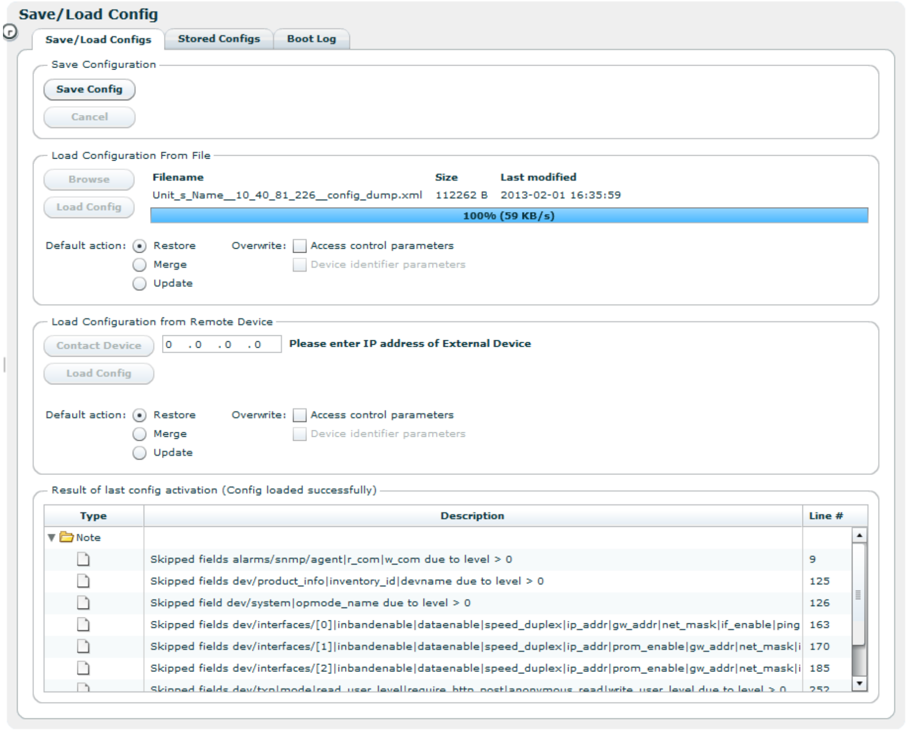
9.4.6.1.1 Save Configuration

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

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

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

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



Filename	Size	Last modified
Unit_s_Name__10_40_81_226__config_dump.xml	112262 B	2013-02-01 16:35:59

100% (59 KB/s)

Default action: ● Restore ○ Merge ○ Update

Overwrite: □ Access control parameters □ Device identifier parameters

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

Default action: ● Restore ○ Merge ○ Update

Overwrite: □ Access control parameters □ Device identifier parameters

Result of last config activation (Config loaded successfully)

Type	Description	Line #
▼ Note		
	Skipped fields alarms/snmp/agent|r_com|w_com due to level > 0	9
	Skipped fields dev/product_info|inventory_id|devname due to level > 0	125
	Skipped field dev/system|opmode_name due to level > 0	126
	Skipped fields dev/interfaces/[0]|inbandenable|dataenable|speed_duplex|ip_addr|gw_addr|net_mask|if_enable|ping	163
	Skipped fields dev/interfaces/[1]|inbandenable|dataenable|speed_duplex|ip_addr|prom_enable|gw_addr|net_mask|i	170
	Skipped fields dev/interfaces/[2]|inbandenable|dataenable|speed_duplex|ip_addr|prom_enable|gw_addr|net_mask|i	185
	Skipped fields dev/tvp|mode|read_user_level|require_http_post|anonymous_read|write_user_level due to level > 0	252

Figure 9.34 Saving and loading of configuration files

9.4.6.1.2 Load Configuration From file

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

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

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

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

By default, options specific to the device, including device name and management port network configuration, are disregarded during the import process. This is a convenience feature allowing configurations to be easily moved from one device to another. It also makes management easier in that the Web UI will continue to communicate with the device after a new configuration has been loaded. The default behaviour can be changed with the load options, please see **Section 9.4.6.1.4** for a desciption of the options.

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

9.4.6.1.3 Load Configuration from Remote Device

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

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

> **Note:** It is possible, but not advisable, to load configuration from other model types. Even if loading from the same model type, loading a configuration might also fail, especially if the two devices have different feature sets. See **Section 9.4.7.1** for a list of features.

Please see next chapter (**Section 9.4.6.1.4**) for a description of the load options.

9.4.6.1.4 Load options

These options are used to modify the behaviour on configuration loading. The options are available both when loading from a file (**Section 9.4.6.1.2**) and when loading from a remove device (**Section 9.4.6.1.3**).

Default action

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

Restore

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

Merge

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

Update

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

Overwrite

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

Access control parameters

Tick to overwrite SNMP community strings and TXP access parameters.

Device identifier parameters

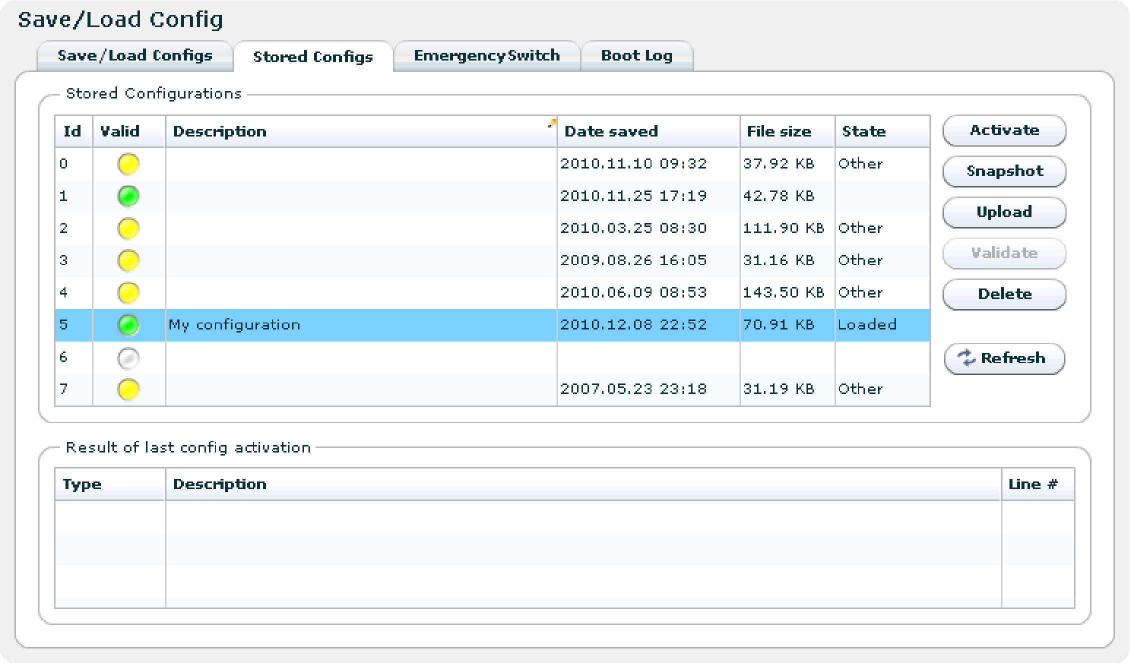
Tick off his check box to overwrite the device identifiers device name and inventory ID. Ethernet Interface IP addresses are not overwritten using this option.

9.4.6.2 Boot Log

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

9.4.6.3 Stored Configs

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



Save/Load Config

Stored Configurations

Id	Valid	Description	Date saved	File size	State
0	🟡		2010.11.10 09:32	37.92 KB	Other
1	🟢		2010.11.25 17:19	42.78 KB	
2	🟡		2010.03.25 08:30	111.90 KB	Other
3	🟡		2009.08.26 16:05	31.16 KB	Other
4	🟡		2010.06.09 08:53	143.50 KB	Other
5	🟢	My configuration	2010.12.08 22:52	70.91 KB	Loaded
6	⚪				
7	🟡		2007.05.23 23:18	31.19 KB	Other

Result of last config activation

Type	Description	Line #

Figure 9.35 Locally stored configuration files

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

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

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

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

Date saved
: Time stamp when the configuration was uploaded to the unit.

File size
: Size of the configuration file.

State
: Extra information regarding the configuration.

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

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

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

Upload
: Import a locally stored configuration file.

Download
: Download selected configuration file to disk.

Delete
: Delete the entry selected in the snapshot list.

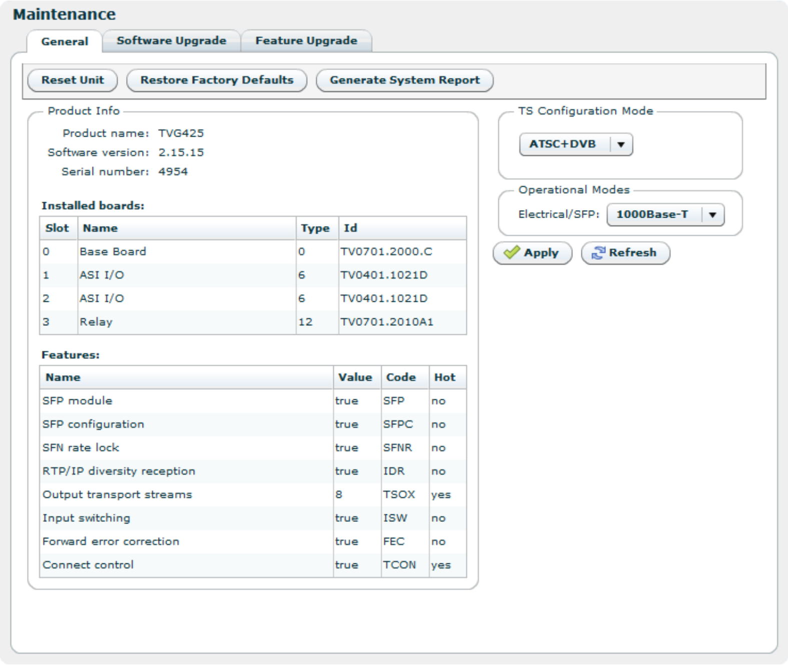
At the bottom of the page is the Results of last config action field, which will show the result of the last action performed.

9.4.7 Maintenance

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

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

9.4.7.1 General



Product Info

Product name: TVG425
Software version: 2.15.15
Serial number: 4954

Installed boards:

Slot	Name	Type	Id
0	Base Board	0	TV0701.2000.C
1	ASI I/O	6	TV0401.1021D
2	ASI I/O	6	TV0401.1021D
3	Relay	12	TV0701.2010A1

Features:

Name	Value	Code	Hot
SFP module	true	SFP	no
SFP configuration	true	SFPC	no
SFN rate lock	true	SFNR	no
RTP/IP diversity reception	true	IDR	no
Output transport streams	8	TSOX	yes
Input switching	true	ISW	no
Forward error correction	true	FEC	no
Connect control	true	TCON	yes

TS Configuration Mode: ATSC+DVB

Operational Modes

Electrical/SFP: 1000Base-T

Figure 9.36 Maintenance

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

At the top are two buttons for resetting purposes:

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

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

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

The Product info field provides the following information:

Product name
: This is the product model name.

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

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

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

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

  Name
  : Name of the feature

  Value
  : State of the feature or number of licenced items

  Code
  : The factory order code used to identify this feature

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

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

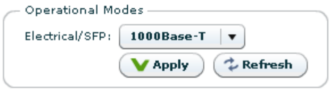
The choices are:

DVB
: DVB transport streams only are accepted.

ATSC+DVB
: Both ATSC and DVB streams are accepted.

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

if the SFP Module SW licence key is installed, the Operational Modes frame is visible and provides the option Electrical/SFP as shown in figure 9.37. This option is used to allocate the Data-2 IP input to operate through the Electrical Ethernet data interface, or through the SFP slot.



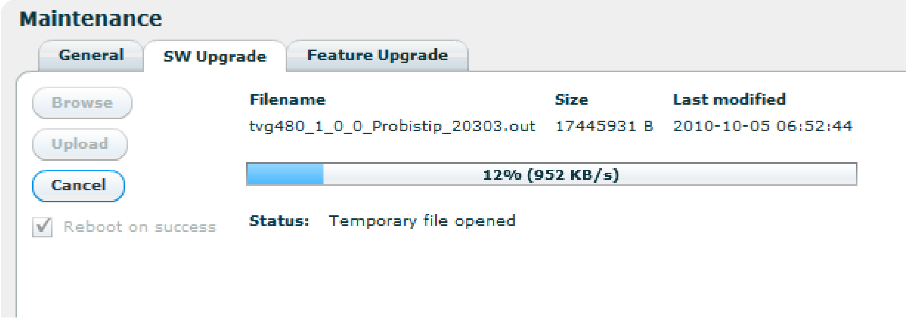
Operational Modes

Electrical/SFP: 1000Base-T

Figure 9.37 SFP and Electrical Ethernet select

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

9.4.7.2 Software Upgrade



Maintenance

☑ Reboot on success

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

12% (952 KB/s)

Status: Temporary file opened

Figure 9.38 Software Upgrade

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

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

Upload
: Once an image file is specified by using the Browse button, the Upload button is used to transmit the file from the administrator PC to the device. Once the file has been transferred, it is verified using and internal checksum value and set as the new active firmware image.

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

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

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

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

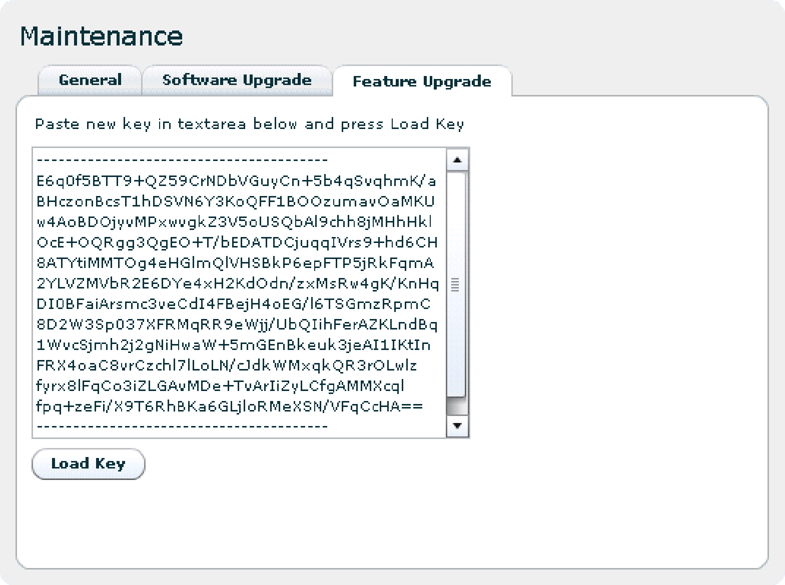
During SW loading, an alarm SW loading in progress is set with the Details field displaying the IP address of the machine from which the loading was initiated. The alarm is turned off when the loading is completed or terminated.

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

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

> **Note:** It is recommended to verify the new software version via the "Product Info" page (**Section 9.4.1**) to verify that the update was successful and the latest software revision is active.

9.4.7.3 Feature Upgrade



Paste new key in textarea below and press Load Key

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

Figure 9.39 Feature Upgrade

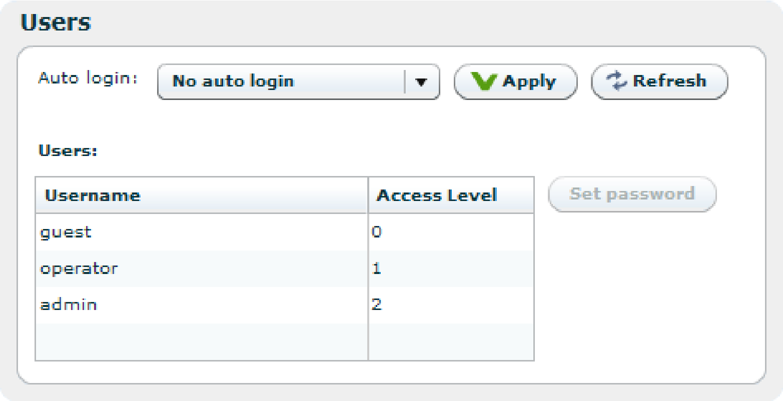
The Feature Upgrade sub-page provides an interface to upload new software licences to upgrade the feature set of the device. The licence key is provided as a text file. Paste the content of file into the text area and click the Load Key button.

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

Reset can be performed from the GUI as explained on the Maintenance > General tab in **Section 9.4.7.1**.

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

9.4.8 Users



Users

Auto login: No auto login

Users:

Username	Access Level
guest	0
operator	1
admin	2

Figure 9.40 Users page

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

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

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

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

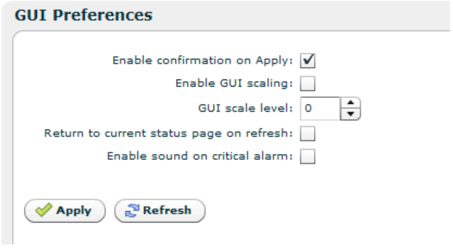
Three user privilege levels are available.

guest
: Can view configuration information and alarm logs

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

admin
: Device administrator, full access to the device.

9.4.9 GUI Preferences



GUI Preferences

Enable confirmation on Apply: ☑

Enable GUI scaling: □

GUI scale level: 0

Return to current status page on refresh: □

Enable sound on critical alarm: □

Figure 9.41 GUI Preferences page

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

Enable confirmation on Apply

Configures the web UI to prompt users for confirmation before committing changes to the device configuration. When disabled the Web UI will only prompt for confirmation prior to performing severe operations such as device reset.

Enable GUI scaling

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

GUI scale level

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

9.5 Inputs

The Inputs page contains all information and settings that apply to the Stream sources of the device. The navigation list to the left lets the user select which input to view, or select Inputs Overview to view a summary of all the inputs to the device. In addition the list also includes the input switchers and their corresponding inputs, if configured.

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

9.5.1 Inputs Overview

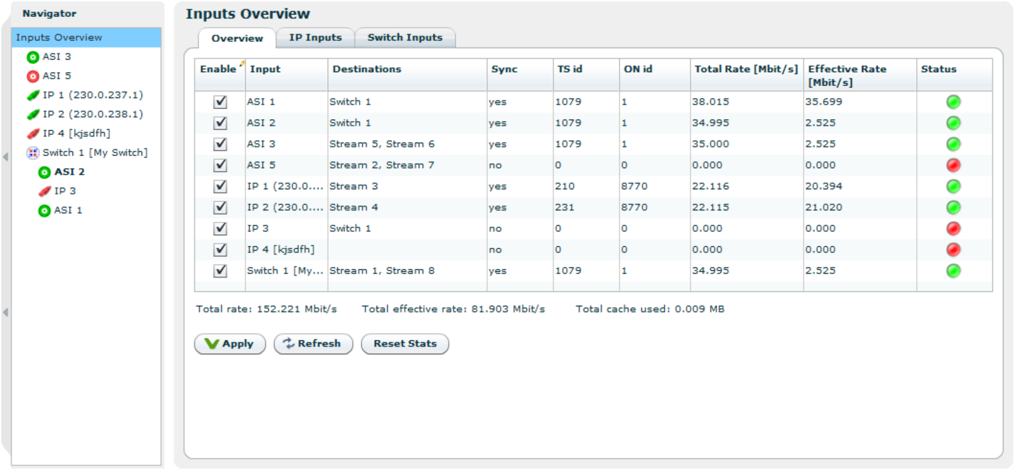
The Inputs Overview page shows a short table summary of all the inputs of the device. The table has the following columns:

Enable

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

Input

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



Inputs Overview

Enable	Input	Destinations	Sync	TS id	ON id	Total Rate [Mbit/s]	Effective Rate [Mbit/s]	Status
☑	ASI 1	Switch 1	yes	1079	1	38.015	35.699	🟢
☑	ASI 2	Switch 1	yes	1079	1	34.995	2.525	🟢
☑	ASI 3	Stream 5, Stream 6	yes	1079	1	35.000	2.525	🟢
☑	ASI 5	Stream 2, Stream 7	no	0	0	0.000	0.000	🔴
☑	IP 1 (230.0....	Stream 3	yes	210	8770	22.116	20.394	🟢
☑	IP 2 (230.0....	Stream 4	yes	231	8770	22.115	21.020	🟢
☑	IP 3	Switch 1	no	0	0	0.000	0.000	🔴
☑	IP 4 [kjsdfh]		no	0	0	0.000	0.000	🔴
☑	Switch 1 [My...	Stream 1, Stream 8	yes	1079	1	34.995	2.525	🟢

Total rate: 152.221 Mbit/s Total effective rate: 81.903 Mbit/s Total cache used: 0.009 MB

Figure 9.42 Inputs Overview

Destination
: The internal routing destination of the input signal

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

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

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

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.

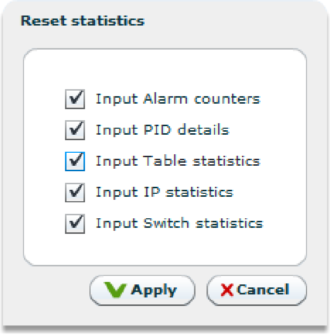
Below the table three values as shown. They are:

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

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

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

The Reset Stats button at the bottom of the page gives access to a dialogue box that allows reset of channel statistics. Figure 9.43 shows the dialogue box. Select the statistics items you want to reset and then press Apply.



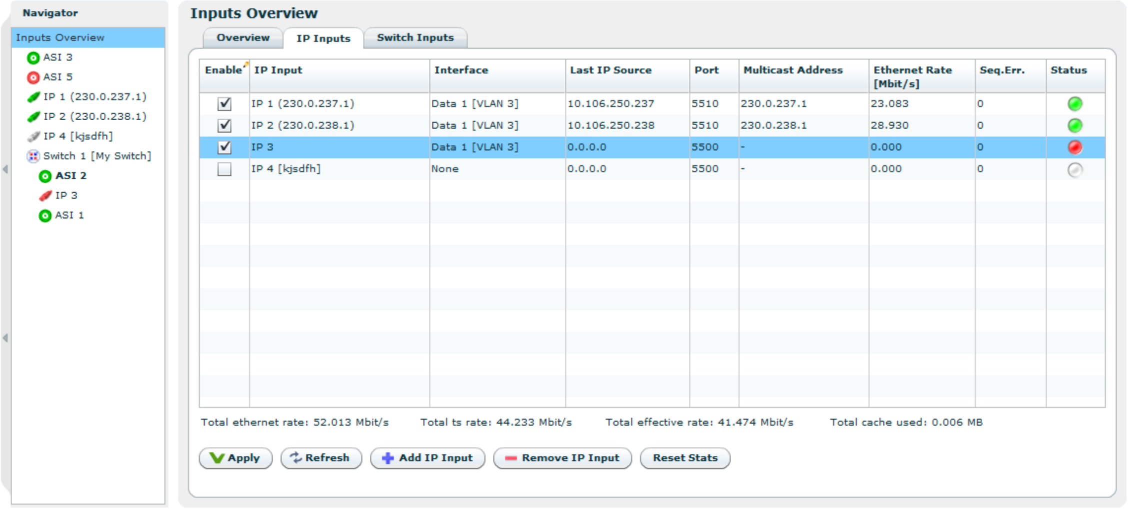
Reset statistics

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

Figure 9.43 Reset statistics dialogue box

9.5.1.1 IP Inputs

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



Enable	IP Input	Interface	Last IP Source	Port	Multicast Address	Ethernet Rate [Mbit/s]	Seq.Err.	Status
☑	IP 1 (230.0.237.1)	Data 1 [VLAN 3]	10.106.250.237	5510	230.0.237.1	23.083	0	🟢
☑	IP 2 (230.0.238.1)	Data 1 [VLAN 3]	10.106.250.238	5510	230.0.238.1	28.930	0	🟢
☑	IP 3	Data 1 [VLAN 3]	0.0.0.0	5500	-	0.000	0	🔴
□	IP 4 [kjsdfh]	None	0.0.0.0	5500	-	0.000	0	○

Total ethernet rate: 52.013 Mbit/s Total ts rate: 44.233 Mbit/s Total effective rate: 41.474 Mbit/s Total cache used: 0.006 MB

Figure 9.44 Inputs Overview - IP Inputs

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

Enable

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

IP Input

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

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

Seq.Err.

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

Status

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

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

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

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

9.5.1.2 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

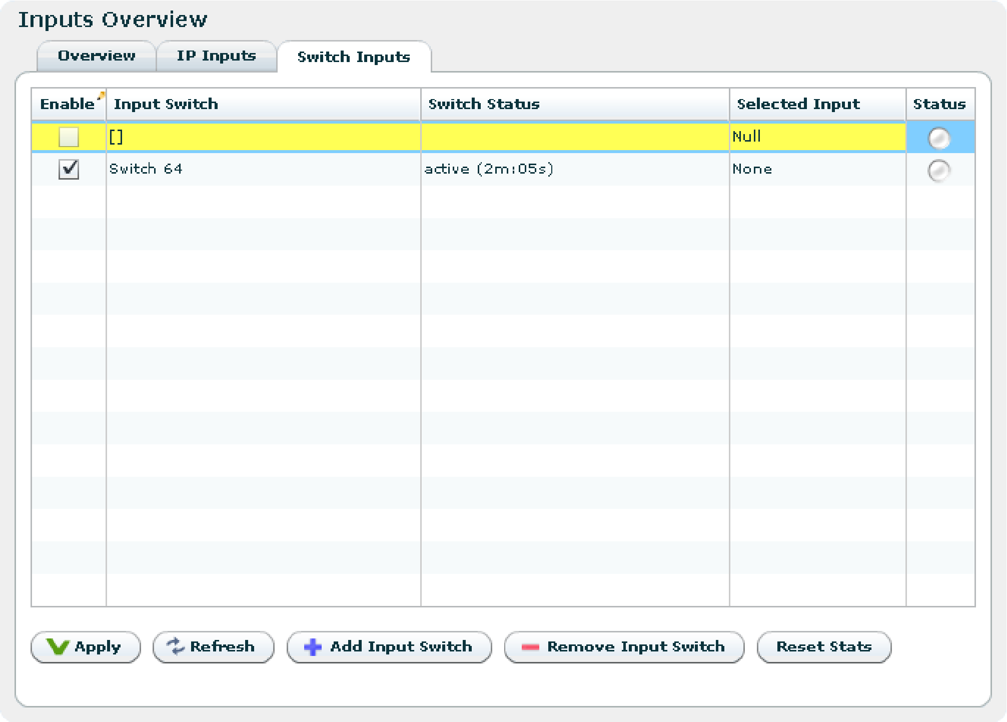
This shows whether the switch input is enabled or not. An input is enabled or disabled by clicking the check box and hitting Apply.

Input Switch

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

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.



Inputs Overview

Enable	Input Switch	Switch Status	Selected Input	Status
□	[]		Null	○
☑	Switch 64	active (2m:05s)	None	○

Figure 9.45 Inputs Overview - Switch Inputs

Selected Input
: Shows the currently selected physical port

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.

9.5.2 Input

When a specific input is selected a page with information about that input is displayed. The top part of the page is common for all sub pages and shows the name and the current alarm status of the input.

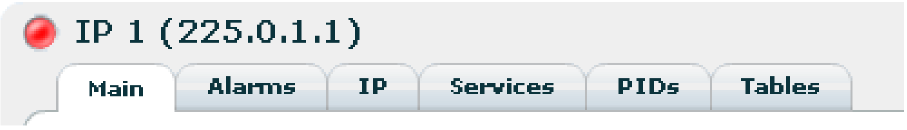


Figure 9.46 Input header

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

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

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

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

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

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

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

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

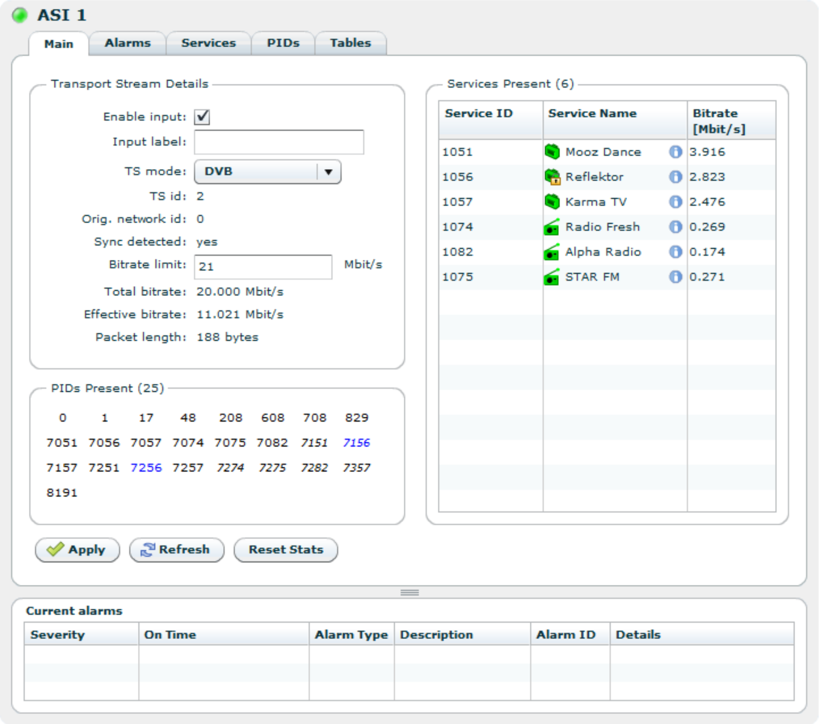
In all sub-pages for a selected input a list of current alarms for that input is shown. The list is identical to the list displayed in the Current Status view, described in section **Section 9.3.1**.

9.5.2.1 Main

The Main page is divided into three sections for ASI Inputs (figure **Figure 9.47**) and five sections for IP inputs. For IP inputs the two extra sections are the IP RX configuration section (top left) and the IP RX status section (top right), see figure **Figure 9.48**.

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

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



Transport Stream Details

Enable input: ☑
Input label:
TS mode: DVB ▾
TS id: 2
Orig. network id: 0
Sync detected: yes
Bitrate limit: 21 Mbit/s
Total bitrate: 20.000 Mbit/s
Effective bitrate: 11.021 Mbit/s
Packet length: 188 bytes

PIDs Present (25)

0	1	17	48	208	608	708	829
7051	7056	7057	7074	7075	7082	*7151*	*7156*
7157	7251	7256	7257	*7274*	*7275*	*7282*	*7357*
8191							

Services Present (6)

Service ID	Service Name	Bitrate [Mbit/s]
1051	Mooz Dance	3.916
1056	Reflektor	2.823
1057	Karma TV	2.476
1074	Radio Fresh	0.269
1082	Alpha Radio	0.174
1075	STAR FM	0.271

Current alarms

Severity	On Time	Alarm Type	Description	Alarm ID	Details

Figure 9.47 Main

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

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

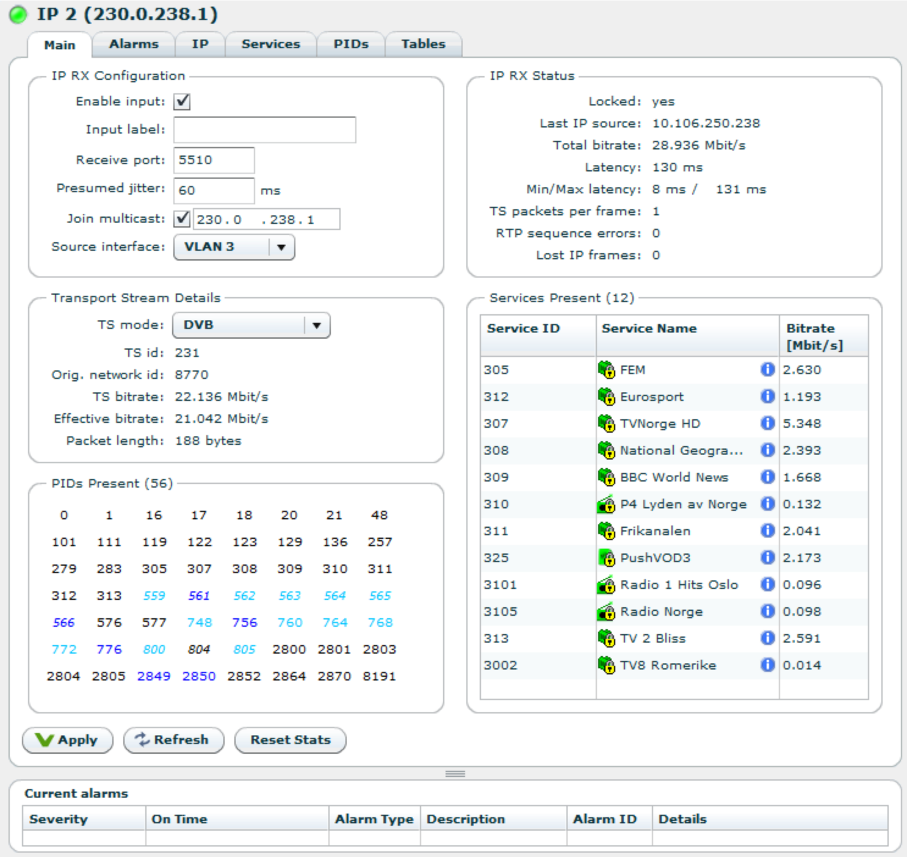
Input label
: This is the user defined name of the input port, which can be changed by typing a new label and hitting Apply. It is only used in the WEB GUI to identify the port.

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

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

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.



IP RX Configuration

Enable input: ☑
Input label:
Receive port: 5510
Presumed jitter: 60 ms
Join multicast: ☑ 230 . 0 . 238 . 1
Source interface: VLAN 3 ▾

IP RX Status

Locked: yes
Last IP source: 10.106.250.238
Total bitrate: 28.936 Mbit/s
Latency: 130 ms
Min/Max latency: 8 ms / 131 ms
TS packets per frame: 1
RTP sequence errors: 0
Lost IP frames: 0

Transport Stream Details

TS mode: DVB ▾
TS id: 231
Orig. network id: 8770
TS bitrate: 22.136 Mbit/s
Effective bitrate: 21.042 Mbit/s
Packet length: 188 bytes

PIDs Present (56)

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

Services Present (12)

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

Current alarms

Severity	On Time	Alarm Type	Description	Alarm ID	Details

Figure 9.48 IP Input Sections

Bitrate limit

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

Total Bitrate

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

Effective Bitrate

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

Packet length

The length of the transport stream packets in bytes.

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

Red

A continuity counter (CC) error alarm is raised.

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

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

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

The list has three columns:

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

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

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

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

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

Service Bitrate
: The current bitrate of the service, i.e. the aggregate bitrate of all the service components.

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

9.5.2.2 Alarms

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

In figure 9.49 the Alarm Config page is shown. Note that the alarms are organised hierarchically and that only the branches in focus need to be expanded.

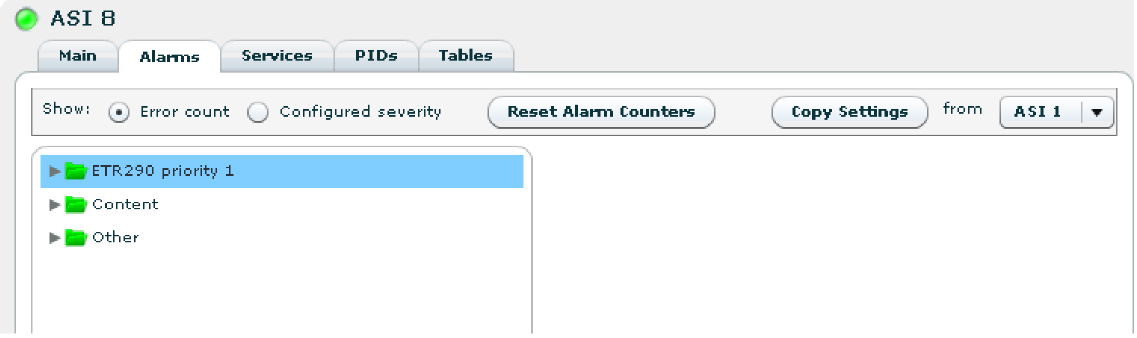


Figure 9.49 Input alarm configuration

The following configuration options are available:

Show
: The radio buttons Error count and Configured severity allows the user to configure what to be shown in the input alarm tree (see figure 9.50).

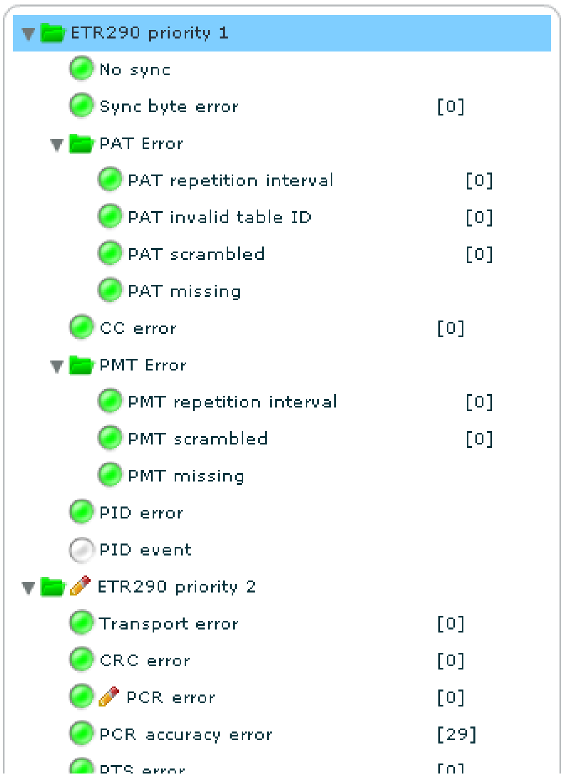
  Error count
  : Display the accumulated number of errors since last alarm counter reset.

  Configured severity
  : Display the configured alarm severity.

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

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

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



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

Figure 9.50 Input alarm tree

The input alarm tree is shown in figure 9.50. By clicking on the alarm nodes in the tree the details for the selected alarm is shown in the Alarm details section (figure 9.51).

The alarm tree has two types of nodes:

Folder

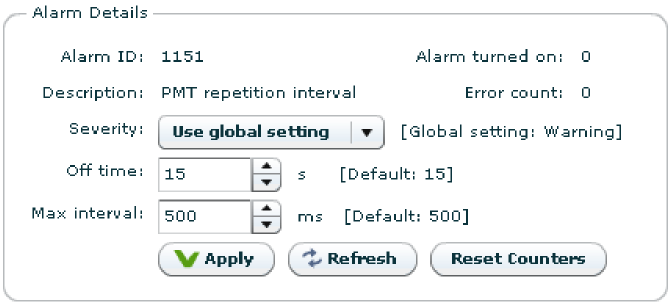
Corresponds to a group of alarms. The colour of the folder shows the highest severity of all the alarms belonging to the group. The group is expanded or collapsed by clicking on the arrow next to the group.

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

Alarm node

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

The right hand side of the page shows details about a single selected alarm (see figure 9.51). The frame appears when a particular alarm is clicked. Its content may vary according to the alarm selected.



Alarm Details

Alarm ID: 1151

Alarm turned on: 0

Description: PMT repetition interval

Error count: 0

Severity: Use global setting [Global setting: Warning]

Off time: 15 s [Default: 15]

Max interval: 500 ms [Default: 500]

Figure 9.51 Alarm details

The alarm details section includes the following information and buttons.

Alarm ID

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

Alarm

Name of the alarm.

Description

A short description of the alarm.

Severity

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

Max interval (alarm dependent label)

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

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

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

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

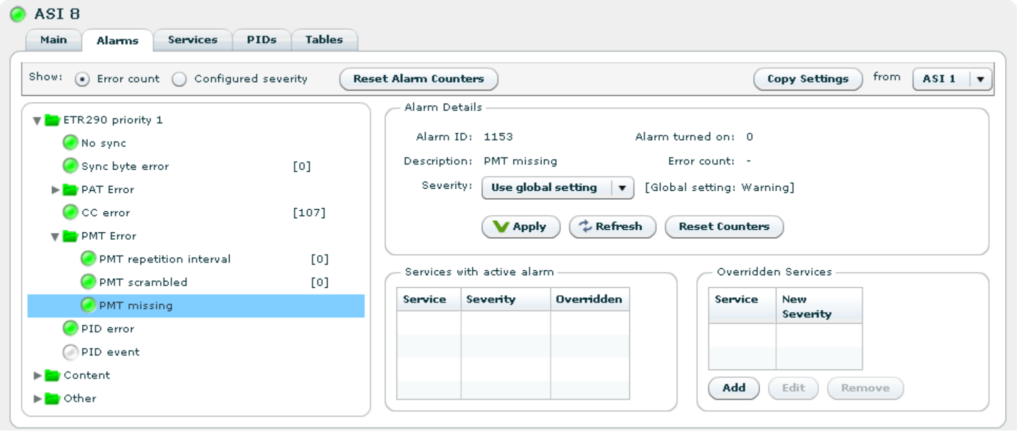
Error count
: For alarms that are checked continuously, this counter shows the number of times an alarm condition has been violated. This counter will increase even if the alarm is filtered.

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

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

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

"PID" and "Service"alarms (**Figure 9.52**) allow overriding of sub items. For such alarms two tables are shown below the alarm details.



Show: ● Error count ○ Configured severity

from ASI 1

- ETR290 priority 1
  - No sync
  - Sync byte error [0]
  - PAT Error
  - CC error [107]
  - PMT Error
    - PMT repetition interval [0]
    - PMT scrambled [0]
    - PMT missing
  - PID error
  - PID event
- Content
- Other

Alarm Details

Alarm ID: 1153 Alarm turned on: 0

Description: PMT missing Error count: -

Severity: Use global setting [Global setting: Warning]

Services with active alarm

Service	Severity	Overridden

Overridden Services

Service	New Severity

Figure 9.52 Alarm severity per sub-ID (typically Service or PID)

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

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

Severity
: The current severity of the item.

Overridden
: Indicates whether the sub item has been overridden.

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

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

Service/PID
: The id of the Sub item.

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

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

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

9.5.2.3 IP

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

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

The Main sub page is shown in figure 9.53.

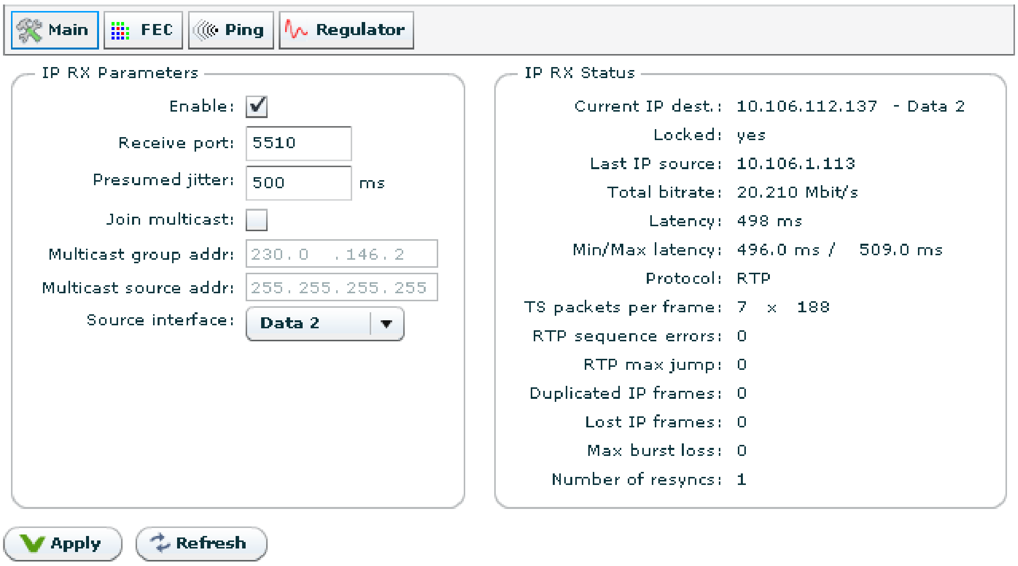
This page allows configuration of the IP parameters for the IP input and shows detailed IP status information for the input.

The IP RX Parameters field:

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

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

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



IP RX Parameters

Enable: ☑
Receive port: 5510
Presumed jitter: 500 ms
Join multicast: □
Multicast group addr: 230.0 .146.2
Multicast source addr: 255.255.255.255
Source interface: Data 2

IP RX Status

Current IP dest.: 10.106.112.137 - Data 2
Locked: yes
Last IP source: 10.106.1.113
Total bitrate: 20.210 Mbit/s
Latency: 498 ms
Min/Max latency: 496.0 ms / 509.0 ms
Protocol: RTP
TS packets per frame: 7 x 188
RTP sequence errors: 0
RTP max jump: 0
Duplicated IP frames: 0
Lost IP frames: 0
Max burst loss: 0
Number of resyncs: 1

Figure 9.53 IP Configuration

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

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

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

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

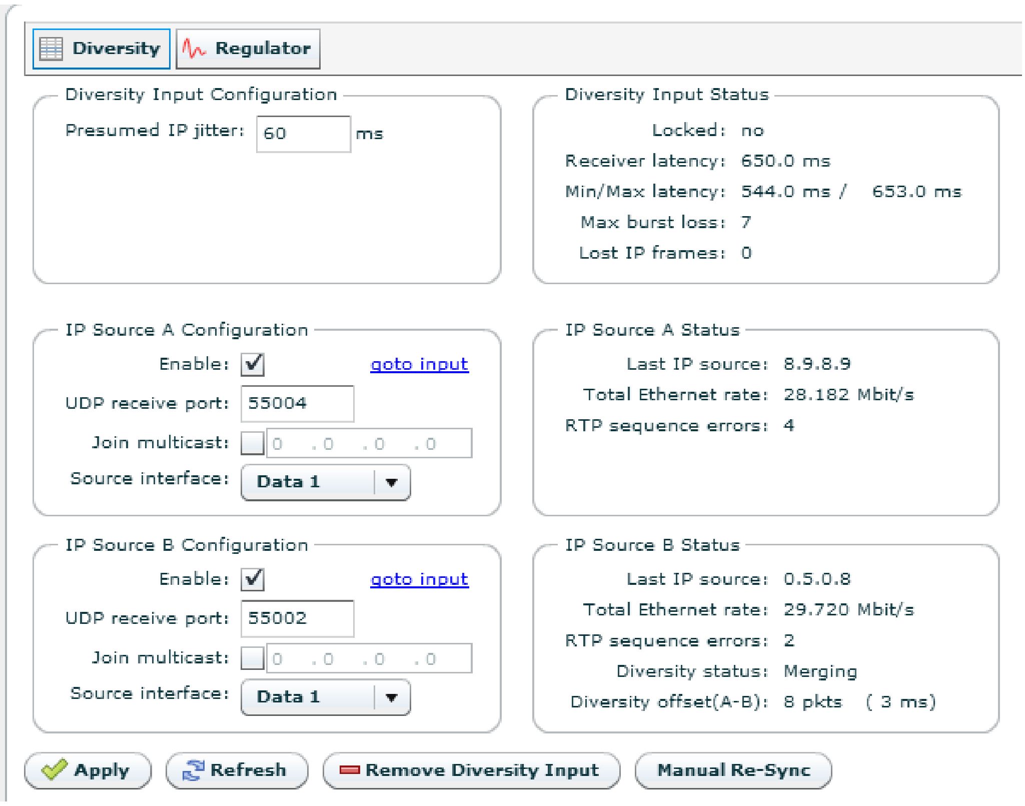
If the product is installed with the IP diversity (IDR) feature an additional button will appear at the right side of the ”Apply” and ”Refresh” button. This button will add another IP channel that will combine the two IP channels into a diversity pair.

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

9.5.2.3.1 RTP/IP Diversity Reception

This tab will only be visible if a diversity input has been added. Please see 6.3 for detailed technical description of RTP/IP Diversity Reception.

The Diversity sub page is shown in figure 9.54.



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: ☑
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: ☑
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 9.54 RTP/IP Diversity Reception Configuration

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.

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 box 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 box 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.

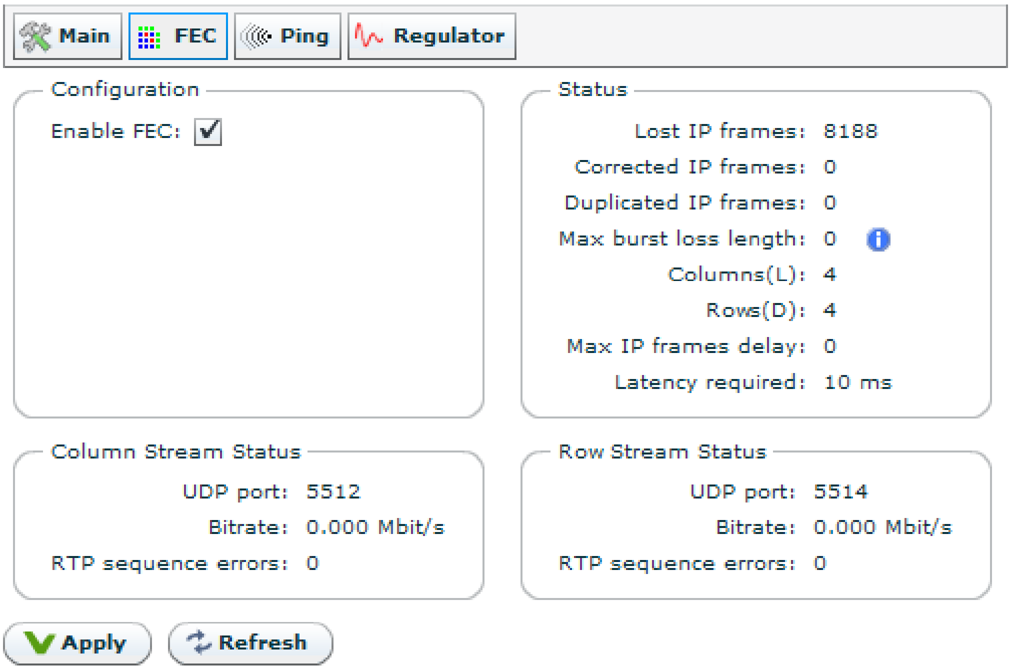
Diversity offset(A-B)
: Offset between source A and B measured in RTP sequence number and corresponding value in time. Measurements are A-B, i.e if positive, A is on a higher RTP sequence number at the same time instance and has therefore less delay since IP transmitter.
Positive: A is received first.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

9.5.2.3.2 FEC

The FEC sub page is shown in **Figure 9.55**. This page displays the status of the forward error correction processing of the IP input.



Configuration

Enable FEC: ☑

Status

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

Column Stream Status

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

Row Stream Status

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

Figure 9.55 Input FEC configuration

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

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

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

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

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

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

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

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

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

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

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

UDP port
: The UDP ports receiving the column/row FEC data.

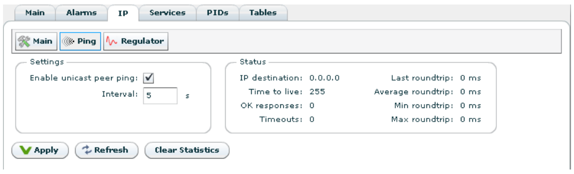
Bitrate
: The bitrates of the Column and row FEC data.

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

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

9.5.2.3.3 Ping

The Ping sub page is shown in figure 9.56.



Settings

Enable unicast peer ping: ☑

Interval: 5 s

Status

IP destination: 0.0.0.0
Time to live: 255
OK responses: 0
Timeouts: 0
Last roundtrip: 0 ms
Average roundtrip: 0 ms
Min roundtrip: 0 ms
Max roundtrip: 0 ms

Figure 9.56 Ping page

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

The Settings field:

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

Interval
: Set the interval in seconds between each Ping.

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

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

IP destination
: The address of the device receiving the Ping requests.

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

OK responses
: Indicates how many valid Ping responses have been received.

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

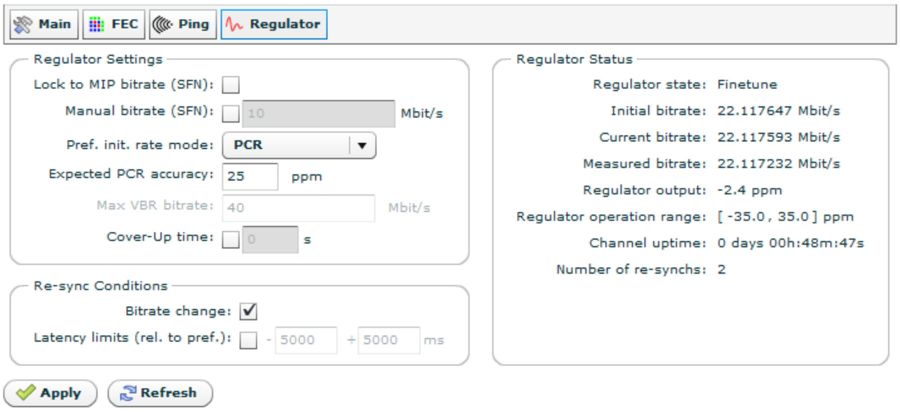
Last roundtrip
: The time taken from last sending the Ping message until the response is received.

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

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

9.5.2.3.4 Regulator

The Regulator sub page is shown if figure 9.57.



Regulator Settings

Lock to MIP bitrate (SFN): □

Manual bitrate (SFN): □ 10 Mbit/s

Pref. init. rate mode: PCR

Expected PCR accuracy: 25 ppm

Max VBR bitrate: 40 Mbit/s

Cover-Up time: □ 0 s

Re-sync Conditions

Bitrate change: ☑

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

Regulator Status

Regulator state: Finetune

Initial bitrate: 22.117647 Mbit/s

Current bitrate: 22.117593 Mbit/s

Measured bitrate: 22.117232 Mbit/s

Regulator output: -2.4 ppm

Regulator operation range: [-35.0 , 35.0] ppm

Channel uptime: 0 days 00h:48m:47s

Number of re-synchs: 2

Figure 9.57 Regulator page

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

Lock to MIP bitrate (SFN)
: Enable this to lock the bitrate to DVB-T MIP timestamp if a MIP is found in the stream. This option will only work over time if both the unit transmitting the MIP and the IP receiver have locked their 27Mhz clocks to the same 1PPS reference.

Manual bitrate (SFN)
: This option lets you configure a bitrate manually on the IP input channel, disabling the buffer

regulator. This method is similar to Lock to MIP bitrate, except that the bitrate is specified manually, and the mode will only work over time if the transmitter and receiver are locked to an external 1PPS time reference.

Pref. Init. Rate Mode

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

PCR

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

MIP

This mode may be used for a signal that does not contain any PCR PIDs, but does have a DVB MIP PID (PID 21) as used in Single Frequency Networks. In MIP mode, two consecutive MIP packets are used to estimate the bitrate. The input signal must be a valid DVB-T feed in the sense that the MIP is valid, for this mode to work.

VBR

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

FAST COARSE

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

Expected PCR accuracy

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

Max VBR bitrate

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

Cover-Up time

This option can be used to cover up for longer breaks in the IP input stream. Ts output integrity is maintained by playing out stuffing packets. The playout continues up to a limited, configurable number seconds, after which the output is interrupted. If the input IP stream returns within the configured Cover-Up time, the buffer is filled up to the configured level and ouput is resumed. This means that equipment receiving the output should not loose TS sync during the loss of input. A dedicated alarm, “Covering up input loss”, is set while stuffing packets are transmitted to keep the output signal up.

The Re-sync Conditions field:

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

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

The Regulator Status field allows inspecting the status of the buffer regulator.

Regulator state
: This parameter shows the current state of the buffer regulator. The possible states are Stopped, Rate Estimation, Coarse and Finetune. When data is received and an initial bitrate estimate is found the regulator enters the Rate Estimation state, where the signal is analysed to check if a better estimate of the bitrate can be found. When a better estimate is found the regulator switches to Coarse mode where the output bitrate is coarsely moved closer to the new rate. From Coarse mode the regulator enters Finetune mode.

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

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

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

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

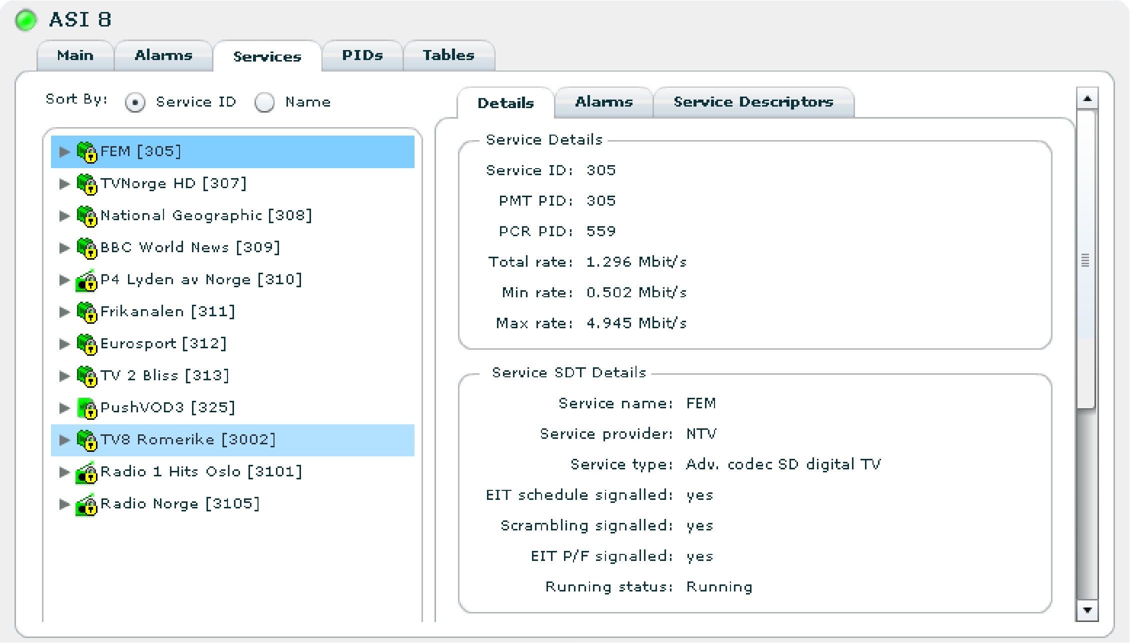
Regulator operation range
: Indicates the maximum clock correction (in ppm) that may be applied. This parameter is affected by the "Expected PCR accuracy" parameter and is typically configured slightly wider to allow headroom for buffer regulation.

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

Number of re-synchs
: Displays the number of re-synchronisations since the last unit power up, or since the Reset Stats function was last used (see **Section 9.5.2.1**).

9.5.2.4 Services

The Services page displays a list of services running in the selected input. Each service type is represented by a symbol coloured to show the current alarm status of the service (figure 9.58).



Sort By: ● Service ID ○ Name

- ▶ FEM [305]
- ▶ TVNorge HD [307]
- ▶ National Geographic [308]
- ▶ BBC World News [309]
- ▶ P4 Lyden av Norge [310]
- ▶ Frikanalen [311]
- ▶ Eurosport [312]
- ▶ TV 2 Bliss [313]
- ▶ PushVOD3 [325]
- ▶ TV8 Romerike [3002]
- ▶ Radio 1 Hits Oslo [3101]
- ▶ Radio Norge [3105]

Service Details

Service ID:	305
PMT PID:	305
PCR PID:	559
Total rate:	1.296 Mbit/s
Min rate:	0.502 Mbit/s
Max rate:	4.945 Mbit/s

Service SDT Details

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

Figure 9.58 Service details overview when service list is not expanded.

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

Clicking on a service name (folder name) brings up a tab navigator to the right of the list containing more information about the selected service. The Details tab shows detailed information about the selected service. The service information may be presented in one or two sections. The first section, Service Details, is always present and consists of the following parameters:

Service ID
: The service id of the selected service.

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

PCR PID
: The PCR PID of the service.

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

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

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

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

Service name
: The name of the service.

Service provider
: The provider of the service.

Service type
: The type of service.

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

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

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

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

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

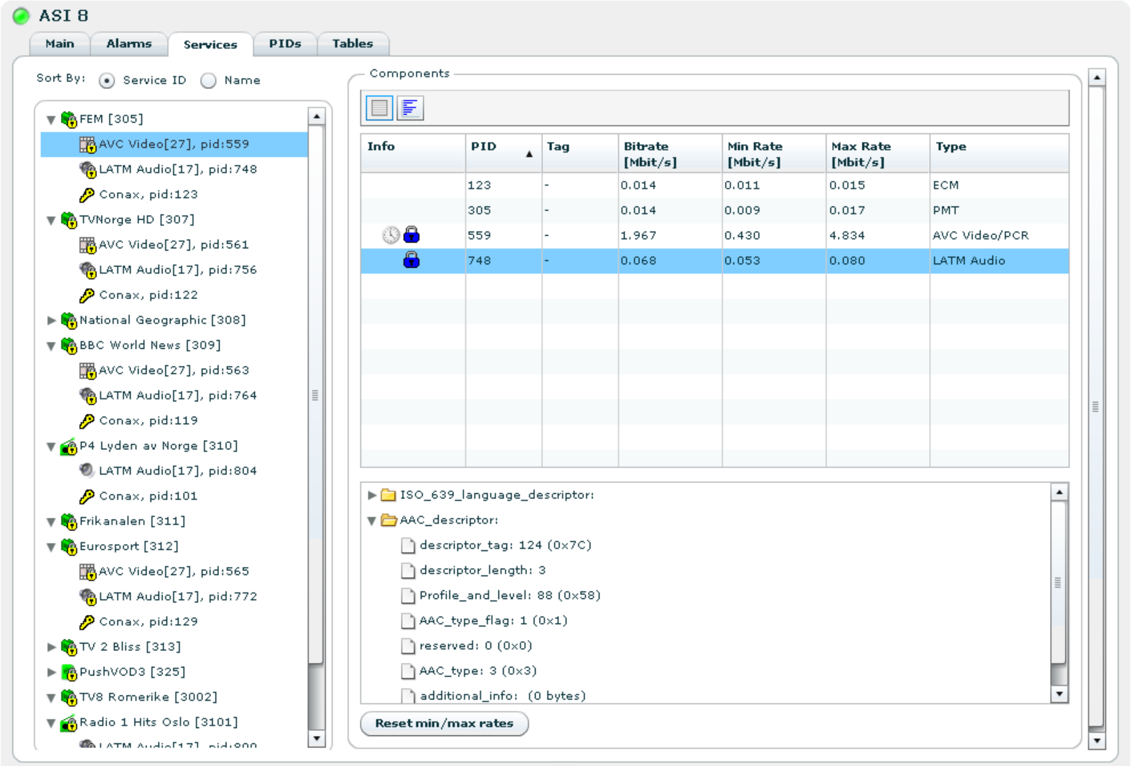
- Channel name
- Major channel number
- Minor channel number
- Service type
- Modulation mode
- Channel TSID
- Access controlled

- Hidden
- Hide guide

The Alarms sub page contains a table showing all alarms currently active on the selected service. The columns in the table (Severity, Description, Alarm ID and Details) have the same meaning as described in **Section 9.3.2**.

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

To list all components contained within a specific service click the arrow for the given service. The expanded view is shown in **Figure 9.59**.



```
▼ FEM [305]
    AVC Video[27], pid:559
    LATM Audio[17], pid:748
    Conax, pid:123
▼ TVNorge HD [307]
    AVC Video[27], pid:561
    LATM Audio[17], pid:756
    Conax, pid:122
▶ National Geographic [308]
▼ BBC World News [309]
    AVC Video[27], pid:563
    LATM Audio[17], pid:764
    Conax, pid:119
▼ P4 Lyden av Norge [310]
    LATM Audio[17], pid:804
    Conax, pid:101
▼ Frikanalen [311]
▼ Eurosport [312]
    AVC Video[27], pid:565
    LATM Audio[17], pid:772
    Conax, pid:129
▶ TV 2 Bliss [313]
▶ PushVOD3 [325]
▼ TV8 Romerike [3002]
▼ Radio 1 Hits Oslo [3101]
    LATM Audio[17], pid:800
```

Info	PID ▲	Tag	Bitrate [Mbit/s]	Min Rate [Mbit/s]	Max Rate [Mbit/s]	Type
	123	-	0.014	0.011	0.015	ECM
	305	-	0.014	0.009	0.017	PMT
	559	-	1.967	0.430	4.834	AVC Video/PCR
	748	-	0.068	0.053	0.080	LATM Audio

```
▶ ISO_639_language_descriptor:
▼ AAC_descriptor:
    descriptor_tag: 124 (0x7C)
    descriptor_length: 3
    Profile_and_level: 88 (0x58)
    AAC_type_flag: 1 (0x1)
    reserved: 0 (0x0)
    AAC_type: 3 (0x3)
    additional_info:  (0 bytes)
```

Figure 9.59 Service details full component overview

Each component is shown with the following information:

Component type symbol
: Symbol showing the kind of component.

Textual description
: A text description of the component type.

Type id
: The component type id.

PID

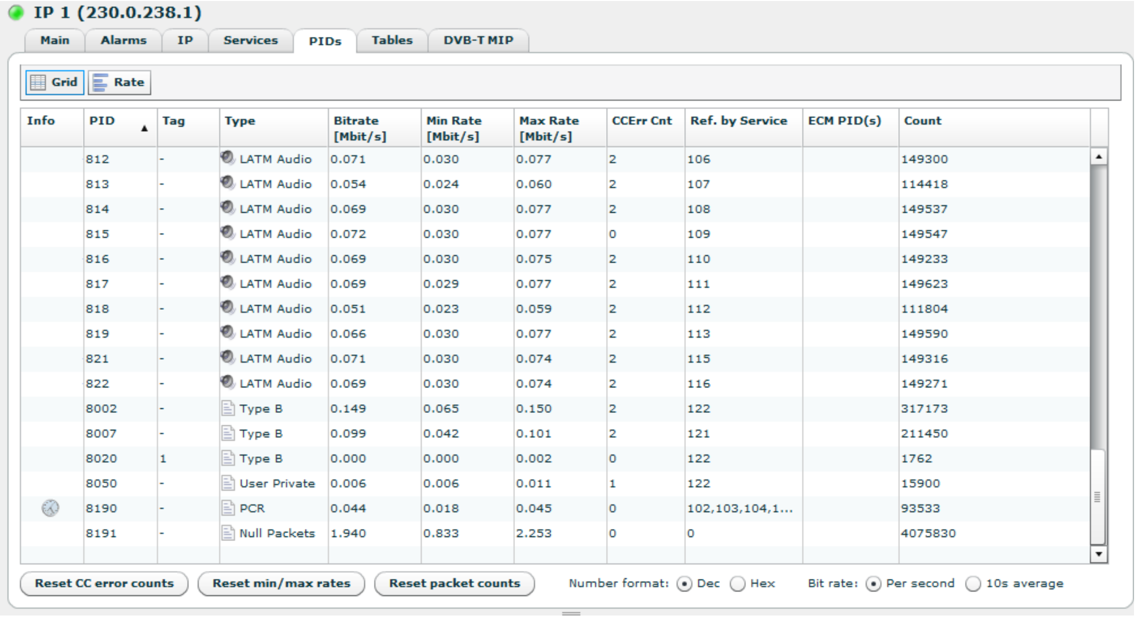
The transport PID number.

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

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

9.5.2.5 PIDs

This page gives detailed information about the PIDs present on the input. Two different PID views may be selected with buttons on the tool bar at the top of the page. The Grid button selects a listing of the PIDs in table form, the Rate button selects a bar graph representation, indicating dynamically the bit rate of each PID.



Info	PID	Tag	Type	Bitrate [Mbit/s]	Min Rate [Mbit/s]	Max Rate [Mbit/s]	CCErr Cnt	Ref. by Service	ECM PID(s)	Count
	812	-	LATM Audio	0.071	0.030	0.077	2	106		149300
	813	-	LATM Audio	0.054	0.024	0.060	2	107		114418
	814	-	LATM Audio	0.069	0.030	0.077	2	108		149537
	815	-	LATM Audio	0.072	0.030	0.077	0	109		149547
	816	-	LATM Audio	0.069	0.030	0.075	2	110		149233
	817	-	LATM Audio	0.069	0.029	0.077	2	111		149623
	818	-	LATM Audio	0.051	0.023	0.059	2	112		111804
	819	-	LATM Audio	0.066	0.030	0.077	2	113		149590
	821	-	LATM Audio	0.071	0.030	0.074	2	115		149316
	822	-	LATM Audio	0.069	0.030	0.074	2	116		149271
	8002	-	Type B	0.149	0.065	0.150	2	122		317173
	8007	-	Type B	0.099	0.042	0.101	2	121		211450
	8020	1	Type B	0.000	0.000	0.002	0	122		1762
	8050	-	User Private	0.006	0.006	0.011	1	122		15900
🕒	8190	-	PCR	0.044	0.018	0.045	0	102,103,104,1...		93533
	8191	-	Null Packets	1.940	0.833	2.253	0	0		4075830

Number format: ● Dec ○ Hex

Bit rate: ● Per second ○ 10s average

Figure 9.60 PID Details, table view

The PID table contains the following columns:

Info

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

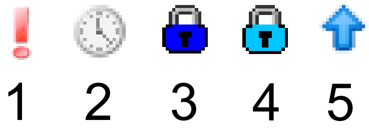


Figure 9.61 Status icons in PID details

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 couter reset.

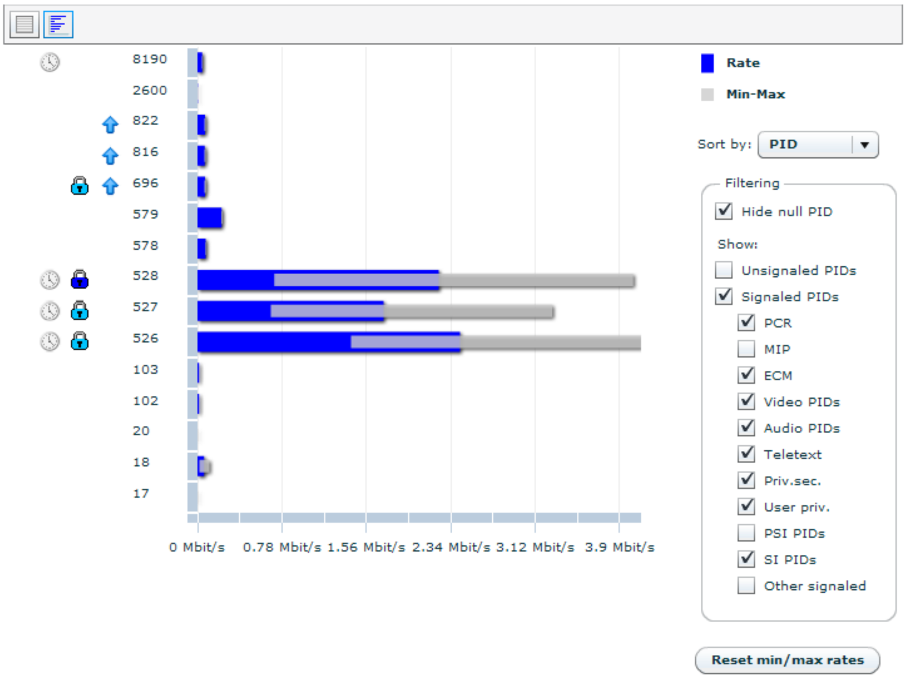
Beneath the PID table are three buttons:

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

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

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

The PID rate view is shown in figure 9.62. To the left is the bar chart showing the PIDs and



Sort by: PID

Filtering

☑ Hide null PID

Show:

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

Figure 9.62 PID Details, rate view

Vertically, the chart displays one bar for each of the packet streams present on the input. Adjacent to the PIDs the symbols shown in figure 9.61 are shown if relevant.

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

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

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

9.5.2.6 Tables

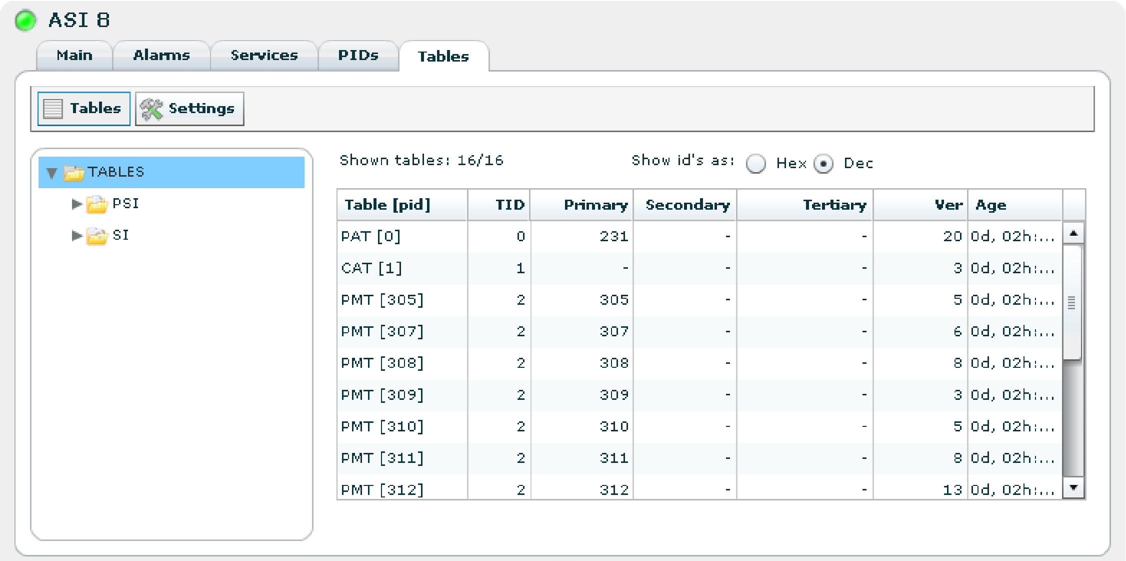
The Tables page shows detailed information about all the tables that are currently residing in the input SI/PSIP database of the device. Accessing the related sub pages gives access to table contents right down to byte level.

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

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

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

9.5.2.7 Tables



Shown tables: 16/16

Show id's as: ○ Hex ● Dec

Table [pid]	TID	Primary	Secondary	Tertiary	Ver	Age
PAT [0]	0	231	-	-	20	0d, 02h:...
CAT [1]	1	-	-	-	3	0d, 02h:...
PMT [305]	2	305	-	-	5	0d, 02h:...
PMT [307]	2	307	-	-	6	0d, 02h:...
PMT [308]	2	308	-	-	8	0d, 02h:...
PMT [309]	2	309	-	-	3	0d, 02h:...
PMT [310]	2	310	-	-	5	0d, 02h:...
PMT [311]	2	311	-	-	8	0d, 02h:...
PMT [312]	2	312	-	-	13	0d, 02h:...

Figure 9.63 Table details, overview.

Figure 9.63 shows the table details in list view.

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

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

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

Shown sections
: The number of PSI/SI/PSIP table sections displayed in the list.

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

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

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

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

TID
The table ID.

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

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

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

Ver
This is the last received version of this table.

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

9.5.2.8 Settings

In this sub page it is possible to select the table types to analyse. Each table type has a corresponding check box. EIT Actual and EIT Other are further configurable as they allow the number of days worth of data to be configured.

To commit changes to the settings on this page, click the Apply button located at the bottom of the page. Press Refresh to reload the settings which may have been changed by another user.

Figure 9.64 shows the page as displayed in DVB mode.

In ATSC mode the page looks different, as shown in figure 9.65

- To be able to see programs and program components you must analyse at least PAT and PMT.
- To see the service name for the services you have to configure analysis of SDTa (SDT actual) for DVB services, or TVCT/CVCT for ATSC services

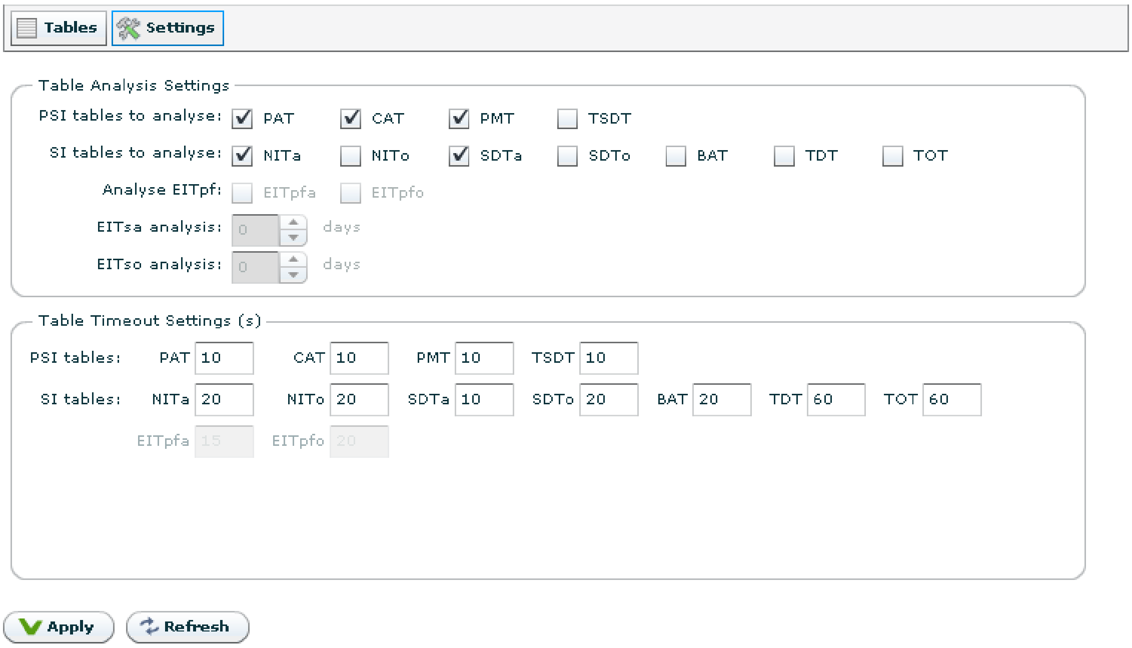


Table Analysis Settings

PSI tables to analyse: ☑ PAT ☑ CAT ☑ PMT □ TSDT

SI tables to analyse: ☑ NITa □ NITo ☑ SDTa □ SDTo □ BAT □ TDT □ TOT

Analyse EITpf: □ EITpfa □ EITpfo

EITsa analysis: 0 days

EITso analysis: 0 days

Table Timeout Settings (s)

PSI tables: PAT 10 CAT 10 PMT 10 TSDT 10

SI tables: NITa 20 NITo 20 SDTa 10 SDTo 20 BAT 20 TDT 60 TOT 60

EITpfa 15 EITpfo 20

Figure 9.64 Table analysis configuration.

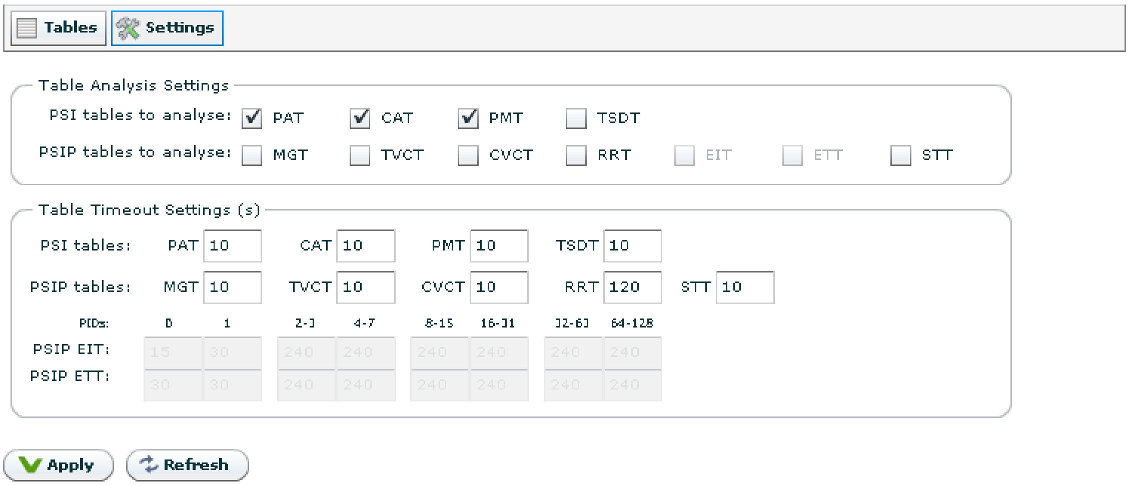


Table Analysis Settings

PSI tables to analyse: ☑ PAT ☑ CAT ☑ PMT □ TSDT

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

Table Timeout Settings (s)

PSI tables: PAT 10 CAT 10 PMT 10 TSDT 10

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

PIDs:	0	1	2-3	4-7	8-15	16-31	32-63	64-128
PSIP EIT:	15	30	240	240	240	240	240	240
PSIP ETT:	30	30	240	240	240	240	240	240

Figure 9.65 Table analysis configuration in ATSC mode.

- In general alarms will not be generated for tables that are not configured for analysis.

In the Table Timeout Settings field it is possible to change the timeouts used when detecting the presence of each table. The values are specified in number of seconds.

Configuring larger time-out tolerances for tables that are occurring with non-standard repetition intervals can reduce the number of alarms generated. Right-clicking each timeout parameter and selecting Set to default resets the original value.

The timeout values are also used to generate Table missing alarms.

9.5.3 Switch Inputs

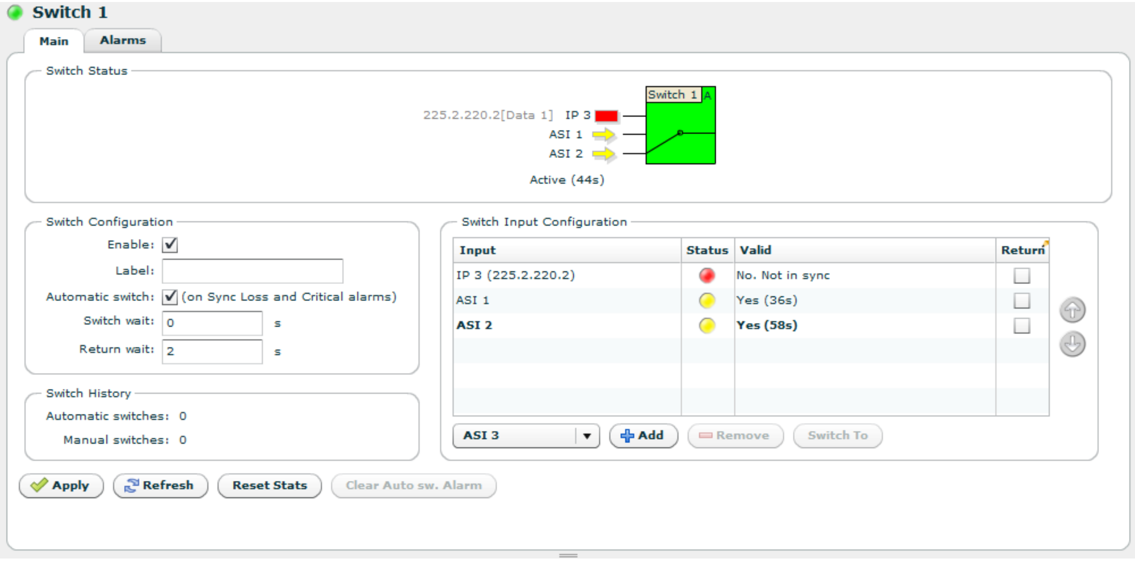
The TVG425 supports combination of several inputs into a prioritized order switching group, where the highest priority source signal that does not have a critical alarm level (red bulb) is automatically selected as the source of program data. The input switch is itself modelled as an input; once defined it can source a TVG425 Stream. Loss of sync or critical alarm level on the currently selected switch input signal will cause the switch to immidiately select the next priority input. The signals on each input 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 sources may be ASI and IP inputs in any combination. Signal loss detection on IP sources is slower than for ASI sources. An input signal applied to a switch cannot be used as input to a TVG425 Stream directly.

The input switching function is subject to SW licensing.

Information about a Stream input switch is displayed on the right when selecting and clicking that input switch in the navigator. The top part shows the name and the current alarm status of the input switch. Holding the mouse cursor over the alarm status indicator brings up a tool tip showing the current alarms on this input switch. Below the Switch entry in the navigator a list of switch inputs will appear as the inputs are configured. The Switch 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 9.3.1.

9.5.3.1 Main

The Main page allows configuring the switch and checking its status.



Enable: ☑

Label:

Automatic switch: ☑ (on Sync Loss and Critical alarms)

Switch wait: 0 s

Return wait: 2 s

Automatic switches: 0

Manual switches: 0

Input	Status	Valid	Return
IP 3 (225.2.220.2)	●	No. Not in sync	□
ASI 1	●	Yes (36s)	□
ASI 2	●	**Yes (58s)**	□

Figure 9.66 Input switch Main page

The Switch Configuration field:

Enable

A tick in the box enables the switch functionality.

Label
: Enter a user defined identification label for the switch.

Automatic switch
: A tick in the box enables automatic switching determined by the status of the inputs to the switch. Sync loss or critical alarm level of the currently passed signal will initiate switching to the first valid input source with the highest priority. Manual switching requires operator intervention.

> **Tip:** All input alarms may be reconfigured to have critical alarm level to switch on alarm events in addition to sync loss.

Switch wait
: The time between a switching condition is detected until switching occurs (automatic switching).

Reswitch wait
: Hold period activated when switching back to the port that was active prior to the last switching action. No auto-switching will be performed within the hold period. This is used to avoid too frequent switching. The Reswitch wait time is used to determine when to activate the hold state. The Hold state is activated when an attempt is made to switch again before the configured reswitch wait time has elapsed.

The Switch Input Configuration field:

Here, the switch sources are selected. From the Inputs drop-down list below the table, select an input to feed the switch and click Add. An entry on a yellow background appears in the table. Click Apply to confirm. Repeat for each additional switch input. An input can be removed by higlighting the appropriate line in the table and clicking Remove. A red background highlights the choice. Confirm by clicking Apply.

The input table shows a list of all inputs related to the switch, whether it be ASI or IP inputs. The list represents the priority in which to select inputs. The input priority may be changed by selecting an entry and moving it up or down in the list using the arrows to the right. Click Apply to commit the change. An entry line with bold characters indicate the input that is currently routed to the switch output.

Enabled
: Indicates if the input source is currently enabled.

Sync
: Indicates if the input signal is synchronised; i.e. a valid transport stream.

Status
: Will indicate if the input signal is non-conformant in any way.

Return
: Tick the box to enable the swicth to return to the previous state if the switching condition is no longer present.

Below the table is also the Switch To button. Highlight a non-active input in the list and click the button to manually make the switch select that input. Click Apply“ to confirm.

The Switch Status field:

Status
: Shows switch state; Idle, Active, Wait or Hold and the time elapsed since the entering the current state.

Selected input
: The input whose signal is currently passed by the switch.

Switches done
: The number of switch actions performed since last counter reset.

At the bottom of the page are the Apply and Refresh buttons. In addition the Reset Stats button is used to clear the statistics counters. The Clear Auto sw. Alarm clears the alarm raised when an automatic switch has been made.

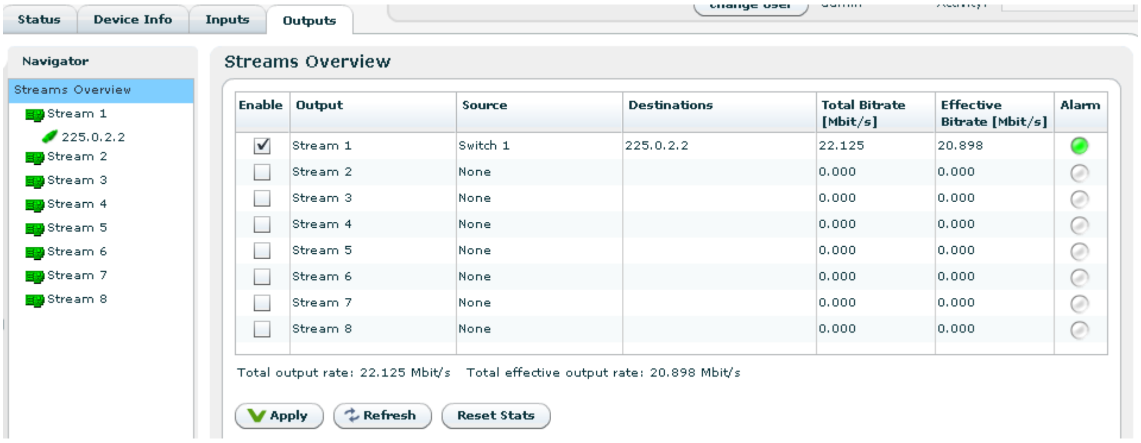
9.6 Streams

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

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

9.6.1 Streams overview

This page shows a short summary of all the device internal 'Streams' and the output(s) allocated to each 'Stream'.



Streams Overview

Enable	Output	Source	Destinations	Total Bitrate [Mbit/s]	Effective Bitrate [Mbit/s]	Alarm
☑	Stream 1	Switch 1	225.0.2.2	22.125	20.898	●
□	Stream 2	None		0.000	0.000	○
□	Stream 3	None		0.000	0.000	○
□	Stream 4	None		0.000	0.000	○
□	Stream 5	None		0.000	0.000	○
□	Stream 6	None		0.000	0.000	○
□	Stream 7	None		0.000	0.000	○
□	Stream 8	None		0.000	0.000	○

Total output rate: 22.125 Mbit/s Total effective output rate: 20.898 Mbit/s

Figure 9.67 Outputs overview

The table has the following columns:

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

Output
: The name of the output, consisting of the user defined name combined with the physical port number.

Source
: The source of the stream; ASI port, switch output or IP interface address

Destination
: The stream destination; ASI port or IP interface address.

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

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

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

9.6.2 Stream

When selecting an output a new page on the right hand side with information about the selected output is displayed. The top part shows the name and the current alarm status of the stream. See figure **Figure 9.68**. All current alarms related to the stream are displayed in a tool tip by holding the mouse cursor over the alarm status indicator.

The tab navigator contains two sub-tabs:

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

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

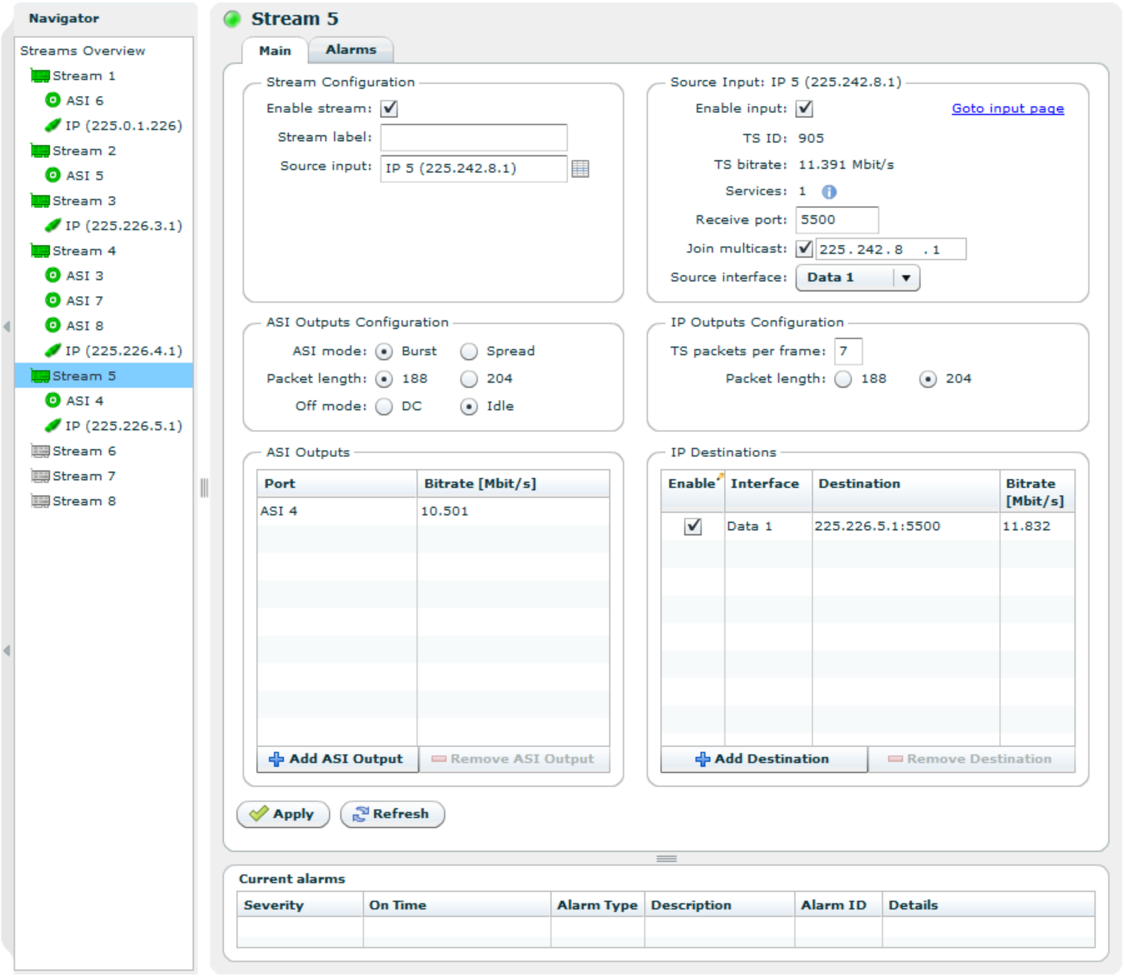
9.6.3 Main

The Main page lets the user configure port parameters for the selected 'Stream', which also includes setting the 'Stream' input source.

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

Enable output
: Enable or disable signal output.

Output label
: This lets the user add a label to the selected output.



Navigator

Streams Overview
- Stream 1
  - ASI 6
  - IP (225.0.1.226)
- Stream 2
  - ASI 5
- Stream 3
  - IP (225.226.3.1)
- Stream 4
  - ASI 3
  - ASI 7
  - ASI 8
  - IP (225.226.4.1)
- Stream 5
  - ASI 4
  - IP (225.226.5.1)
- Stream 6
- Stream 7
- Stream 8

Stream 5

Stream Configuration

Enable stream: ☑

Stream label:

Source input: IP 5 (225.242.8.1)

Source Input: IP 5 (225.242.8.1)

Enable input: ☑ Goto input page

TS ID: 905

TS bitrate: 11.391 Mbit/s

Services: 1

Receive port: 5500

Join multicast: ☑ 225 . 242 . 8 . 1

Source interface: Data 1

ASI Outputs Configuration

ASI mode: ● Burst ○ Spread

Packet length: ● 188 ○ 204

Off mode: ○ DC ● Idle

IP Outputs Configuration

TS packets per frame: 7

Packet length: ○ 188 ● 204

ASI Outputs

Port	Bitrate [Mbit/s]
ASI 4	10.501

IP Destinations

Enable	Interface	Destination	Bitrate [Mbit/s]
☑	Data 1	225.226.5.1:5500	11.832

Current alarms

Severity	On Time	Alarm Type	Description	Alarm ID	Details

Figure 9.68 Stream main page

Source input
: Clicking on the icon to the right of the text box brings up a list of the possible input sources to the stream. Click on the appropriate input source and confirm with the Apply button.

Having selected the input source the Input Source field will reflect the choice and provide input signal status:

Enable input
: Enable or disable signal input.

TS ID
: The transport_stream_ID of the input signal.

TS bitrate
: The bit rate of the input transport stream.

Services
: The number of services carried by the input transport stream. Holding the mouse pointer over the blue i icon brings up a tool-tip listing the transport stream services.

Goto input page
: This link provides a short-cut to configuring the chosen input.

The ASI Outputs Configuration field defines the output format on all ASI ports:

ASI mode
: Burst mode means that transport stream packets may appear in bursts with larger intervals. Spread mode means that the transport stream packets are evenly distributed with shorter, more frequent intervals.

Packet length
: 188 means that the output packets contain 188byte, i.e. do not include the 16 additional bytes for Reed-Solomon error correction. 204 means that these bytes are included.

Off mode
: This parameter controls the behaviour of the ASI signals connected to this stream when the stream does not have any data to transmit, i.e when the input signal is not present. DC means the port is electrically shut down, i.e no signal. Idle means the port is kept up transmitting only idle symbols.

: The intension with this setting is to be able to use simple switching devices on the outputs that use loss of signal as switching criterion.

The ASI Ports field allows selection of any of the ASI ports to output the current stream, provided the port is not used as an input. Click the Add as Output button in the line of the desired port and click Yes in the pop-up box to confirm. The list provides an overview of the status of each ASI port, and the bit rate of the carried transport stream (if any).

The fields IP Outputs Configuration, IP Output Basic Configuration and IP Output Status are only visible if an IP destination has been added for the stream. This is accomplished by clicking the Add Destination button at the page bottom, followed by clicking Yes in the pop-up box to confirm.

The IP Outputs Configuration field:

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

Packet length
: Configures the TS packet length to transmit on the IP layer. Normally this parameter should be set to 188. If set to 204, RS (Reed-Solomon) bytes received on the input signal to the stream will be forwarded onto the IP layer. If the input signal does not contain 204 byte packets, the 16 RS bytes will be filled with a deterministic pattern. Remember that the MTU requirements increase by 16 X the number TS packets per frame when configuring 204 byte TS packets.

The IP Output Basic Configuration field:

Enable
: Enable or disable the IP output.

IP destination address

The IP address of the receiving unit.

Protocol

Select RTP or UDP from the pull-down list.

UDP destination port

The port number used by the receiving unit.

Manual destination interface

A tick in the box allows selection of an interface other than default. The pull-down list provides the possible choices. Click on the desired interface and click Yes in the pop-up box to confirm.

The *IP Output Status* field:

Current interface

Shows the currently used IP interface for the 'Stream'

Resolved

Yes if the destination address has been reached, No otherwise.

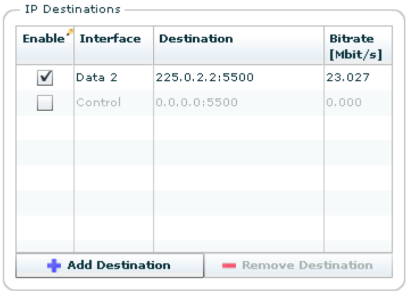
Dest. MAC address

The Ethernet MAC address of the receiving unit.

Total bitrate

The bitrate of the IP stream carrying the transport stream.

If multiple IP outputs are enabled for the same 'Stream' the IP Basic Configuration and IP Output Status fields are replaced by the IP Destinations field, see figure **Figure 9.69**.



IP Destinations

Enable	Interface	Destination	Bitrate [Mbit/s]
☑	Data 2	225.0.2.2:5500	23.027
□	Control	0.0.0.0:5500	0.000

Figure 9.69 Multiple IP destinations

The table contains a tick box to enable or disable each output in addition to showing the status of each output. Each output is configured in the dedicated page, reached by double-clicking on the entry in the table.

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

9.6.4 Alarms

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

9.6.5 Stream to IP destination

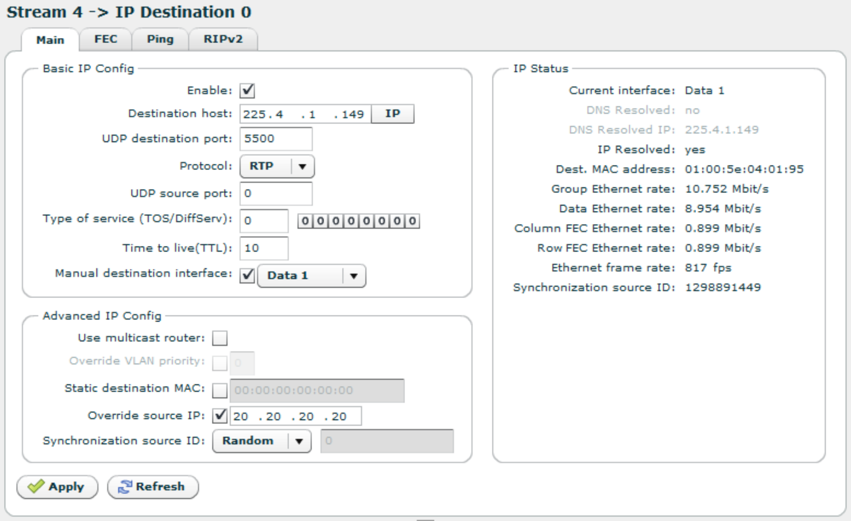
If an IP destination has been allocated to a 'Stream' this is shown in the Outputs navigator list. Refer to 9.70. Clicking the navigator entry opens the page to edit the IP destination settings.

> **Note:** The IP output must be added before configuring it. Refer to **Section 9.6.3**.

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

9.6.5.1 Main

This page is shown in **Figure 9.70**.



Stream 4 -> IP Destination 0

Basic IP Config

Enable: ☑
Destination host: 225 . 4 . 1 . 149 IP
UDP destination port: 5500
Protocol: RTP ▾
UDP source port: 0
Type of service (TOS/DiffServ): 0 0|0|0|0|0|0|0|0
Time to live(TTL): 10
Manual destination interface: ☑ Data 1 ▾

Advanced IP Config

Use multicast router: □
Override VLAN priority: □ 0
Static destination MAC: □ 00:00:00:00:00:00
Override source IP: ☑ 20 . 20 . 20 . 20
Synchronization source ID: Random ▾ 0

IP Status

Current interface: Data 1
DNS Resolved: no
DNS Resolved IP: 225.4.1.149
IP Resolved: yes
Dest. MAC address: 01:00:5e:04:01:95
Group Ethernet rate: 10.752 Mbit/s
Data Ethernet rate: 8.954 Mbit/s
Column FEC Ethernet rate: 0.899 Mbit/s
Row FEC Ethernet rate: 0.899 Mbit/s
Ethernet frame rate: 817 fps
Synchronization source ID: 1298891449

Figure 9.70 IP Configuration.

The Basic IP Config field:

Enable

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

Destination host

Identifies the destination for the data stream. The identification can be set by entering the destination IP address directly, or by specifying the machine's DNS name. Use the button to the right of the field to toggle between the modes.

If you use IP address mode, the address entered may be either a unicast address or a multicast address.

If you use host mode, you can enter a local host name or a fully qualifying host name which includes the domain name. The device will resolve the name to an IP address by asking the DNS server. The DNS name will be regularly queried, and if the name is not resolving any more, the data transmission will be stopped.

DNS servers are either configured manually as described in **Section 9.4.4.2** or automatically when using DHCP, see **Section 9.4.4.1.1.2**.

Protocol

Select UDP or RTP transmission mode. See **Section 6.6.1** for more information on this.

UDP destination port

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

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

UDP source port

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

Type of service (TOS)

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

Time to Live (TTL)

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

Manual destination interface

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

The Advanced IP Config field:

Use multicast router

Click this box to forward the multicast stream to an external multicast router. The unicast IP address to the multicast router can be configured for each Ethernet or SFP interface and also for each VLAN. This IP address must be within the sub-net range. When this option is enabled the multicast MAC destination address will be replaced with a unicast MAC destination address. The unicast MAC destination address is detected by resolving the unicast IP address of the multicast router using ARP. If the ARP request fails, the multicast transmission will not start (or will be stopped). If this option is disabled then the standard multicast destination MAC address will be selected.

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.

SSRC Mode

Option to control SSRC (Synchronization source) identifier field transmitted in RTP header of data stream.

Random

Use a random number as suggested in RFC3550 and allowed by SMPTE2022-1. A new random number is generated every time channel is enabled for transmission. The same random number is shared between all small-casts. **This is the default mode**.

Manual

Configure the SSRC ID field to be used manually. Allowed to adapt to any special requirements or get around compatibility issues.

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.

DNS Resolved

If host name mode for destination host parameter, this field shows whether the name has successfully been resolved to an IP address.

DNS Resolved IP

This field shows the IP address that was found for the specified host name when specifying destionation by name.

IP Resolved

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

Dest. MAC address

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

Group Ethernet rate

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

Data Ethernet rate

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

Column FEC Ethernet rate

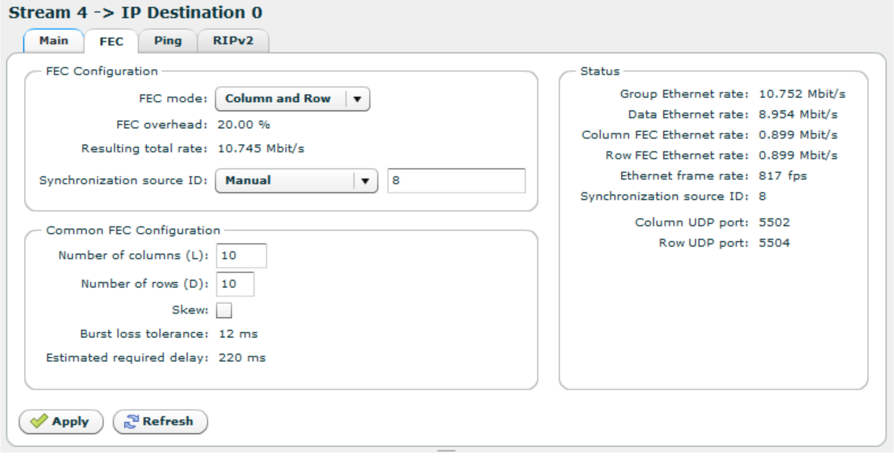
The bitrate of the column FEC contribution to the IP data.

Row FEC Ethernet rate

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

9.6.5.2 FEC

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



Stream 4 -> IP Destination 0

FEC Configuration

FEC mode: Column and Row

FEC overhead: 20.00 %

Resulting total rate: 10.745 Mbit/s

Synchronization source ID: Manual 8

Common FEC Configuration

Number of columns (L): 10

Number of rows (D): 10

Skew: □

Burst loss tolerance: 12 ms

Estimated required delay: 220 ms

Status

Group Ethernet rate: 10.752 Mbit/s

Data Ethernet rate: 8.954 Mbit/s

Column FEC Ethernet rate: 0.899 Mbit/s

Row FEC Ethernet rate: 0.899 Mbit/s

Ethernet frame rate: 817 fps

Synchronization source ID: 8

Column UDP port: 5502

Row UDP port: 5504

Figure 9.71 IP output FEC page

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

FEC mode

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

SSRC Mode

Option to control SSRC (Synchronization source) identifier field transmitted in RTP header of data stream. Normally this parameter should be left at its default setting, but in case of special requirements or compatibility issues, it can be used.

Manual

Configure the SSRC ID field to be used manually. Allowed to adapt to any special requirements or get around compatibility issues.

0 (SMPTE 2022-1)

Transmit the value 0 as specified in SMPTE2022-1 and Cop3. **This is the default setting**.

Follow data stream

Use same value as used on data stream protected by the FEC. If data stream is configured with the default value, Random, the same random number is used on the FEC stream(s).

FEC overhead

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

Resulting total rate

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

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

Number of columns (L)

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

Number of rows (D)

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

Skew

Check this box to enable a skewed FEC matrix.

For a detailed description of FEC usage, refer to **Appendix C**.

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

Group Ethernet rate

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

Data Ethernet rate

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

Column FEC Ethernet rate

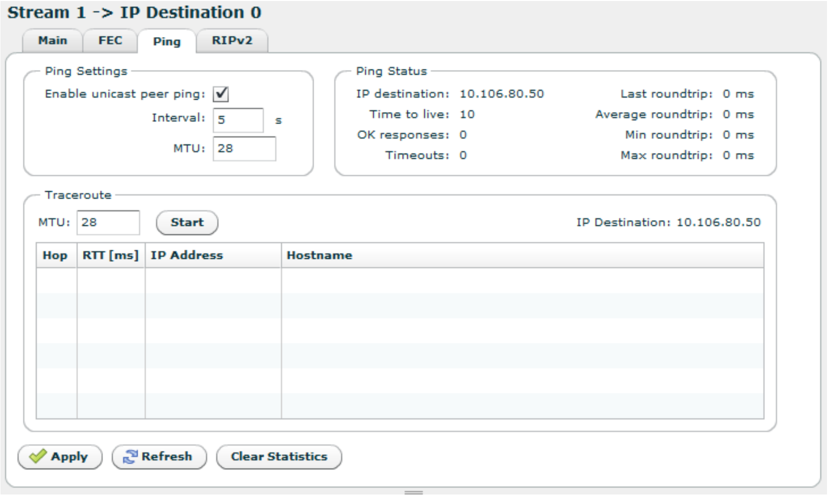
The bitrate of the column FEC contribution to the IP data.

Row FEC Ethernet rate
: The bitrate of the row FEC contribution to the IP data.

Column UDP port
: The UDP port used for column FEC data.

Row UDP port
: The UDP port used for row FEC data.

9.6.5.3 Ping



Stream 1 -> IP Destination 0

Ping Settings

Enable unicast peer ping: ☑
Interval: 5 s
MTU: 28

Ping Status

IP destination: 10.106.80.50
Time to live: 10
OK responses: 0
Timeouts: 0
Last roundtrip: 0 ms
Average roundtrip: 0 ms
Min roundtrip: 0 ms
Max roundtrip: 0 ms

Traceroute

MTU: 28 Start
IP Destination: 10.106.80.50

Hop	RTT [ms]	IP Address	Hostname

Figure 9.72 Ping page

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

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

IP destination
: The address of the device receiving the Ping requests.

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

OK responses

Indicates how many valid Ping responses have been received.

Timeouts

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

Last roundtrip

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

Min roundtrip

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

Max roundtrip

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

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

The Traceroute field enables debugging of network connection with unicast remote host.

See **Section 9.4.4.6.2** for a description of trace route. The IP used is the same as the destination configured for the stream, and the routing follows the interface settings for the stream, so that a manual interface selection overrides the IP routing table.

9.6.6 RIP-2

The TVG425 is equipped with RIP-2 functionality. If enabled, the TVG425 will transmit RIP-2 messages regularly. The content of the RIP-2 messages is set as specified in this section.

RIP-2 messages are sent with one entry each. The metric of this entry can be set either manually or automatically based on the current alarm level of the unit. This information may be used by network routers to select the source with the lowest metric; i.e. in effect automatic redundancy switchover.

> **Note:** Manual destination interface must be enabled when using RIP-2 and source IP must be overridden to identify each stream individually.

Figure 9.73 shows the layout of the RIP-2 page.

The *Related IP Destination Settings* field shows IP destination parameters that RIP-2 depends on.

Manual destination interface

Must be turned on when using RIP2.

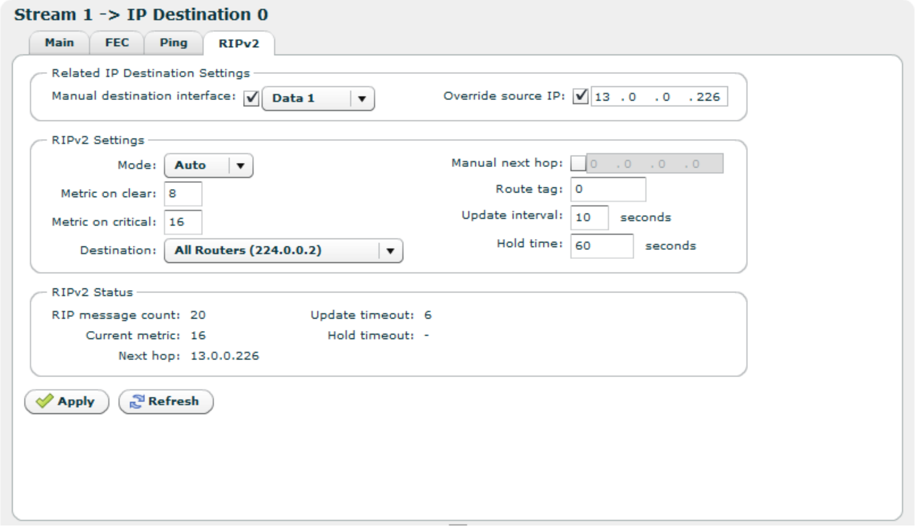
Override source IP

Must be enabled and set to a unique source address for each stream transmitted.

The *RIPv2 Settings* field allow configuring of parameters are as follows:

Mode

Controls the mode of the RIP-2 engine.



Stream 1 -> IP Destination 0

Related IP Destination Settings

Manual destination interface: ☑ Data 1

Override source IP: ☑ 13 .0 .0 .226

RIPv2 Settings

Mode: Auto

Metric on clear: 8

Metric on critical: 16

Destination: All Routers (224.0.0.2)

Manual next hop: □ 0 .0 .0 .0

Route tag: 0

Update interval: 10 seconds

Hold time: 60 seconds

RIPv2 Status

RIP message count: 20

Current metric: 16

Next hop: 13.0.0.226

Update timeout: 6

Hold timeout: -

Figure 9.73 RIP-2 page

Off

No RIP-2 messages are sent.

Auto

RIP-2 messages are sent. The metric in the RIP entry is set according to the current unit alarm state. If the alarm state is critical, the "Metric on critical" value is used. If the alarm state is "OK", the "Metric on clear" value is used.

Alarm

RIP-2 messages are sent. The "Metric on critical" value is used, independently of the alarm state.

Clear

RIP-2 messages are sent. The "Metric on clear" value is used, independently of the alarm state.

Metric on clear

The metric number to be used in the RIP-2 messages when there are no active alarms in the unit.

Metric on critical

The metric number to be used in the RIP-2 messages when there are at least one critical alarm present.

Destination

The IP destination address to use for the RIP messages.

Enable manual next hop

If set, the RIP-2 messages will specify the next hop as defined in the "Next hop address" field.

Next hop address
: The address to be used for the next hop.

Route tag
: Corresponds to the route tag field in the outgoing RIP-2 messages.

Update interval
: Specifies the average update interval for the RIP-2 messages. Note that the TVG425 adds some random delay to avoid sending messages too regularly.

Hold time
: Hysteresis time to keep signaling alarm level metric after alarm level is going from critical to non-critical, to avoid toggling situations when alarm is turned on and off continuously.

The *RIPv2 Status* field show the following parameters:

RIP-2 message count
: The number of RIP-2 messages transmitted.

Current metric
: The current metric used in outgoing RIP-2 messages. Will be either the "Metric on clear" or the "Metric on critical" value.

Next hop
: The next hop address.

9.7 Redundancy

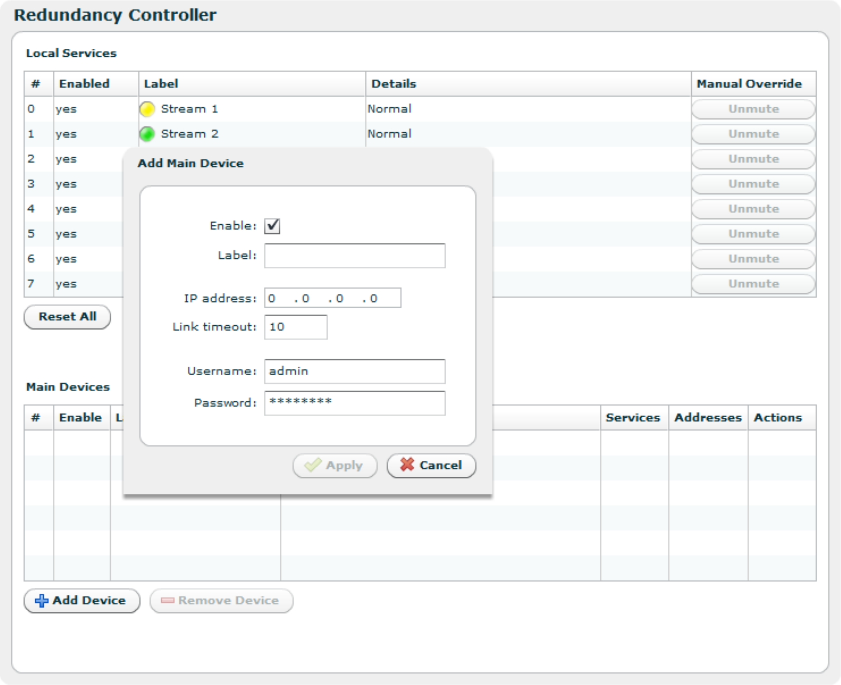
9.7.1 Redundancy Controller

Figure 9.74 shows the user interface. The page is divided into five sections: Settings, Main Device Status, Main Device Statistics, Device Switch Status and Service Redundancy Settings.

Settings
: Allows the user to label this specific redundancy controller and also to enable or disable it.

Main Device Status
: Shows the name, label and alarm status of the main device. It also shows the status of the connection to the main 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. If there is only one IP address configured, there will a single alarm and the IP shown.

Main Device Statistics
: Shows communication statistics against main device. As long as everything is operating correctly, only Polls OK should increment.



Redundancy Controller

Local Services

#	Enabled	Label	Details	Manual Override
0	yes	● Stream 1	Normal	Unmute
1	yes	● Stream 2	Normal	Unmute
2	yes			Unmute
3	yes			Unmute
4	yes			Unmute
5	yes			Unmute
6	yes			Unmute
7	yes			Unmute

Main Devices

#	Enable	L			Services	Addresses	Actions

Add Main Device

Enable: ☑

Label:

IP address: 0 .0 .0 .0

Link timeout: 10

Username: admin

Password: ********

Figure 9.74 The user interface

Device Switch Status

Shows the status of the redundancy controller on a device level. The information shown in this section changes when a global switch is performed, either by an automatic switch to spare or a manual switch. The SNMP switch action state attribute reflects the combined state of the configured SNMP switch actions. If all switch actions are configured to main value the SNMP switch action state is Main. If all switch actions are configured to spare value the SNMP switch action state is Spare. Otherwise the SNMP switch action state is Unknown.

Service Redundancy Settings

This section shows a table of the main and spare services. For each main service the user can configure a spare replacement by using the select box on each row in the Spare service column. When a spare replacement is configured a service switcher is added to the redundancy controller. The service switcher parameters Switch Status, Configuration Received, Switch Mode and Return Mode is shown in the table. Refer to Section 9.7.2 for detailed information on service switchers.

9.7.1.1 Device redundancy controller switching

A device switch can be performed either manually or automatically. Figures 9.75 and 9.76 show redundancy controller state diagrams when switching to spare or main services respectively.

If making a manual switch to spare services, the redundancy controller will try to disable to main services.

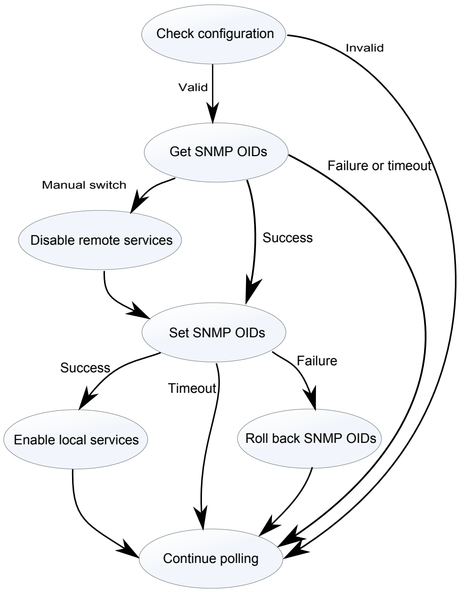


Figure 9.75 The actions performed when the redundancy controller loses contact with the main device.

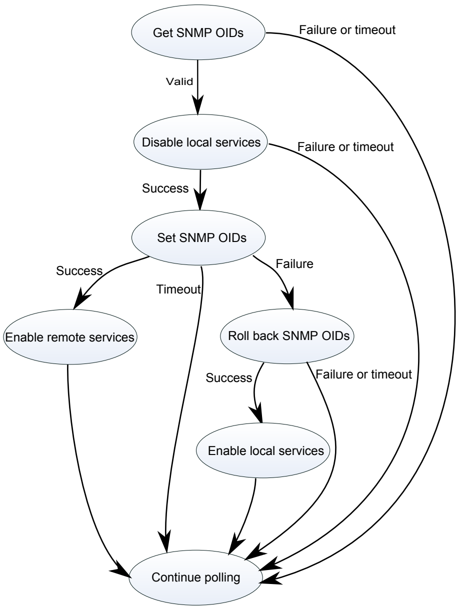


Figure 9.76 The actions performed when a manual redundancy controller switch to main services is forced.

9.7.1.2 Communication

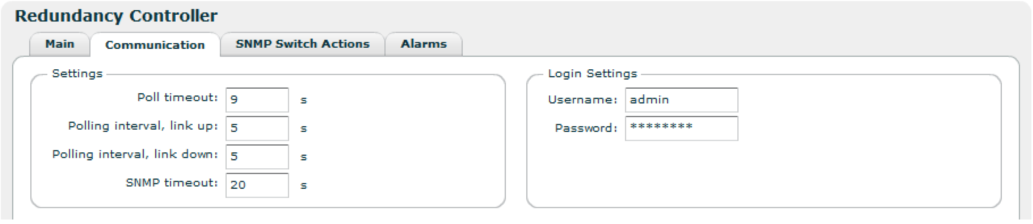
The main device is polled through a set of IP addresses. Loss of contact towards any of these addresses causes an alarm.

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 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 main, Polling interval, link up) and link down (no contact with main, Polling interval, link down) scenarios.

If an authorization error towards any address occurs the redundancy controller cannot resolve the state of the main device. In this case the redundancy controller assumes the main device is healty and will not switch to spare.

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 the main device, each service switcher will be informed that the main device is down. In addition, a set of SNMP actions will be performed.



Poll timeout: 9 s
Polling interval, link up: 5 s
Polling interval, link down: 5 s
SNMP timeout: 20 s

Username: admin
Password: ********

Figure 9.77 Poll settings

Figure 9.77 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 main device are also configurable.

Poll timeout

Configure the number of seconds the Redundancy Controller will attempt contacting the main device before deciding connection is lost. If neither of the IP addresses has been able to contact the main device within Poll timeout seconds the Redundancy Controller will assume that the main device is not operational and perform a switch to spare device. Poll timeout should be set by considering the Max RTT value per IP address. Should be set some seconds higher that the lowest Max RTT value. If set too low the Redundancy Controller might switch to spare device, even if main device is operational.

Polling interval, link up

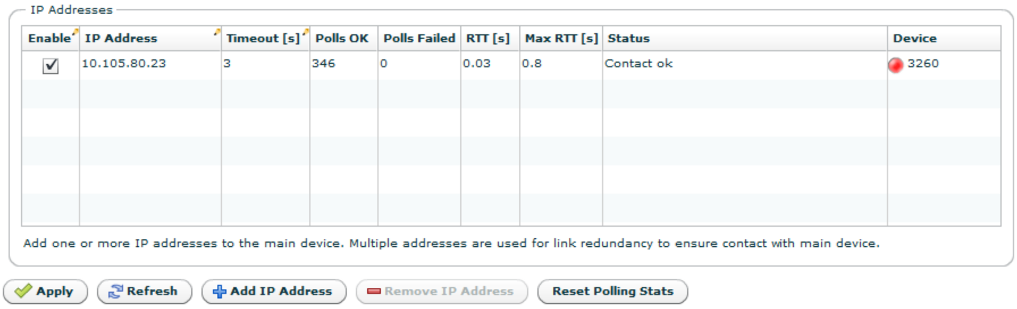
Number of seconds between each poll when the link to the main device is OK. This parameter effectively controls the responsiveness of switching to a spare service based on the alarm level of the main service. Should be set low, but might stress the IP infrastructure.

Polling interval, link down

Number of seconds between each poll when the link to the main device is not OK. This parameter controls how fast the Redundancy Controller detects that the link to main device is OK. Should be set low, but might stress the IP infrastructure.

SNMP timeout

NUmber of seconds to wait on response when issuing SNMP Set and SNMP Get commands. An alarm will be raised if operation times out.



IP Addresses

Enable	IP Address	Timeout [s]	Polls OK	Polls Failed	RTT [s]	Max RTT [s]	Status	Device
☑	10.105.80.23	3	346	0	0.03	0.8	Contact ok	● 3260

Add one or more IP addresses to the main device. Multiple addresses are used for link redundancy to ensure contact with main device.

Figure 9.78 The IP Addresses to the main device

Figure 9.78 shows the IP address configuration. At least one IP address must be provided to contact the main device, but in the case of link redundancy, multiple IP addresses may be configured. If so, the Redudancy Controller will use all links to reach the same main device. All IP addresses in the list must therefore end at the same physical device.

Each entry in the list has three configurable fields:

Enable

Enable usage of the IP address. If disabled the Redudancy Controller will not contact this IP address.

IP Address

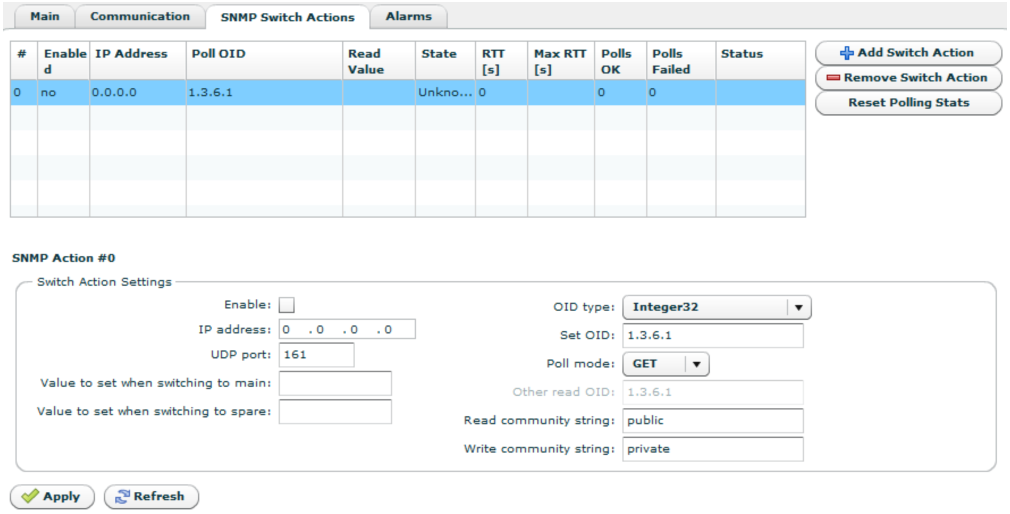
Configure the IPv4 IP address to contact.

Timeout

Configure a poll timeout for each IP address in seconds. If contacting the IP address takes less time than the configured Timeout value, Polls OK will be incremented and the Round trip time (RTT) will be measured. If however the the poll duration is higher than the configured Timeout value, Polls failed will be incremented. Most importantly, a failed poll in itself will not make the Redundancy Controller switch. See the description of the Poll timeout above on how the Redundancy Controller decides to switch on link loss.

Basic poll statistics are provided to measure the round trip time between the main and spare device. 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 timeout **and** not be lower than the maximum measured round trip time.

9.7.1.3 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		Unkno...	0		0	0	

SNMP Action #0

Switch Action Settings

Enable:	□	OID type:	Integer32
IP address:	0 .0 .0 .0	Set OID:	1.3.6.1
UDP port:	161	Poll mode:	GET
Value to set when switching to main:		Other read OID:	1.3.6.1
Value to set when switching to spare:		Read community string:	public
		Write community string:	private

Figure 9.79 The SNMP switch actions

Figure 9.79 shows the SNMP switch action configuration. Note that these OIDs are only set after a loss of contact with the main device or when manually switching the entire redundancy controller between main and spare services, i.e. during a device switch. The OIDs are not set when switching a single service switcher between main and spare.

Basic poll statistics are provided to measure the round trip time between the main and spare device. 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 main value if the link to the main device is up and spare value if the link is down. The get oid mode just reads the oid. The get other oid reads the Other read OID.

9.7.2 Service switchers

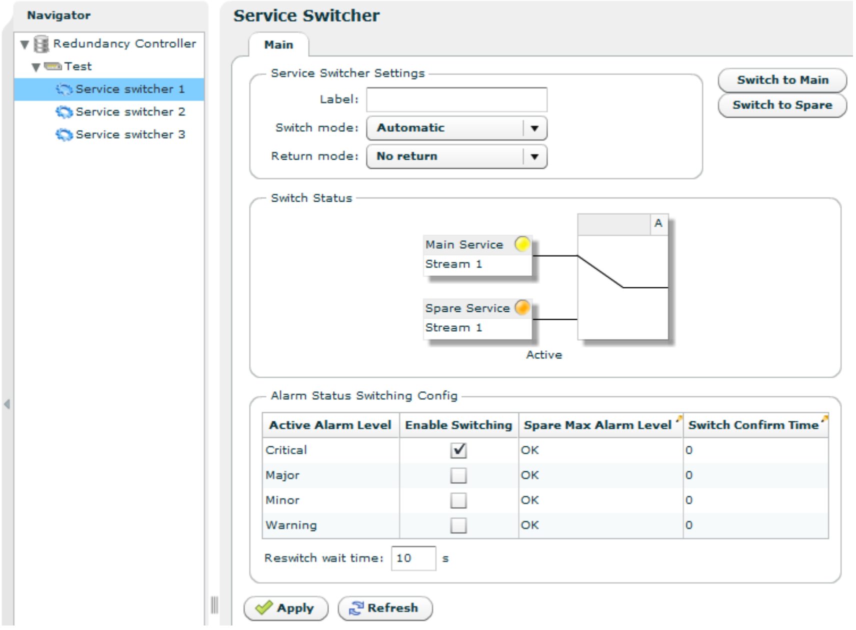
A service switcher is assigned to each pair of main and spare services. As long as the Redundancy Controller has contact with the main device, the service switcher will acquire the current status and configuration.

The service switchers are added by selecting a Spare Service for a Main service as shown in Figure 9.74.

The service switcher does not perform a switchover unless it has received a valid configuration.

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:



Service Switcher Settings

Label:

Switch mode: Automatic

Return mode: No return

Alarm Status Switching Config

Active Alarm Level	Enable Switching	Spare Max Alarm Level	Switch Confirm Time
Critical	☑	OK	0
Major	□	OK	0
Minor	□	OK	0
Warning	□	OK	0

Reswitch wait time: 10 s

Figure 9.80 The service switcher configuration page

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 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 main service. After a switch to the spare service has been performed, the spare device continues to poll the main device. When the main 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 spare alarm", "No return".

Return if OK

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

Return if spare alarm

This option will return automatically to the main device if the main device has recovered **and** the spare device 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 main.

10 SNMP

The product supports SNMP – Simple Network Management Protocol – for remote control and supervision. SNMP uses an extensible design, where management information bases (MIBs) describe the structure of the management data of a device subsystem. The primary purpose of SNMP is to export alarm and status information, but a range of MIBs related to configuration settings are also supported.

10.1 SNMP agent characteristics

The SNMP agent supports the SNMPv2c (Community based SNMPv2) protocol. All custom MIBS are written in SMIv2 format. The SNMP agent will accept both SNMPv1 and SNMPv2 messages. The SNMP agent uses the normal UDP sockets for communication and listens for requests at UDP port 161.

Both legacy SNMPv1 traps and SNMPv2 notifications are supported. It is however recommended to use the new SNMPv2 notification types for new deployments.

10.2 MIB naming conventions

All custom MIB files start with the prefix `VIGW`. MIBs that defines data structures that are not connected to one specific product start with `VIGW-PLAT`. Most MIBs are of generic type and therefore starts with this prefix.

Some MIB-files are very custom and corresponds to a specific product only. These MIBs start stats with the prefix `VIGW-PROD`.

10.3 MIB overview

This section describes the different MIBs. Detailed description of MIBs is included later on in this document.

10.3.1 Supported standard MIBs

RFC1213-MIB

MIB-II according to RFC1213.

10.3.2 Custom MIBs

VIGW-TC-MIB

Describes common textual conventions (data types etc.) used throughout the entire MIB set. For example, definition of alarm status numbers are defined in this MIB.

VIGW-BASE-MIB

Defines the top level MIB structure including the enterprise specific root node for device control (1.3.6.1.4.1.22909).

VIGW-UNIT-MIB

This is a generic MIB module that defines parameters supported by all products. It is the main source for alarm and status related information. The following objects are examples of contents in this MIB:

- Top level alarm status
- Table of current alarms
- History of last transmitted TRAP messages
- Trap destination list
- Force reset of the unit
- TRAP/NOTIFICATION definitions
- Other, general product information:
  - Serial number
  - SW version

> **Note:** When setting values in the unitAddressTable it is important to send all values for one interface in the same request. This is to prevent the unit from entering an undefined intermediate state.

VIGW-PLAT-TS-MIB

This MIB contains Transport Stream related information for each of the transport stream inputs. It is supported by transport stream related products that are able to analyse incoming transport streams. For each input transport stream, the following information is available:

- Transport stream sync status and total/effective bitrate.
- Present PIDs with information about bit rates and CC errors.
- Present services with information about service name and service ID.

VIGW-PLAT-TSOUT-MIB

This MIB is supported by products that can generate an outgoing transport stream. Parameters include:

- Control of output bitrate and other ASI parameters (spread/burst mode).
- Control of MIP insertion (if enabled in the product)
  - OFDM modulation parameters
  - Enable/disable of MIP insertion
- Control of PSI/SI/PSIP table playout

VIGW-PLAT-SWITCH-MIB

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

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

VIGW-PLAT-TS-INPUTSWITCHING-MIB

MIB containing parameters related to control of second generation input port redundancy switch with more than 2 sources.

VIGW-PLAT-IPTRANSPORT-MIB

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

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

VIGW-PLAT-VIDEO-MIB

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

Examples of included information are:

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

VIGW-PLAT-RF-MON-MIB

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

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

10.4 SNMP related configuration settings

The SNMP related configuration parameters are located on the Device Info/SNMP settings page in the GUI.

10.4.1 Community strings

The community strings are used to provide simple password protection for SNMP read and write requests. The strings can be configured from the GUI. It is also possible to configure the community strings to be used for trap messages.

10.4.2 Trap destination table

The Trap Destination table lets the user configure the external entities that should receive SNMP traps from the device. The table is both accessible via `VIGW-UNIT-MIB` and the product GUI (Device Info/SNMP settings). A maximum of 8 different destinations are supported.

10.4.3 Trap configuration

All supported traps are currently defined in the `VIGW-UNIT-MIB`. Via the GUI you can control the trap forwarding. For detailed information about each trap and the corresponding variable bindings, please see **Section 10.5**.

Trap version

This parameter controls the TRAPs that will be sent from the device in case of alarm conditions.

SNMPv1 (Legacy)

If this option is selected, the unit will send the traps located under the `vigwLegacyTraps` MIB node. These traps are included mostly for historical reasons and it is not recommended to use these for new deployments.

SNMPv2

This is the recommended setting. The traps defined under the node `unitNotifications` will be used while the traps under the node `vigwLegacyTraps` will be disabled.

Status change traps

If enabled, the unit will transmit `unitAlarmStatusChanged` traps whenever the top level alarm status is changed for the unit.

Alarm event forwarding

This setting controls how internal alarm event will be forwarded as TRAP messages. Adjust this value if you want to control the number of traps sent from the unit. The settings are only used when SNMPv2 is selected as TRAP version. The settings are:

Disabled

No specific event traps are transmitted when alarms are raised or cleared. (The `unitAlarmStatusChanged` trap may however be transmitted).

Basic

The device forwards alarms as traps on a basic level. No information about `subid3` will be transmitted.

Detailed

The device forwards alarms as traps. If there are sub-entries that are using the `subid3` value, each sub.entry will be transmitted in separate trap messages.

10.5 Alarm/status related SNMP TRAPs

All TRAP messages are defined in `VIGW-UNIT-MIB`. This section describes each trap message.

10.5.1 The main trap messages

The main (SNMPv2) trap messages are defined under the `unitNotifications` node in `VIGW-UNIT-MIB`. The messages are described briefly in **Table 10.1**.

Table 10.1 List of SNMPv2 traps

`unitAlarmStatusChanged`	This trap is sent when the top level unit alarm status (indicated by the `unitAlarmStatus` variable) changes. The trap indicates both the old and new alarm level. Transmission of this trap type can be enabled/disabled through configuration.
`unitAlarmAsserted`	This trap is sent when an internal alarm is raised. No `subid3` information is included. A corresponding `unitAlarmCleared` trap is sent when the alarm cause is cleared.
`unitAlarmCleared`	This trap is sent when an alarm condition previously indicated with `unitAlarmAsserted` is cleared.
`unitAlarmEvent`	This trap is sent when an alarm event (with no on/off state) is generated. No corresponding "cleared" message is expected for these traps. A typical example is an event like "User logged in".
`unitDetailedAlarmAsserted`	This trap is a more detailed version of `unitAlarmAsserted`. `subid3` information is included in addition to the basic parameters defined in `unitAlarmAsserted`.
`unitDetailedAlarmCleared`	This trap is sent when an alarm condition previously indicated with `unitDetailedAlarmAsserted` is cleared.
`unitDetailedAlarmEvent`	This is a more detailed version of `unitAlarmEvent`. `subid3` information is included in addition to the basic parameters defined in `unitAlarmEvent`.

10.5.2 Severity indications

All alarm event traps (i.e. all traps defined in **Table 10.1** except `unitAlarmStatusChanged`) contain a severity field which is encoded according to the definition below:

Severity	Description
1	Cleared
2	Indeterminate
3	Warning
4	Minor
5	Major
6	Critical

10.5.3 Alarm event fields

A description of the fields in the alarm event traps is presented in **Table 10.2**. Most of the fields are entries from the `unitEventHistoryTable`. The instance identifier for each variable binding corresponds to the index in this table. This index is of kind `CircularLog` and will wrap around at 2^{32}.

Table 10.2 Variables in SNMPv2 traps and their meanings

Field	Description
`unitEventSeverity`	This field indicates the severity of the alarm, 2-6. 1 will never be used, as this condition is indicated by transmitting a `unitAlarmCleared` message.
`unitEventAlarmType`	This is an integer that describes the alarm type. Please refer to alarm documentation for description. From this type, one can extract the actual meaning of the `subid1` and `subid2` values in the message.
`unitEventAlarmId`	A unique identifier for this alarm type. Refer to alarm documentation in the user manual for values.
`unitEventAlarmName`	A fixed name corresponding to the alarm id.
`unitEventRefNumber`	This field is provided to easily match asserted/cleared alarms. In the cleared alarm it is set to the same number as in the asserted alarm.
`unitEventSubId1`	The first subidentifier to identify the source of the alarm. For products with single base boards it is typically set to a fixed value (0 or 1) and can be ignored.
`unitEventSubId2`	This field's purpose is dependent on the alarm type (alarm id). For some alarms it is not used and set to zero. For other alarms, it may e.g. indicate the channel/port number for the entity that generated the alarm.
`unitEventSubId3`	This field provide an even more detailed description of the alarm source. This field is only present in the "detailed" type of trap messages (`unitDetailedAlarmAsserted`, `unitDetailedAlarmEvent`). It's usage is dependent on the alarm ID. For example, in transport stream related alarms, `subid3` is used to indicate the PID value that caused the alarm.
`unitEventSourceText`	A textual description of the source of the alarm. This is typically a textual description of the `subid1` and `subid2` fields. For example, for transport stream related alarms, the text indicates the name (with label) of the port that generated the alarm.
`unitEventSubId3Label`	This field is fixed and indicates the label (meaning) of the `subid3` field, contained in the `unitEventSubId3` variable. It is intended to make it easy to log the alarm.
`unitEventDetails`	This is a generic text string that contains more details related to the alarm event. It's usage and content is dependent on the alarm ID.
`unitAlarmStatus`	This variable contains the new, top level alarm status of the unit *after* the condition leading to this trap messsage. It may be used to quickly update the top level status for the device after receiving the trap message.

10.5.4 Matching of on/off traps

As mentioned previously, a unitAlarmCleared message is sent after a unitAlarmAsserted message and a unitDetailedAlarmCleared message is sent after a unitDetailedAlarmAsserted message.

The "cleared" event contains exactly the same identifiers as the "asserted" trap. This includes the alarm ID, subid1, subid2 and subid3 fields. This set of four identifiers uniquely identifies the source of an alarm.

A more easy way to match the traps is by using the unitEventRefNumber field. This is a simple integer that is the same in an "asserted" trap and in a "clear" trap.

10.5.5 Legacy trap messages

Note: The information in this section relates to trap definitions that are marked as deprecated in VIGW-UNIT-MIB. They are included for backwards compatibility with earlier product versions and should not be used for new deployments.

The legacy traps are defined under the vigwLegacyTraps node. Transmission of these traps is specified by selecting "SNMPv1 (Legacy)" for the trap version field. The format of these traps follow the SNMPv1 trap format.

In contrast to the SNMPv2 alarm messages, the SNMPv1 messages has its severity implicitly encoded in the trap type.

The trap messages are defined in **Table 10.3**.

Table 10.3 List of legacy (SNMPv1) traps

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

All these trap messages contain variable bindings from the unitTrapHistoryTable. This table is filled up with historical trap messages, only when SNMPv1 mode is selected.

The fields in these traps are fetched from the unitAlarmTrapHistoryTable. The meaning of these fields correspond to the fields in the unitEventHistoryTable for SNMPv2 traps and are not described in more detail here.

10.6 Using net-snmp to access MIB information

Net-SNMP is a useful collection of free command line tools that can be downloaded from http://www.net-snmp.org/. The WEB site provides installation packages for several operating systems, including Windows.

The most important tools that can be utilized in scripts etc. is `snmpget` for get operations and `snmpset` for set operations.

The WEB site and the tools provides extensive usage information. We do however present some examples in this chapter for convenience.

10.6.1 Reading a parameter with snmpget

The command line tool to read an SNMP parameter is `snmpget`. The following example shows how the command is used to read system up time from a device:

```
snmpget -v 2c -c public <ip-address> sysUpTime.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (250792000) 29 days, 0:38:40.00
```

Note the following parameters used:

`-v 2c`
: This indicates that the version to be used is 2c. This is important as the default value is 3, which is currently not supported.

`-c public`
: This is the community string (password) used for the request. It should match the configured SNMP agent settings. The default value is “public”.

`<ip-address>`
: This is the IP address for the device to read from.

`sysUpTime.0`
: This is the OID for the parameter to read. Since we read a scalar value, we need to add `.0` to the OID from the MIB. Note that it is legal to use a numerical OID in this list; the OID must match the parameter definition in the MIB file.

10.6.2 Writing a parameter with snmpset

The command line tool to set an SNMP parameter is `snmpset`. The following example shows how the command is used to change the system name (`sysName`) for a device:

```
snmpset -v 2c -c private <ip-address> sysName.0 s "New name"
SNMPv2-MIB::sysName.0 = STRING: Siggens
```

Note the following parameters used:

`-v 2c`
: This indicates that the version to be used is 2c. This is important as the default value is 3, which is currently not supported.

`-c private`
: This is the community string (password) used for the request. It should match the configured SNMP agent settings. The default value for write access is “private”.

`<ip-address>`
: This is the IP address for the device.

`sysName.0`
: This is the OID for the parameter to change. Since we read a scalar value, we need to add `.0` to the OID from the MIB. Note that it is legal to use a numerical OID in this list; the OID must match the parameter definition in the MIB file.

`s "New name"`
: This is the parameter type and value. We use “s” to indicate a string and “New name” is the actual string value. The type should match the type defined in the MIB file.

11 Preventive Maintenance and Fault-finding

This chapter provides the schedules and instructions, where applicable, for routine inspection, cleaning and maintenance of the TVG425, 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 TVG425 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 Nevion.

In case of equipment failure unplug the unit from the power and refer servicing to qualified personnel with information of the failure conditions:

- The power supply cord or plug is damaged
- Liquid has been spilled or objects have fallen into the product
- Product has been exposed to rain or water
- Product does not operate normally when following the operating instructions
- Product has been dropped or has been damaged
- Product exhibits a distinct change in performance

11.1.4 Warranty

The TVG425 is covered by standard Nevion warranty service for a period of 24 months following the date of delivery.

The warranty covers the following:

- All defects in material and workmanship (hardware only) under normal use and service.
- All parts and labour charges
- Return of the repaired item to the customer, postage paid.
- Customer assistance through Nevion Customer Service Help Line

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

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 Nevion trained and approved service engineers are permitted to service this equipment.

> ⚠ **Caution:** Unauthorised maintenance or the use of non-approved replacement parts may affect the equipment specification and will invalidate any warranties.

If the following information fails to clear the abnormal condition, please contact your local reseller or Nevion customer care.

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 Nevion 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 TVG425 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 TVG425. 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 TVG425 to Nevion, contact your local Nevion reseller or Nevion directly for additional advice.

1. Write the following information on a tag and attach it to the TVG425.
   - Name and address of the owner
   - Model number
   - Serial number
   - Description of service required or failure indication.
2. Package the TVG425.
   - The original shipping containers or other adequate packing containers must be be used.
3. Seal the shipping container securely, and mark it FRAGILE.

Appendix A Glossary

1000Base-T

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

3G-SDI

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

ARP

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

ATSC

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

DiffServ

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

DVB

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

DVB ASI

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

DWDM

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

Ethernet

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

FEC

Forward Error Correction. A mechanism to protect data transmission by adding redundant information. Increasing the amount of redundant data will enable the receiver to correct more errors (i.e. regenerate lost packets) in case of network data loss.

HD-SDI

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

HDTV

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

HTTP

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

ICMP

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

IGMP

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

JPEG2000

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

Meta-data

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

MPEG-2

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

MPLS

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

MPTS

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

Multicast

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

MXF

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

NMS

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

PCR

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

PID

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

PSI/SI/PSIP

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

QAM

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

QoS

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

QPSK

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

RIP2

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

RSVP

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

RTP

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

SD-SDI

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

SDI

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

SDP

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

SDTI

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

SDTV

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

SFP

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

SIP

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

SNDU

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

SNMP

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

SNTP

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

SPTS

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

TCP

Transmission Control Protocol. A “reliable” protocol above the IP layer that provides automatic retransmission of datagrams in case of packet loss, making it very robust and tolerant against network errors. TCP is the fundamental protocol used in the Internet for WEB traffic (HTTP protocol). TCP is indented for point-to-point 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 illegaly distributed content. Watermarks are invisible to the viewer.

XML

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

Appendix B Technical Specification

B.1 Physical details

B.1.1 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.2 Environmental conditions

Table B.1 Environmental specification

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

B.3 Power

B.3.1 AC Mains supply

Table B.2 AC Power Supply Specification

Rated voltage	100-240 VAC
Voltage tolerance limits	85-264 VAC
Rated frequency	50/60 Hz
Rated current	0.7 A
Power consumption	< 50 W

B.3.2 DC supply

Table B.3 DC Power Supply Specification

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

Table B.4 Physical details

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

B.4 Input/output ports

B.4.1 DVB ASI port

Table B.5 ASI Port Specification

Type	ASI-C, Coaxial cable
Connector type	BNC 75 Ω socket
Signal	Compliant with ETSI EN 50083-9 (DVB A010 rev.1)
Line rate	270 Mbit/s +/- 100 ppm
Data rate	0.1 - 213 Mbit/s
Packet length	188 or 204 bytes
Max cable length (Belden 8281 type)	300 m typical

B.4.2 Ethernet management port

Table B.6 Ethernet Management Port Specification

Type	10/100Base-T
Connector type	RJ45

B.4.3 Ethernet data port

Table B.7 Ethernet Data Port Specification

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

Table B.8 Optional SFP Ethernet Data Port Specification

Type	Gigabit Ethernet, Small Form-Factor Pluggable (SFP) slot to carry copper or optical SFP, compatible with approved modules conforming to the Small Form-factor Pluggable Transceiver Multi Source agreements (Sept. 14, 2000).

B.4.4 Serial USB interface

Table B.9 USB port specification

USB 1.1
Compatible with USB 2.0
Mini USB Connector

B.5 Alarm ports

B.5.1 Alarm relay/reset port specification

Table B.10 Alarm Relay and Reset Port Specification

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

Table B.11 Alarm Relay and Reset Port Pin Out

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

B.6 External reference

B.6.1 10MHz/1 PPS input

Connector type	BNC 50 Ω socket

B.7 Compliance

B.7.1 Safety

The equipment has been designed to meet the following safety requirements: **Table B.12**.

Table B.12 Safety requirements met.

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

B.7.2 Electromagnetic compatibility - EMC

The equipment has been designed to meet the following EMC requirements:

EN 55022 and AS/NZS 3548 (European, Australian and New Zealand)
Emission Standards Limits and methods of measurement of radio frequency interference characteristics of information technology equipment - Class A.

EN 61000-3-2 (European)
Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

EN 50082-1 (European)
Generic Immunity Standard Part 1: Domestic, commercial and light industry environment.

FCC (USA)
Conducted and radiated emission limits for a Class A digital device, pursuant to the Code of Federal Regulations (CFR) Title 47-Telecommunications, Part 15: radio frequency devices, sub part B -Unintentional Radiators.

B.7.3 CE marking

The CE mark indicates compliance with the following directives:

89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility.

73/23/EEC of 19 February 1973 on the harmonisation of the laws of the Member States relating to electrical equipment designed for the use within certain voltage limits.

1999/5/EC of March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity.

B.7.4 Interface to “public telecommunication system”

The equipment is not constructed for electrical connection directly to a “public telecommunication system”. None of the signals shall be connected directly from the unit to a “public telecommunication system” leaving the building without using some kind of interface in between such as a telecom terminal, switch or similar unit. Such kind of buffer is required to achieve a protective electrical barrier between the “public telecommunication system” and the unit. This electrical barrier is required to achieve protection against lightening or faults in nearby electrical installations.

Appendix C Forward Error Correction in IP Networks

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

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

C.1 IP stream distortion

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

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

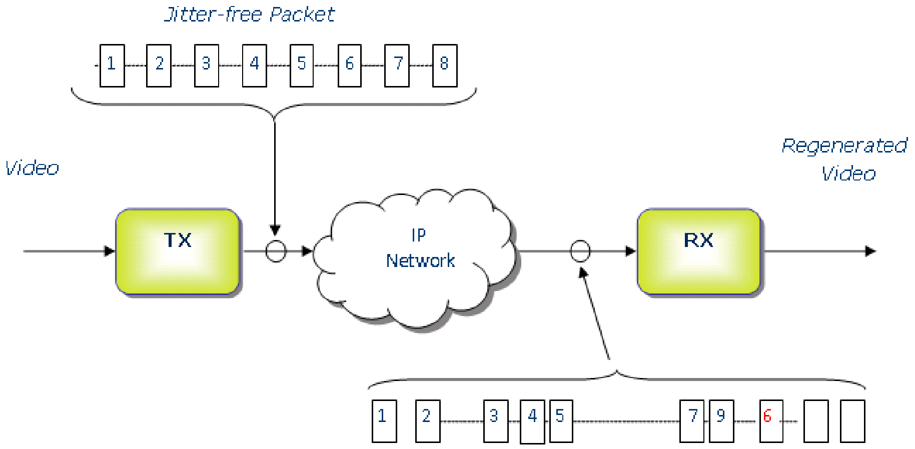


Figure C.1 Impairments of an IP packet stream

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

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

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

C.2 Standardisation

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

C.3 FEC matrix

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

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

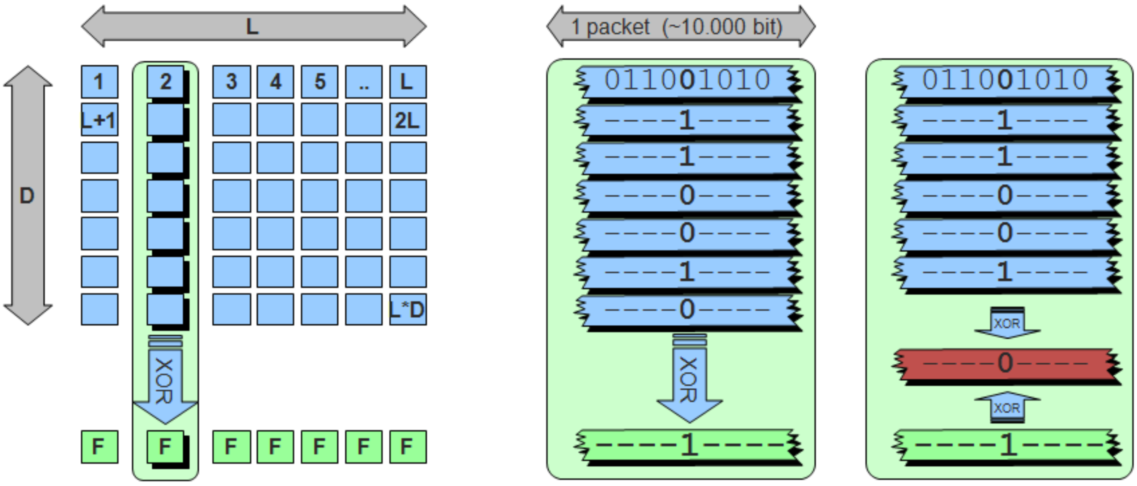


Figure C.2 IP packet FEC calculation matrix

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

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

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

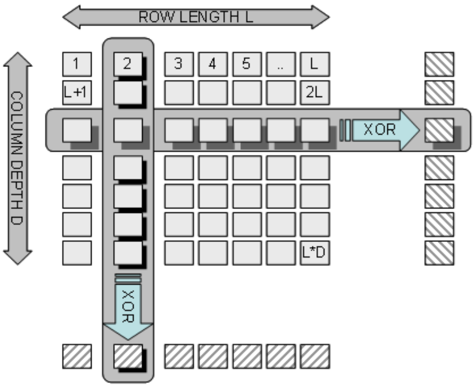


Figure C.3 Two-dimensional FEC calculation matrix

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

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

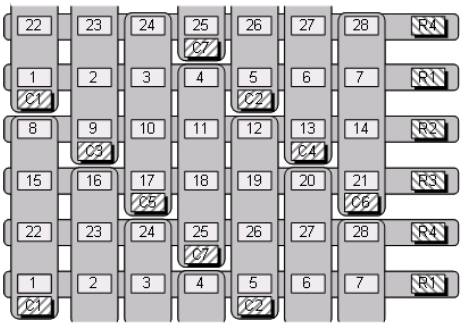


Figure C.4 FEC matrix with column offset

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

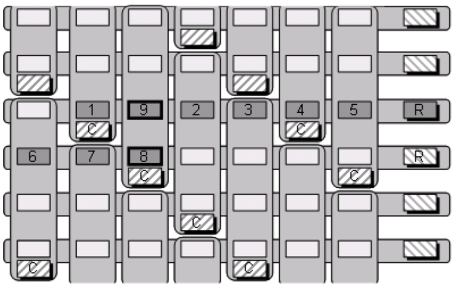


Figure C.5 Offset FEC matrix with missing packets

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

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

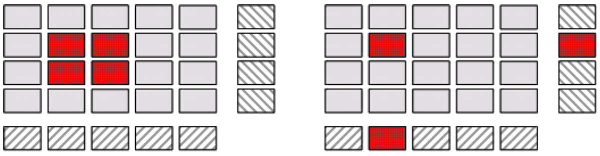


Figure C.6 Uncorrectable error patterns

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.

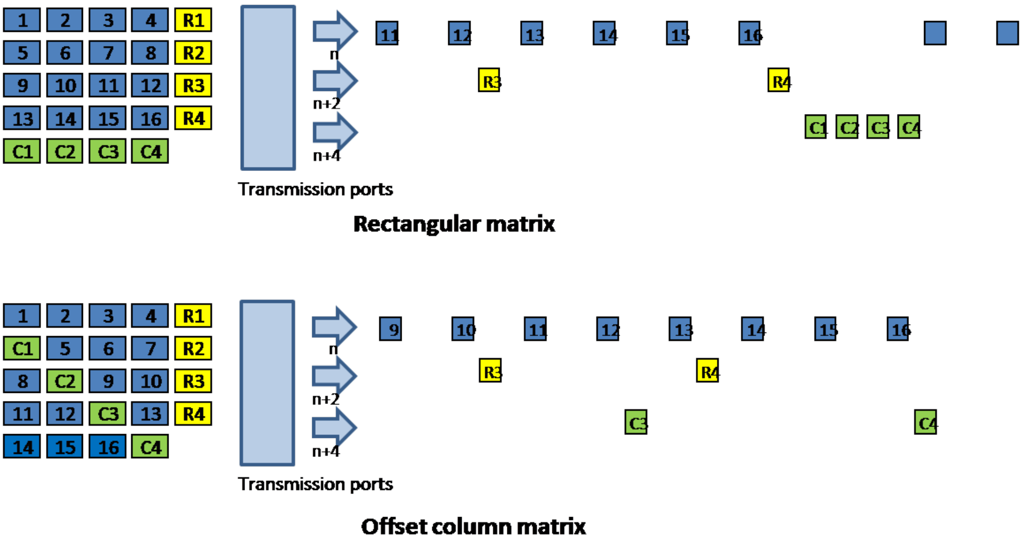
The specifications allow several parameter combinations for the FEC stream generation. The FEC matrix sizes can in principle be chosen at will to suit the operational conditions. Operators may easily be confused by the number of options, and it is not straightforward to choose the optimal FEC setting 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.



Rectangular matrix

Offset column matrix

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.

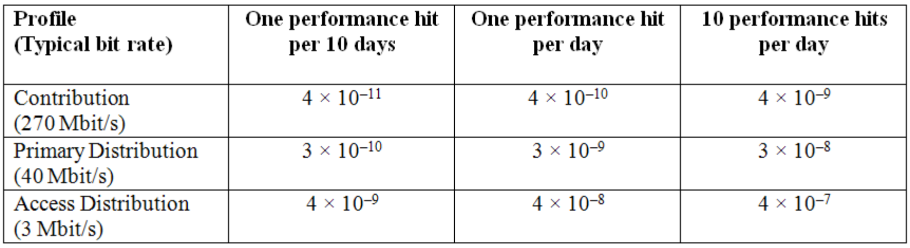
There are three main factors that cause packet loss:

- 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 x 10^{-6}, but occasionally a link may become degraded showing PLR figures like 3 x 10^{-3}. The performance will vary over the day with the lowest performance tending to occur at about the same time every weekday and lasting for one-half to one hour. The FEC setting should be set up to handle this peak hour with low residual loss.

The table of **Figure C.8** shows the IP network performance figures to meet the quality requirements of various grades of television services, as given by ITU recommendation Y.1541 **[10]**. Along these lines the DVB IPTV standard sets the performance requirement for a 4Mbit/s IPTV service at 1 visible error per hour, which means an IP packet loss ratio of 1x10^{-6}.



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

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

C.6 Error improvement

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

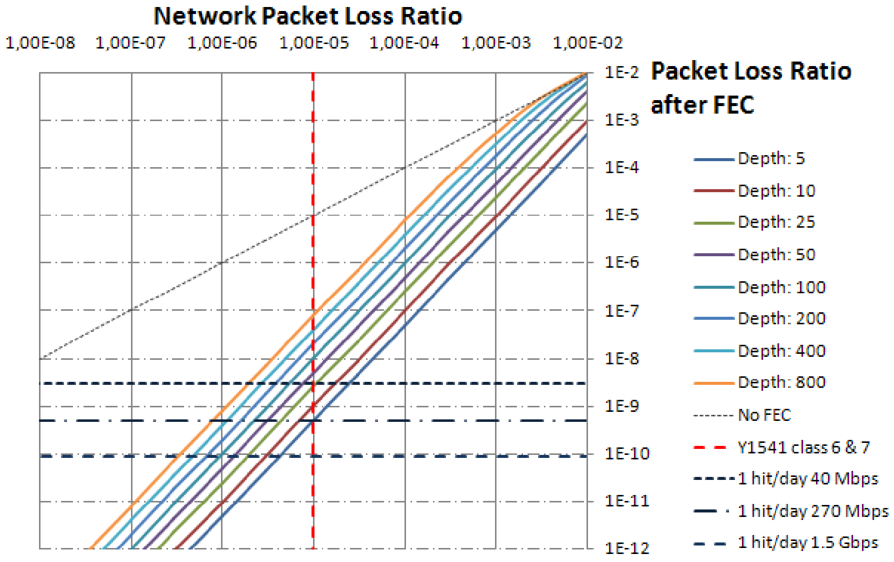


Figure C.9 Error improvement using column FEC only

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

For ease of reference the diagram indicates packet loss rates resulting in one visible impairment (error hit) per day at transport stream bit rates of 40Mb/s, 270Mb/s and 1,5Gb/s, respectively. It can be seen that in a network with worst hour packet loss rate of 3x10^{-3} it is not possible to provide distribution of a 3Mb/s transport stream with less that 10 hits per day (i.e. packet loss rate of 4x10^{-7}, as recommended in Figure C.8) using column-only FEC. In IP networks of ITU class 6 and 7 however, column-only FEC with reasonably small column depths will perform nicely for bit rates up to 270Mb/s.

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

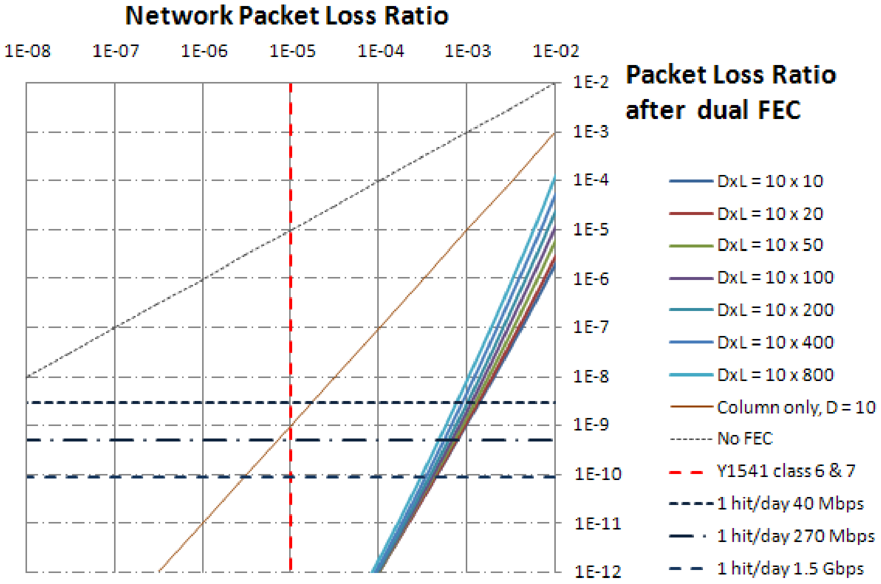


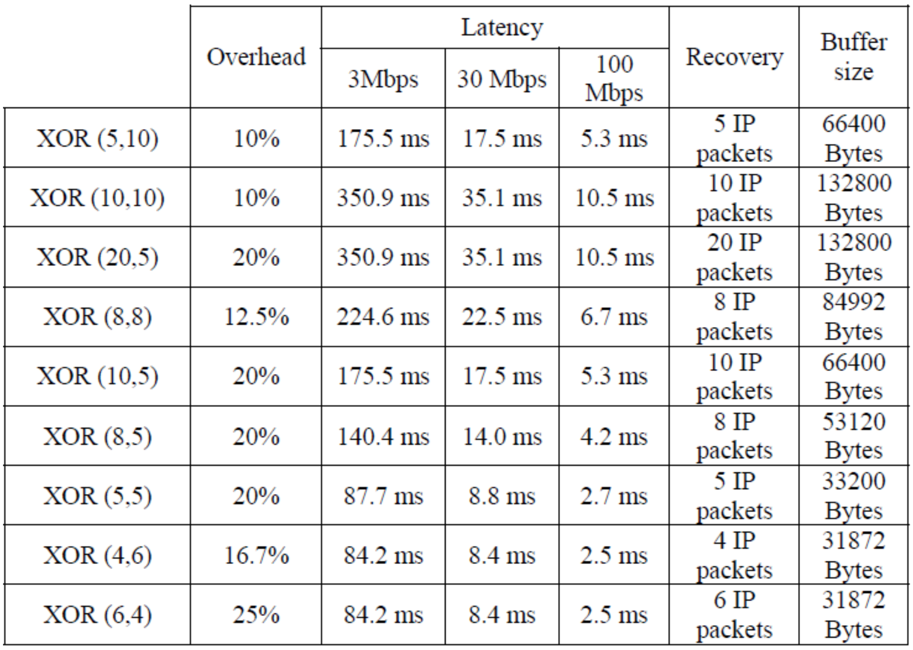
Figure C.10 Error improvement using two-dimensional FEC

Figure C.10 shows how adding row FEC dramatically increases performance in high packet loss networks. Reverting to the previous case, a 3Mbit/s video transport stream in an IP network with worst hour PLR of 3x10^{-3}, a service with less than 10 error hits per day may be provided using any of the matrix sizes shown. In less error-prone networks however, using two-dimensional FEC schemes may be overkill and generate unneccessary 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.

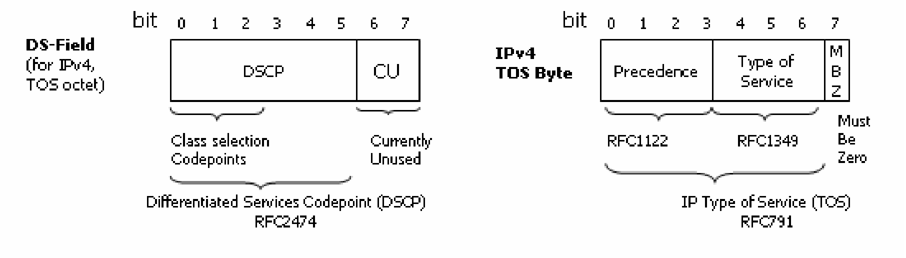


Figure D.1 Differentiated services (Diff-serve) and precedence bits (TOS)

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 TVG425 configuration

The number entered into the Type of service (TOS) field in TVG425 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-serve or precedence bits regarding packet classification in the network.

D.3.1 TVG425 configuration

The COS priority is entered in the VLAN configuration page in the TVG425 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 TVG425 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 TVG425. 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 *types*. This field contains a textual description of the type.
Type ID	Each alarm type has a corresponding number (ID).
Clear event	Set to *Yes* if an "off/cleared" alarm is expected after an "asserted" alarm. In most cases the value is *Yes*. For "stateless" alarms, e.g. the event that a user has logged into the system, no explicit clear events are expected.
Subid2	This field is present if the `Subid2` value of the alarm type is used. The text in the table describes the usage of the `Subid2` value.
Subid3	This field is present if the `Subid3` value of the alarm type is used. The text in the table describes the usage of the `Subid3` value.

Table E.3.a Alarms

Alarm ID	Text	Def. severity	Details
106	Unable to transmit	Critical	*Description:* Channel not able to transmit any data, or only part of the data is transmitted. *Type:* IP Output (*Type ID* = 24) *Clear event:* Yes *Subid2:* IP output channel identifier *Subid3:* IP Dest
107	Output parameter conflict	Critical	*Description:* *Type:* IP Output (*Type ID* = 24) *Clear event:* Yes *Subid2:* IP output channel identifier *Subid3:* IP Dest
108	Destination hostname unresolved	Warning	*Description:* Unable to DNS resolve hostname specified as destination. *Type:* IP Output (*Type ID* = 24) *Clear event:* Yes *Subid2:* IP output channel identifier *Subid3:* IP Dest
130	Ethernet link down	Critical	*Description:* No link on Ethernet layer. *Type:* Ethernet port (*Type ID* = 17) *Clear event:* Yes *Subid2:* Ethernet port ID
131	Ethernet output overflow	Critical	*Description:* The total bitrate of the streams to transmit is too high compared to the available ethernet bitrate. *Type:* Ethernet port (*Type ID* = 17) *Clear event:* Yes *Subid2:* Ethernet port ID
133	Generic SFP alarm	Critical	*Description:* Generic SFP alarm for Mipot and SFF-8472 based modules. *Type:* Ethernet port (*Type ID* = 17) *Clear event:* Yes *Subid2:* Ethernet port ID
134	Ethernet link problem	Critical	*Description:* Problem on the ethernet link *Type:* Ethernet port (*Type ID* = 17) *Clear event:* Yes *Subid2:* Ethernet port ID
140	IP address unresolved	Warning	*Description:* IP address is not resolved into physical MAC address. *Type:* IP Output (*Type ID* = 24) *Clear event:* Yes *Subid2:* IP output channel identifier *Subid3:* IP Dest
150	RTP sequence error	Warning	*Description:* Network error. Analysis of the sequence number of the RTP layer indicates that IP frames have been lost or that they have been received out of order. The alarm details field shows the actual jumps in the RTP sequence number field. *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier

Table E.3.b Alarms

Alarm ID	Text	Def. severity	Details
151	No data received	Critical	*Description:* No data received on Ethernet input for stream. See details field on alarm for description. *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier
152	FEC threshold exceeded	Warning	*Description:* The frequency of lost frames is higher than the configured value. Threshold values are configured per stream. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
153	Ethernet input overflow	Critical	*Description:* The total bitrate of the IP input streams is too high. *Type:* Ethernet port (*Type ID* = 17) *Clear event:* Yes *Subid2:* Ethernet port ID
154	Data lost	Critical	*Description:* The data stream received for a channel is incomplete or packets were received out of order and the buffer was not large enough. Also, if running FEC, the FEC engine was not able to recover all the lost frames. *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier
155	No lock	Critical	*Description:* The incoming packet stream is absent or incompatible with the expected format. *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier
157	Too low latency for FEC	Warning	*Description:* The preferred latency is set lower than the latency required to fully utilize the current FEC. Increase presumed jitter to resolve. *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier
158	SFN mode config error	Warning	*Description:* Lock to MIP bitrate mode requires configuration and locking to an external 1PPS source (Device Info-Clock Regulator). *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier
159	Unsynchronized diversity source	Warning	*Description:* Data received on diversity sources cannot be used for merging of streams. *Type:* IP Input (*Type ID* = 23) *Clear event:* Yes *Subid2:* IP input channel identifier
160	SNTP server unreachable	Warning	*Description:* The unit is not receiving answers from the SNTP server. *Type:* System (*Type ID* = 13) *Clear event:* Yes
161	Too high temperature	Warning	*Description:* Internal temperature of unit is too high. *Type:* System (*Type ID* = 13) *Clear event:* Yes

Table E.3.c Alarms

Alarm ID	Text	Def. severity	Details
162	Defective fan	Warning	*Description:* One or more fans are not spinning. *Type:* System (*Type ID* = 13) *Clear event:* Yes
163	Time reference unreachable	Warning	*Description:* No selected timesources are OK. *Type:* System (*Type ID* = 13) *Clear event:* Yes
164	Illegal board configuration detected	Critical	*Description:* A board configuration that is incompatible with this product has been detected. *Type:* System (*Type ID* = 13) *Clear event:* Yes
165	Time source not OK	Notification	*Description:* One or more time sources are not OK. *Type:* System (*Type ID* = 13) *Clear event:* Yes
166	Time source switch	Notification	*Description:* Device started using a new time source. *Type:* System (*Type ID* = 13) *Clear event:* No
167	Time adjusted	Notification	*Description:* The real time clock of the device was adjusted significantly. *Type:* System (*Type ID* = 13) *Clear event:* No
168	Power failed	Warning	*Description:* One or more power supplies have failed, or are out of regulation. *Type:* System (*Type ID* = 13) *Clear event:* Yes *Subid3:* Power supply ID
169	Virtual alarm relay activated	Notification	*Description:* A virtual alarm relay has been activated. *Type:* System (*Type ID* = 13) *Clear event:* Yes *Subid3:* Relay ID
200	No GPS 1PPS ref. signal	Critical	*Description:* The 1PPS reference signal is lost (The regulator has however not lost synchronization). *Type:* System (*Type ID* = 13) *Clear event:* Yes
201	Lost GPS 1PPS sync.	Critical	*Description:* The clock synchronization mechanism has been resynchronized due to too large phase error. *Type:* System (*Type ID* = 13) *Clear event:* Yes
210	Emergency switch active	Notification	*Description:* A user has activated the remote emergency switch. *Type:* System (*Type ID* = 13) *Clear event:* Yes
211	Emergency switch unreachable	Warning	*Description:* The device is not able to communicate with the remote emergency switch. *Type:* System (*Type ID* = 13) *Clear event:* Yes
212	Emergency switch rule config error	Warning	*Description:* An error has been detected in the configuration of the emergency switch. *Type:* System (*Type ID* = 13) *Clear event:* Yes

Table E.3.d Alarms

Alarm ID	Text	Def. severity	Details
501	User logged in	Notification	*Description:* This event is generated when a user logs on to the system. *Type:* System (*Type ID* = 13) *Clear event:* No
502	User logged out	Notification	*Description:* This event is generated when a user logs out from the system. *Type:* System (*Type ID* = 13) *Clear event:* No
503	System started	Notification	*Description:* The system has booted. *Type:* System (*Type ID* = 13) *Clear event:* No
504	Switch done	Notification	*Description:* The input relay has switched position. *Type:* Relay Switch (*Type ID* = 19) *Clear event:* No *Subid2:* Relay switch controller ID
505	Config changed	Notification	*Description:* A modification has been made to the configuration of the device. *Type:* System (*Type ID* = 13) *Clear event:* No
506	Unable to switch	Warning	*Description:* The relay controller is unable to switch because the spare input is not sufficiently good. *Type:* Relay Switch (*Type ID* = 19) *Clear event:* Yes *Subid2:* Relay switch controller ID
507	Auto switching disabled	Warning	*Description:* Enabled when auto switching is turned off. *Type:* Relay Switch (*Type ID* = 19) *Clear event:* Yes *Subid2:* Relay switch controller ID
508	Auto switch performed	Filtered	*Description:* Automatic switch is performed. This alarm will stay on until it is manually confirmed by the operator (see chapter on switch config). *Type:* Relay Switch (*Type ID* = 19) *Clear event:* Yes *Subid2:* Relay switch controller ID
517	Alarm log cleared	Notification	*Description:* Alarm log was cleared, user in details *Type:* System (*Type ID* = 13) *Clear event:* No
518	System is starting up	Critical	*Description:* This alarm is set when the system is starting. Once booted correctly, the alarm is cleared. *Type:* System (*Type ID* = 13) *Clear event:* Yes
519	Forced reset initiated	Notification	*Description:* A reset of the device was forced by the operator. *Type:* System (*Type ID* = 13) *Clear event:* No
520	SW loading in progress	Notification	*Description:* Loading of an embedded SW image is in progress *Type:* System (*Type ID* = 13) *Clear event:* Yes

Table E.3.e Alarms

Alarm ID	Text	Def. severity	Details	
521	New SW pending	Notification	*Description:*	A SW image has been successfully loaded, but manual reboot is needed for SW to be activated.
			Type:	System (*Type ID* = 13)
			Clear event:	Yes
524	Simultaneous users	Notification	*Description:*	Multiple users with administrator or operator access level are logged in.
			Type:	System (*Type ID* = 13)
			Clear event:	Yes
526	Action performed	Notification	*Description:*	Action performed by user. Used to log generic important events, see details field on each alarm event for additional information.
			Type:	System (*Type ID* = 13)
			Clear event:	No
527	New SW license pending	Notification	*Description:*	New SW licenses have been loaded but requires a re-boot to be activated.
			Type:	System (*Type ID* = 13)
			Clear event:	Yes
528	New SW license installed	Notification	*Description:*	New SW licenses have been loaded and installed without requiring reboot.
			Type:	System (*Type ID* = 13)
			Clear event:	No
601	Poll failed	Critical	*Description:*	The redundancy controller could not contact the main unit.
			Type:	Redundancy (*Type ID* = 18)
			Clear event:	Yes
			Subid2:	Redundancy Controller ID
602	Authorization error	Critical	*Description:*	The redundancy controller got response from the main unit but authorization failed.
			Type:	Redundancy (*Type ID* = 18)
			Clear event:	Yes
			Subid2:	Redundancy Controller ID
603	Link switchover performed	Notification	*Description:*	The redundancy controller has performed a switchover.
			Type:	Redundancy (*Type ID* = 18)
			Clear event:	No
			Subid2:	Redundancy Controller ID
604	Switchover failed	Critical	*Description:*	The redundancy controller failed to perform a switchover.
			Type:	Redundancy (*Type ID* = 18)
			Clear event:	Yes
			Subid2:	Redundancy Controller ID
605	Rollback failed	Critical	*Description:*	The redundancy controller failed to perform a switchover and the rollback failed as well.
			Type:	Redundancy (*Type ID* = 18)
			Clear event:	No
			Subid2:	Redundancy Controller ID
606	SNMP error	Critical	*Description:*	This alarm is triggered if a redundancy controller SNMP request fails.
			Type:	Redundancy (*Type ID* = 18)
			Clear event:	Yes
			Subid2:	Redundancy Controller ID

Table E.3.f Alarms

Alarm ID	Text	Def. severity	Details
607	Illegal configuration	Critical	*Description:* This alarm is triggered if the redundancy controller configuration is invalid. *Type:* Redundancy (*Type ID* = 18) *Clear event:* Yes *Subid2:* Redundancy Controller ID
608	Service switchover performed	Notification	*Description:* A switchover has been performed by the redundancy controller service switcher. *Type:* Redundancy (*Type ID* = 18) *Clear event:* No *Subid2:* Redundancy Controller ID
609	Automatic switchover is disabled	Warning	*Description:* The redundancy controller service switcher is in manual mode, no automatic switchover will be performed. *Type:* Redundancy (*Type ID* = 18) *Clear event:* Yes *Subid2:* Redundancy Controller ID
610	Spare service alarm level too high	Critical	*Description:* The redundancy controller alarm level switching criteria are met, but the spare service has a too high alarm level. *Type:* Redundancy (*Type ID* = 18) *Clear event:* Yes *Subid2:* Redundancy Controller ID
611	Illegal configuration	Notification	*Description:* The redundancy controller service switcher has either never received a configuration from the main service or received an invalid configuration. *Type:* Redundancy (*Type ID* = 18) *Clear event:* Yes *Subid2:* Redundancy Controller ID
1100	Sync unstable	Major	*Description:* Two separate sync-losses in 10s. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1101	TS unstable	Minor	*Description:* Lots of PIDs appearing/disappearing or CC errors. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1110	No sync	Critical	*Description:* No valid ASI stream detected. See test 1.1 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1120	Sync byte error	Warning	*Description:* Sync byte not equal to 0x47. See test 1.2 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1131	PAT repetition interval	Warning	*Description:* Measured interval between each PAT is greater than the configured limit. ETR290 specifies limit to 500 ms. Part of test 1.3 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier

Table E.3.g Alarms

Alarm ID	Text	Def. severity	Details
1132	PAT invalid table ID	Warning	*Description:* Unable to find section with table_id 0x00 on PID 0. Part of test 1.3 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1133	PAT scrambled	Warning	*Description:* Scrambling control field set for PID 0. Part of test 1.3 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1134	PAT missing	Warning	*Description:* PAT not found in transport stream. The PAT is required to do any further PSI decoding. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1140	CC error	Warning	*Description:* The Continuity Counter in the TS header was not as expected. Should increase by 1 for each packet with the Payload bit set, and not increase if not. Typically caused by lost TS packets. See test 1.4 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier *Subid3:* PID
1151	PMT repetition interval	Warning	*Description:* Measured interval between each PMT on a specific PID referenced in the PAT is greater than the configured limit. ETR290 specifies limit to 500 ms. Part of test 1.5 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1152	PMT scrambled	Warning	*Description:* Scrambling control field set for any PID carrying table_id 0x02, i.e. a PMT. Part of test 1.5 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1153	PMT missing	Warning	*Description:* PMT referenced in the PAT, but not found in transport stream. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier *Subid3:* Service
1160	PID error	Warning	*Description:* PID referred in a PSI table, but not found in within the configured period. The period is configured using the "PID Event" alarm. See test 1.6 in ETR 101 290 v1.2.1. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier *Subid3:* PID

Table E.3.h Alarms

Alarm ID	Text	Def. severity	Details	
1161	PID event	Filtered	*Description:*	This alarm is currently used to configure the time before a PID is assumed to have disappeared. See "PID error" alarm.
			Type:	Port (*Type ID* = 9)
			Clear event:	No
			Subid2:	Port identifier
			Subid3:	PID
1500	Input overflow	Critical	*Description:*	The total bit rate of the input stream is too high.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1509	Output muted	Warning	*Description:*	The output has been shut down by the output mute controller based on configured criterias.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1524	MIP PID not present	Warning	*Description:*	The MIP PID is not present.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1525	MIP CRC error	Critical	*Description:*	A CRC error has been detected in the MIP.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1526	MIP new parameters	Notification	*Description:*	An update has been detected in the parameters contained in MIP (TPS field or maximum delay field).
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1527	MIP CC error	Warning	*Description:*	TS packet header CC error has been detected on the MIP PID.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1528	MIP STS range error	Warning	*Description:*	The STS field indicates a value larger than a second.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1529	MIP pointer error	Warning	*Description:*	The number of TS packets in the megaframe does not match the parameters in MIP.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier

Table E.3.i Alarms

Alarm ID	Text	Def. severity	Details
1530	MIP timing error	Warning	*Description:* STS values in consecutive MIPs have wrong timing values. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1531	Extra MIP	Warning	*Description:* An extra MIP has been detected within a megaframe. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1532	Missing MIP	Warning	*Description:* No MIP is detected. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1533	MIP periodicity error	Warning	*Description:* The MIP periodicity is not correct. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1534	MIP ts rate error	Warning	*Description:* The rate of the transport stream does not match the rate signaled in the MIP. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1535	MIP network delay too high	Filtered	*Description:* Measured Network delay higher than configured maximum delay. Network delay is the time elapsed since the SFN adapter. Important: Both the monitor and the SFN adapter must be locked to the same external reference. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1536	MIP network delay too low	Filtered	*Description:* Measured Network lower higher than configured maximum delay. Network delay is the time elapsed since the SFN adapter. Important: Both the monitor and the SFN adapter must be locked to the same external reference. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1542	MIP size error	Warning	*Description:* There is not enough space in the MIP packet for all configured transmitter function loops. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier
1543	MIP Inserter time reference problem	Warning	*Description:* MIP Inserter time reference problem. *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* Port identifier

Table E.3.j Alarms

Alarm ID	Text	Def. severity	Details	
1601	Covering up input loss	Major	*Description:*	Loss of input signal is covered up by inserting stuffing packets at the last stream bitrate.
			Type:	IP Input (*Type ID* = 23)
			Clear event:	Yes
			Subid2:	IP input channel identifier
1801	TS-ID incorrect	Filtered	*Description:*	The TS-ID of the incoming stream does not match the TS-ID of the configured CSI section. For modes where the input TS-ID is not known, the TS-ID expected must be configured manually.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1802	PID rate too high	Filtered	*Description:*	PID bitrate is higher than set limit. Only PIDs added to override list are monitored, and the max rate must be set per PID.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
			Subid3:	PID
1803	PID rate too low	Filtered	*Description:*	PID bitrate is lower than set limit. Only PIDs added to override list are monitored, and the min rate must be set per PID.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
			Subid3:	PID
1812	TS rate too high	Filtered	*Description:*	TS bitrate is higher than set limit.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
1813	TS rate too low	Filtered	*Description:*	TS bitrate is lower than set limit.
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
2400	Input has critical alarm	Critical	*Description:*	Input soure has critical alarm
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
2401	Input has major alarm	Major	*Description:*	Input soure has major alarm
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier
2402	Input has minor alarm	Minor	*Description:*	Input soure has minor alarm
			Type:	Port (*Type ID* = 9)
			Clear event:	Yes
			Subid2:	Port identifier

Table E.3.k Alarms

Alarm ID	Text	Def. severity	Details
2403	Input has warning alarm	Warning	*Description:* Input soure has warning alarm *Type:* Port (*Type ID* = 9) *Clear event:* Yes *Subid2:* 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