

TVG420

ASI to IP Video Gateway

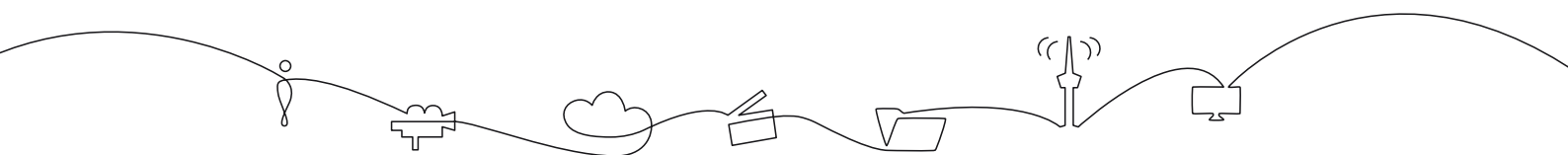
User's Manual

Revision: (2176)

2011-05-27



Valid for SW version 3.26.6 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	14
4	Getting Started	15
4.1	Configure the management interface	15
4.2	Configure device name and time settings	16
4.3	Configure the operational mode	16
4.3.1	ASI to IP	16
4.3.2	IP to ASI	17
5	Installing the Equipment	19
5.1	Inspect the package content	19
5.2	Installation Environment	19
5.3	Equipment installation	20
5.4	Ventilation	20
5.5	Power supply	21
5.5.1	AC power supply	21
5.5.2	Dual AC power supplies	21
5.5.2.1	AC power cable	21
5.5.2.2	Protective Earth/technical Earth	22
5.5.2.3	Connecting to the AC power supply	23
5.5.3	DC power supply	23
5.5.3.1	DC power cable	23
5.5.4	Powering up/down	24
6	Functional Description	25
6.1	IP transmit mode	25
6.2	IP receive mode	26
6.3	Management sub-system	26

6.3.1	Graphical user interface	27
6.3.2	Configuration database	27
6.3.3	Alarm manager	27
6.4	Time synchronisation	28
6.5	Video over IP	28
6.5.1	Protocol mapping	28
6.5.1.1	UDP mode	29
6.6	Forward Error Correction (FEC)	29
6.7	Redundancy controller	30
6.7.1	Operation	31
6.8	The SFP module	32
7	Physical Description of the TVG420	35
7.1	ASI ports	35
7.1.1	ASI input ports	36
7.1.2	ASI output ports	36
7.2	1 PPS Input	36
7.3	Ethernet data ports	37
7.4	Ethernet management port	38
7.5	Power supply	38
7.6	Technical earth	38
7.7	Alarm/Reset/RS232 connector	38
8	Operating the Equipment	41
8.1	Accessing the graphical user interface	41
8.2	Password protection	41
8.2.1	Resetting the password list	42
8.3	Changing the IP address of the unit	42
8.3.1	Changing IP address via the Web GUI	42
8.3.2	Changing the maintenance port IP address via terminal interface	43
9	WEB Interface	45
9.1	Login	45
9.2	Status header	46
9.3	Status	47
9.3.1	Current Status	47
9.3.2	Alarm log	49
9.4	Device Info	50
9.4.1	Product info	51
9.4.2	Alarms	53
9.4.2.1	Device alarms	53
9.4.2.2	Global Configuration	54
9.4.2.3	Relays and LED configuration	55
9.4.2.4	Alarm Log Settings	57

9.4.3	Time Settings	58
9.4.4	Network	60
9.4.4.1	Interfaces	61
9.4.4.1.1	Main	61
9.4.4.1.2	Alarms	62
9.4.4.1.3	Advanced	63
9.4.4.1.4	Status	63
9.4.4.1.5	VLAN	65
9.4.4.1.6	SFP	66
9.4.4.2	IP Routing	70
9.4.4.3	TXP Settings	71
9.4.4.4	SNMP Settings	72
9.4.4.5	Tools	73
9.4.5	Clock Regulator	74
9.4.5.1	Main	74
9.4.5.2	Alarms	75
9.4.6	Save/Load Config	76
9.4.6.1	Save/Load Configs	76
9.4.6.2	Boot Log	77
9.4.6.3	Stored Configs	77
9.4.7	Maintenance	79
9.4.7.1	General	79
9.4.7.2	Software Upgrade	80
9.4.7.3	Feature Upgrade	82
9.4.8	Users	82
9.4.9	GUI Preferences	83
9.5	IP TX	84
9.5.1	Main	84
9.5.2	Alarms	88
9.5.3	FEC	88
9.5.4	Ethernet	90
9.5.5	Ping	91
9.5.6	RIP-2	91
9.6	IP RX	93
9.6.1	Main	94
9.6.2	Alarms	96
9.6.3	FEC	97
9.6.4	Ping	98
9.6.5	Advanced	99
9.7	Streams	102
9.8	Redundancy	103
9.8.1	Redundancy Controller	103
9.8.1.1	Global redundancy controller switching	104
9.8.1.2	Poll settings	105
9.8.1.3	Remote device IP addresses	106
9.8.1.4	SNMP switch actions	106
9.8.2	Service switchers	107

10	SNMP	109
10.1	SNMP agent characteristics	109
10.2	MIB naming conventions	109
10.3	MIB overview	109
10.3.1	Supported standard MIBs	109
10.3.2	Custom MIBs	109
10.4	SNMP related configuration settings	111
10.4.1	Community strings	111
10.4.2	Trap destination table	111
10.4.3	Trap configuration	112
10.5	Alarm/status related SNMP TRAPs	112
10.5.1	The main trap messages	113
10.5.2	Severity indications	113
10.5.3	Alarm event fields	114
10.5.4	Matching of on/off traps	115
10.5.5	Legacy trap messages	115
11	Preventive Maintenance and Fault-finding	117
11.1	Preventive maintenance	117
11.1.1	Routine inspection	117
11.1.2	Cleaning	117
11.1.3	Servicing	117
11.1.4	Warranty	118
11.2	Fault-finding	118
11.2.1	Preliminary checks	118
11.2.2	PSU LED not lit / power supply problem	119
11.2.3	Fan(s) not working / unit overheating	120
11.3	Disposing of this equipment	120
11.4	Returning the unit	120
A	Quality of Service, Setting Packet Priority	121
A.1	MPLS	121
A.2	Layer 3 routing	121
A.2.1	TVG420 configuration	122
A.3	Layer 2 priority	122
A.3.1	TVG420 configuration	122
B	Glossary	123
C	Alarms	129
D	Technical Specification	141
D.1	Physical details	141
D.1.1	Half-width version	141
D.1.2	Full-width (dual power) version	141

D.2	Environmental conditions	141
D.3	Power	142
D.3.1	AC Mains supply	142
D.3.2	DC supply	142
D.4	Input/output ports	143
D.4.1	DVB ASI port	143
D.4.2	Ethernet management port	143
D.4.3	Ethernet data port	143
D.4.4	Alarm relay and maintenance port specification	144
D.5	External reference	144
D.5.1	10MHz/1 PPS input	144
D.5.2	10 MHz input	145
D.6	Compliance	145
D.6.1	Safety	145
D.6.2	Electromagnetic compatibility - EMC	145
D.6.3	CE marking	145
D.6.4	Interface to “public telecommunication system”	146
E	References	147

1 History

Revision	Date	SW version	Comments
3.26	May 2011	3.26.4	New IP RX Advanced page.
3.18	November 2010	3.18.2	Revised manual lay-out, improved VLAN support, IP routing table, Virtual alarm relays, SFP configuration, RIPv2 support for VLAN interfaces.
3.12	June 2009	3.12.12	Updated product base. Embedded redundancy controller, input/output direction change without reset, SNMPv2c support, VLAN tagging of management traffic, RIPv2 configuration per channel
2.10	January 2008	2.22.0	204 byte MPEG-2 transport stream support
2.9	November 2007	2.20.4	Data channel ping, ASI bitrate limiter, Static MAC
2.8	April 2007	1.4.0	Dual ASI, Increased FEC matrixes, VBR mode, new FEC alarm, password resetting.
2.7	March 2007	1.3.33	SNMP tab, Burst/Spread mode, No lock mode, updated features list.
2.6	Oct. 2006	1.3.22	Added support for User Security and RIPv2.
2.5	September 2006	1.3.18	Added support for GPS module.
2.4	July 2006	1.3.11	Ping option, New clock options, Advanced tab on IPRX, Speed-/ duplex mode for management port
2.3b	May 2006	1.3.x	Small patch on description of RTP sequence errors.
2.3	April 2006	1.3.x	Release with bi-directional operation, and IGMPv3 support.
2.2	January 2006	1.2.2	Release with SNMP support as optional feature and support for UDP transmission mode
2.1	November 2005	1.1.5	Intermediate release with implementations on iterative FEC, more on alarms and other general improvements.
2.0	September 2005	1.1.0	Release with FEC, VLAN and SFP interface
1.1	July 2005	0.11.4	Initial release

2 Introduction

2.1 Scope

This manual is written for operators and users of the TVG420 ASI to IP Video 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 3.26.6, or later and continues to be relevant to subsequent software versions where the functionality of the equipment has not been changed. When a new software version changes the functionality of the product, an updated version of this manual will be provided.

The manual covers the following topics:

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

2.2 Warnings, cautions and notes

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



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



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



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

2.3 Heed Warnings

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

2.4 Contact Information

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

Please contact us at:

Telephone	+47 22 88 97 50
Fax	+47 22 88 97 51
E-mail	support@t-vips.com
WEB	www.t-vips.com
Mail and visiting address	T-VIPS AS Nils Hansens vei 2 NO-0667 Oslo Norway

3 Short Product Description

The TVG420 provides a bridge between the MPEG-2 world and the IP world. The unit provides an interface between MPEG-2 transport streams, via DVB-ASI interface, to the IP based Network. It provides the ability to carry up to 8 individual MPEG-2 transport streams over an IP network. Each individual MPEG-2 transport stream is carried on an individual UDP port. At the reception site, the unit de-concentrates the MPEG-2 transport streams from the IP network, back to individual MPEG-2 transport streams and out through the DVB-ASI connections.

The TVG420 consists of a 1RU high rack-mounted enclosure with 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 TVG420 include:

- Transmission of MPEG2 Transport Streams over Gigabit Ethernet
 - MPTS / SPTS inputs
 - 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
 - 1 PPS/10 MHz synchronisation for accurate bitrate control in SFN DVB-T/H networks
 - 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
- Redundancy
 - Embedded redundancy controller
 - Scalable redundancy scheme
 - RIPv2 assisted redundancy

- 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 T-VIPS Connect

3.2 Options

The TVG420 is modular and may be equipped according to user requirements. Available hardware and software options are described below.

3.2.1 Hardware options

4 additional ASI ports

The TVG420 is fitted with at least 4 ASI ports from factory, of which any number from 1 to 4 are enabled as ordered. As an option, the unit can be fitted with an additional ASI module providing 4 additional ASI ports, giving a total of 8 ASI ports.

SFP Module

The TVG420 can optionally be equipped with an SFP socket to accommodate an SFP module with optical Gigabit or electrical Gigabit port. The SFP module itself is not provided.

SFP/1 PPS Module

As a factory option the TVG420 can be equipped with an SFP socket in combination with a 1 PPS synchronising signal input. The SFP module itself is not provided.

Dual power supplies

The TVG420 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 following table describes the features available as software options. Please refer to section [9.4.7.3](#) for more information on feature upgrades.

Table 3.1 Functionality enabled through software licences

Functionality	Max value	Function
SFP module	-	Enables operation of the Small form-factor pluggable (SFP) transceiver slot.
SFP configuration	-	Enables configuration interface and parameter storage for some specifically supported SFP modules.
Number of enabled ports	8	The number of ASI ports enabled. This can be different from the number of ports physically mounted.
Data port max. speed	1000 Mbit/s	The speed of the data port can be 100 Mbit/s or 1000 Mbit/s.
Connect Control	-	Enabled supervision of the unit through the Connect software.
Forward Error Correction	-	Pro-MPEG Forward Error Correction enabled for use on all streams.
Bi-directional operation	-	Enables simultaneous transmission and reception of MPEG2 data on the Ethernet data interface.
Embedded redundancy controller	-	Provides a generic software module that implements redundancy scenarios.

4 Getting Started

This section provides a short description of the minimum steps that must be taken in order to start operating the TVG420.

If you are an experienced user of T-VIPS equipment or similar types of MPEG-2 processing equipment the following description should enable you to quickly install the TVG420 ASI to IP Video Gateway and start operation. If this is your first time to install such equipment you are strongly advised to read the full installation procedure. To gain full benefit of the product functionality and capabilities refer to the user interface description.

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

4.1 Configure the management interface

Since the TVG420 is all Web controlled the first step is to set up the IP address for the management interface.

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



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

1. Connect an Ethernet cable directly between the PC and the Ethernet “Control” port of the TVG420. The default IP address of the TVG420 is **10.0.0.10/255.255.255.0**. Configure the PC to be on the same subnet as the TVG420.
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 TVG420 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 the operational mode

The TVG420 operates as a gateway to encapsulate MPEG2 transport streams in IP, or to extract MPEG2 transport streams from IP. Individual transport stream inputs and outputs are provided as ASI ports. If required, the TVG420 may perform these two functions simultaneously, provided that a sufficient number of ASI ports has been enabled. The TVG420 does not distinguish between IP encapsulation of single program and multi program transport streams.

4.3.1 ASI to IP

The following describes the basic procedure to enable IP encapsulation of an MPEG2 transport stream.

1. Select the ASI input port to receive the transport stream to encapsulate. Browse to IP TX and click on the ASI port you want to activate, designated ASI #.
2. In the Main page, Input Configuration field, tick the Enable input check box and type an identifying name, e.g. the service name, in the Input name box. In the Max bitrate

field type the expected maximum input bit rate. Tick the Keep 204 bytes check box to preserve 204 byte transport stream packet length. Click Apply to activate.

3. If a transport stream is applied to the ASI input connector the Input Status field will now indicate its presence.

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.

1. Configure the IP transmission parameters. In the IP TX parameters field tick the Enable IP transmission box. Enter the IP address of the receiving unit in the Destination IP address field and select RTP or UDP form the Protocol pull-down list. Specify the UDP destination port.

If you do not have a reason to do otherwise, set the TS packets per frame to 7, to avoid fragmentation. The Time to live number should be set higher than the expected number of IP switchers and routers passed en route. Do not change the remaining settings at this stage. Click Apply to activate.

2. The default for theTVG420 is to use the Data port, thus the network ethernet cable should be connected to the rear Data connector. The IP TX Status field will confirm if a receiving interface with the given IP destination address is within reach.

4.3.2 IP to ASI

The basic procedure to enable extraction of an MPEG2 transport stream from IP is described below.

1. Select ASI output port for the extracted transport stream. Browse to IP RX and click on the ASI port you want to activate, designated ASI #.
2. In the Main page, Output Configuration field, tick the Enable output check box and type an identifying name, e.g. the service name, in the Output name box. From the Packet length pull-down list select if the output transport stream packet format shall be 188 or 204 byte. Click Apply to activate.
3. Configure the IP reception parameters. In the IP RX parameters field specify the UDP destination port. Type a number to specify the Preferred latency, i.e. the nominal signal delay introduced in the extraction process. Do not change the remaining settings at this stage. Click Apply to activate.
4. The IP RX Status field will indicate if the Data network cable carries a valid signal and the Output Status will report the status of the outgoing transport stream.

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

5 Installing the Equipment



Caution: The TVG420 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 TVG420 is mechanically and electrically in order.
- Verify that you received the following items:
 - TVG420 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 TVG420 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 TVG420.

- 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 TVG420 has been subject to a lightning strike or a power surge which has stopped it working, disconnect the power immediately. Do not re-apply power until it has been checked for safety. If in doubt contact T-VIPS.

5.3 Equipment installation

The TVG420 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 TVG420 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 each side of the TVG420.

5.4 Ventilation

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



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

- This product should never be placed near or over a radiator or heat register. Do not place in a built-in installation (e.g. a rack) unless proper ventilation is provided in accordance with the device airflow design as depicted in [Figure 5.1](#).
- The TVG420 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 TVG420 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 TVG420 has a wide-range power supply accepting the voltage range 100-240 VAC, 50/60 Hz. Please refer to [Appendix D](#) for a detailed specification of the AC power supply.

5.5.2 Dual AC power supplies

Alternatively, the TVG420 may be fitted with dual internal wide-range AC power supplies. If so, the size of the cabinet is full-width 19" rack, 1RU. The power supplies cover the voltage range 100-240 VAC, 50/60 Hz.

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

Please refer to [Appendix D](#) for a detailed specification of the AC power supply.

5.5.2.1 AC power cable

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



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

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

Table 5.1 Supply cable wiring colours

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

5.5.2.2 Protective Earth/technical Earth

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



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



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

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

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



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

5.5.2.3 Connecting to the AC power supply



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

To connect the unit to the local AC power supply, connect the AC power lead to the TVG420 mains input connector(s) and then to the local mains supply.

5.5.3 DC power supply

The TVG420 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 D](#) for detailed specification of the power supply.

5.5.3.1 DC power cable

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

Table 5.2 DC power connector pin assignment

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

To connect the unit to the local DC power supply:

1. Use an electronics soldering iron or a hot air workstation to attach the supplied female D-SUB power connector to suitable power leads.
2. Connect the power leads to your local power supply.
3. Connect the DC power connector, with attached power leads, to the TVG420 power input connector.

5.5.4 Powering up/down

Before powering-up the unit, please ensure that:

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

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

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

6 Functional Description

This chapter provides a high-level functional description of the TVG420 and an overview of transmission of MPEG-2 data over IP networks.

The TVG420 consists of a main module and 1 or 2 ASI boards, each handling up to 4 ASI ports.

With the software option 'Bi-directional operation' the direction of each input and output can be individually configured without the need for a reset. Without this licence all ports operate in the same direction and switch simultaneously.

In the IP transmit mode, the TVG420 encapsulates MPEG-2 transport streams received on the ASI ports into IP streams. These streams are sent on an Ethernet interface onto the IP network.

In IP receive mode, the TVG420 receives and extracts up to 8 transport streams from the IP network and outputs the MPEG-2 transport streams on the DVB ASI ports.

Optical Gigabit network interface is provided as a hardware option.

The following figure shows the data flow between two TVG420 over an IP network.

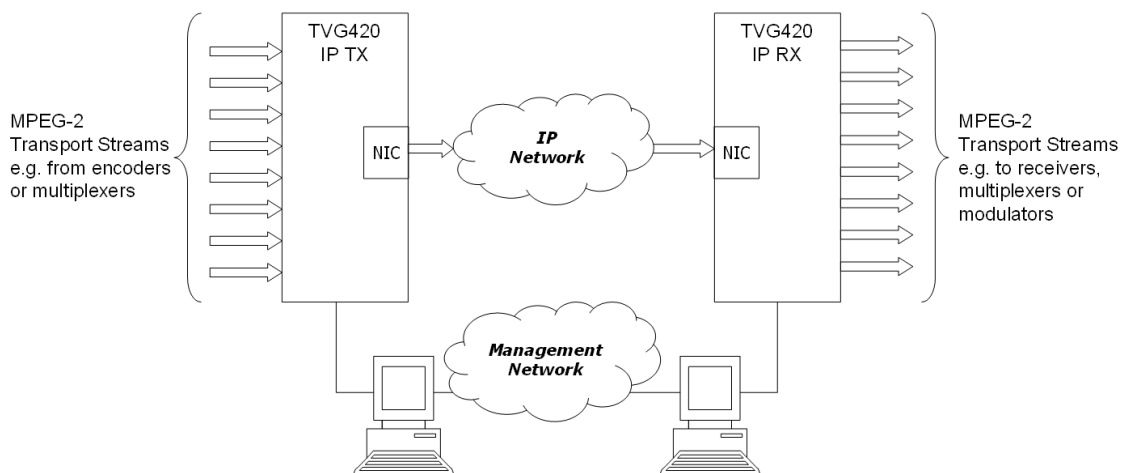


Figure 6.1 Data flow between two units

6.1 IP transmit mode

In the IP transmit mode the MPEG-2 transport streams are sourced from the ASI ports on the ASI boards. The TVG420 is able to handle source transport streams on ASI in the following formats:

- Packet format of 188 bytes
- Packet format of 204 bytes, including padding
- Packet format of 204 bytes, including RS bytes (no RS checking performed)

The sourced transport stream is then processed by the Main board. The TVG420 will send 188 bytes packets over the IP network by default, but you can configure it to keep 204 byte packets if required. The MPEG-2 transport stream packets are encapsulated as described in section 6.5.1. 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 are configured. The TVG420 handles both unicast and multicast transmissions.

The IP packets from one ASI input port are then merged with the IP packets from the other ASI inputs. The combined IP stream is then passed onto the physical Ethernet connector.

6.2 IP receive mode

In IP receive mode the TVG420 receives IP packets from the data Ethernet interface. The TVG420 will receive streams from different sources. In the case of unicast, the TVG420 will parse the IP stream and send the transport stream to the ASI output set up to listen to the appropriate UDP port. In case of multicast, the TVG420 will send a join message to join the configured multicast. When reception is disabled, the TVG420 will send a leave message to the network. For each transport stream, the reassembled MPEG-2 transport packets are held in a buffer. The function of this buffer is to handle re-ordering of packets, eliminate network jitter and support the adaptive rate recovery.

After clock recovery, the MPEG-2 transport stream is passed to the DVB ASI output port.

6.3 Management sub-system

The management subsystem is a set of modules that handles all the interfaces to monitor and control the operation of the TVG420.

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
- Alarm relays on alarms
- SNTP client for real time clock synchronisation
- Terminal interface either over Telnet or serial 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.

6.3.1 Graphical user interface

Operators monitor and control the TVG420 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 TVG420 can be controlled from the web GUI.

6.3.2 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

6.3.3 Alarm manager

The TVG420 contains an integrated alarm manager responsible for consistently displaying the alarm status of each individual interface.

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

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

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

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

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

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

As an additional option, the alarm manager in the TVG420 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.

6.4 Time synchronisation

The TVG420 contains an internal real-time clock that is used for all internal timestamps. The clock is reset when the unit has no power.

The internal time can be synchronised as follows:

- Manual setting.
- From NTP servers using SNTP protocol. Up to four NTP servers can be configured for NTP server redundancy.

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

6.5 Video over IP

One of the core functions in the TVG420 is the IP encapsulation of the MPEG-2 transport streams. The task is basically to encapsulate video packets into IP frames, using the appropriate headers.

6.5.1 Protocol mapping

Figure 6.2 shows the layering of the transport protocols used.

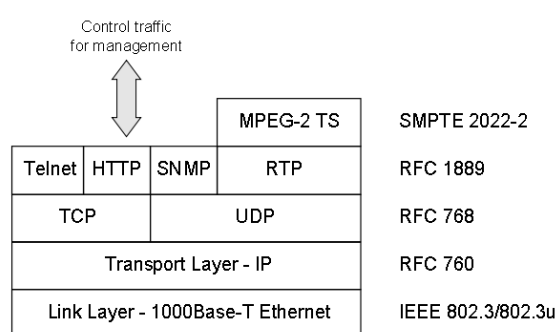


Figure 6.2 Protocol mapping

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

The TVG420 is able to handle both Multi-Program Transport Streams (MPTS) and Single-Program Transport Streams (SPTS). In the current version, the TVG420 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.

6.5.1.1 UDP mode

To allow interoperability with legacy equipment, the TVG420 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 TVG420 unit, and automatically detected by the receiving TVG420.



Note: FEC relies on information in the RTP protocol, and will not be available in UDP mode. FEC is explained in section [6.6](#).

6.6 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 TVG420 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 [6.3](#) 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 $4 \leq L \leq 32$, $4 \leq D \leq 32$ and $L+D \leq 32$ and that the maximum matrix size is $256(L*D)$. When using column FEC only,

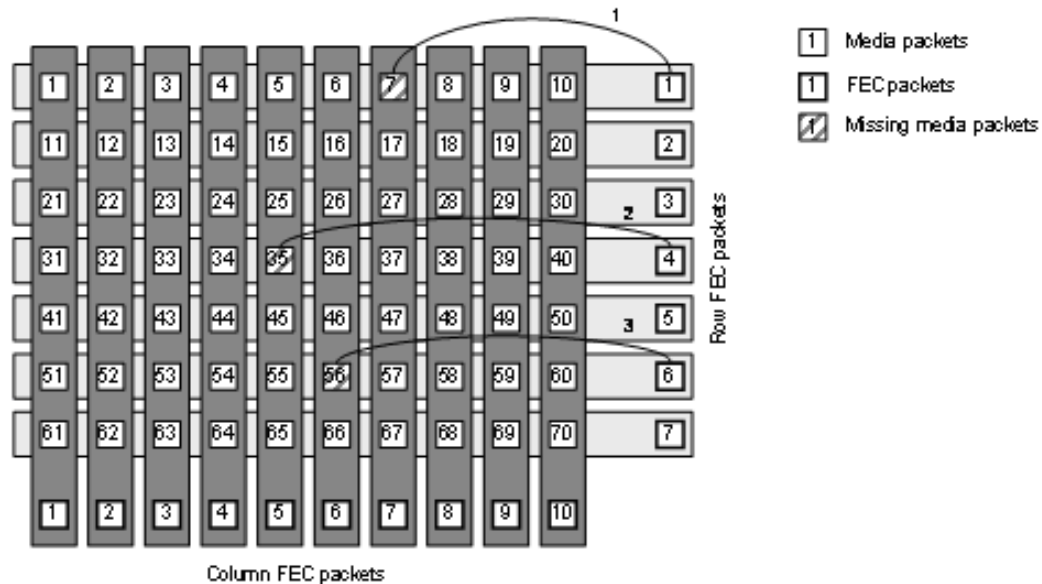


Figure 6.3 Illustration of two-dimensional FEC, where packet 7, 35 and 56 are lost and corrected.

L is allowed to be in the range $1 \leq L \leq 32$. 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.

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.

6.7 Redundancy controller

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

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

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

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

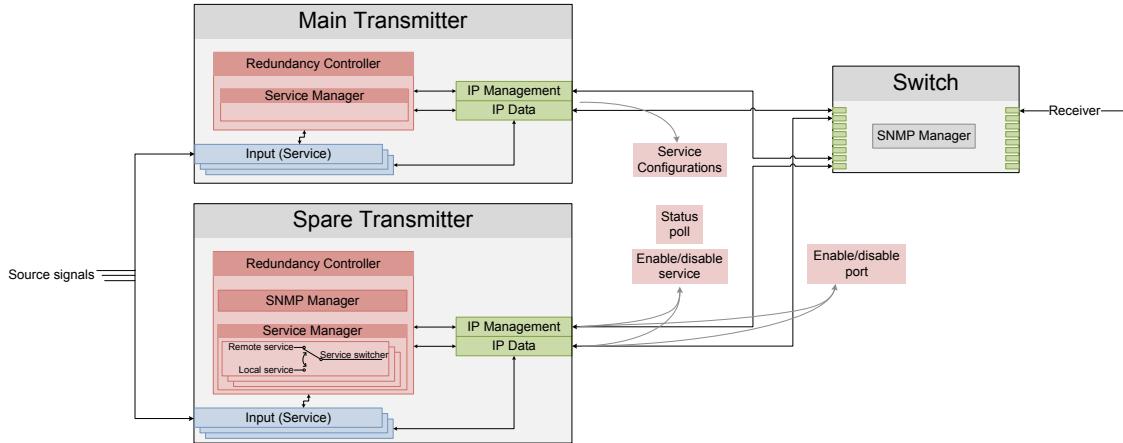


Figure 6.4 An overview of the embedded redundancy controller

6.7.1 Operation

All redundancy control enabled T-VIPS devices advertise a set of services. A service might be an IP transmitter port, ASI port, SDI port etc. Any service on a T-VIPS device with redundancy control can be a spare for any compatible service on another T-VIPS device licenced for 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	Remote	Local
Normal operation	Output enabled	Output disabled
Remote service has alarm	Output disabled	Output enabled
No contact with remote device	Unknown, typically port on switch disabled	Output enabled

Normal Operation

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

Remote service has alarm

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

No contact with remote device

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

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 TVG420. 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 6.5 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 TVG420 WEB interface. Control information is passed to and from the SFP module using the I²C protocol.

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

The TVG420 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 9.4.7](#)).

The SFP interface must be expressly enabled from the TVG420 user interface (Device Info > Data > Main) by selecting SFP from the Media select dropdown menu and hitting Apply.

7 Physical Description of the TVG420

The TVG420 ASI to IP Video 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 rear panel and there are no front panel keypads or display.

The front panel provides four LEDs per TVG420. 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
IP TX	Blue	This LED is lit when the unit is configured to transmit data to the IP Network.
IP RX	Yellow	This LED is lit when the unit is configured to receive data from the IP Network

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

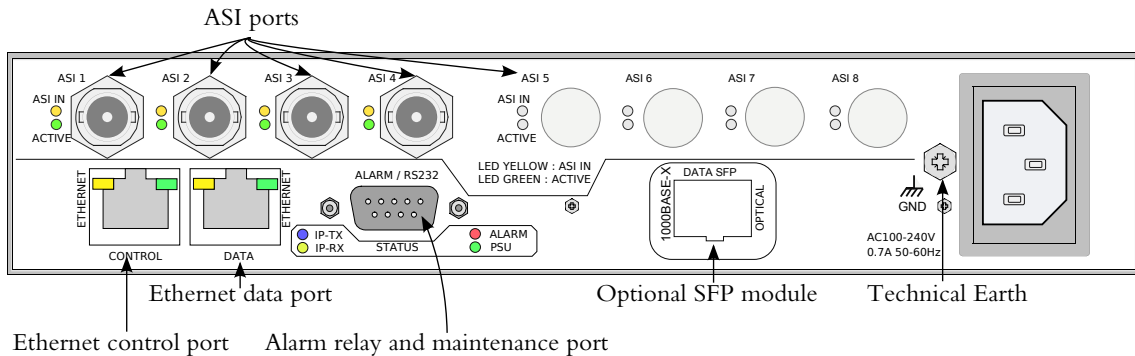


Figure 7.1 Rear panel

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

7.1 ASI ports

The TVG420 ASI ports can be operated in IP Transmit or IP Receive mode.

In IP transmit mode, the equipment receives up to 8 DVB-ASI streams and sends them to the IP network. In this mode, connect the individual DVB-ASI input signals to the connectors marked with ASI. If you have ordered the unit with less than 4 ASI ports, the enabled ports starts at number 1 up to the number of ports ordered.

In IP receive mode, the equipment receives an IP stream and sends the individual MPEG-2 transport streams out on the DVB-ASI connectors. In this mode, connect the DVB-ASI output to the input of the equipment to receive MPEG-2 transport stream from the unit. If you have ordered the unit with less than 4 ASI ports, the enabled ports starts at number 1 up to the number of ports ordered.

For more details regarding the ASI ports, please refer to [Appendix D: Technical Specification](#).

7.1.1 ASI input ports

Inputs signals connected to the DVB ASI ports should DVB compliant transport streams in asynchronous serial format.

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.

Table 7.2 ASI Input LED description

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

When in IP receive mode the ASI port will output a DVB compliant transport stream. When no stream is received over the IP network, the output will be idle characters. If a stream is received, the output will be a combination of MPEG-2 transport stream data bytes and idle characters.

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 TVG420 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 input module features a 1 PPS input and 4 ASI ports, thus at the same time allowing 8 ASI ports in total.

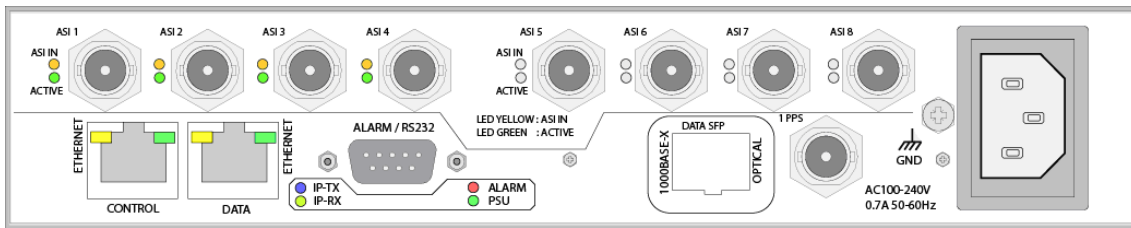


Figure 7.2 TVG420 with separate 1 PPS interface module

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 D.5.1.

7.3 Ethernet data ports

The Ethernet port provides an electrical Ethernet data port. The default interface is 100Base-T. As an option, the port can be operated as 1000Base-T. In this case the port can auto sense between 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 TVG420 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 TVG420 is prepared for electrical (1000Base-T) or optical 1000BASE-SX and 1000BASE-LX SFP transceivers.

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

In addition two LEDs are used to show IP network transmission and reception:

Table 7.5 Ethernet data port LEDs

LED indicator	Description	Colour
IP TX	This LED is lit when the unit is configured to transmit data to the IP Network.	Blue
IP RX	This LED is lit when the unit is configured to receive data from the IP Network	Yellow



Note: The optional SFP slot always provides Gigabit Ethernet. Other bitrates are not supported by the SFP slot.



Note: Data will not be available simultaneously on the electrical Ethernet port and the SFP slot. The user selects this in the user interface.

7.4 Ethernet management port

The TVG420 provides one Ethernet port for control and management. Connect the management port to the management network. The LEDs for the management port are used as follows:

Table 7.6 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.

7.7 Alarm/Reset/RS232 connector

The unit is equipped with a 9-pin male DSub connector to provide alarm information and RS232 access.

One programmable relay is provide for alarm information. The pin out of the connector is shown in table Document: tbl_alarm_connector_pinout.

When there is a *critical* (level 6) alarm in the unit, unit is not powered or any other programmed condition for the relay 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.

In addition the relay can also be programmed to be activated for alarm levels other than level 6. Please refer to section 9.4.2.3 for a description of how to program the relays.

A connection between pin 9 and 5 (or a TTL low on pin 9) will hold the unit in reset. The connection must be held for 8 seconds in order to activate the reset. This can be used to force a hard reset of the unit from an external control system.

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

Table 7.7 Alarm/Reset
connector pin out

Pin	Function
1.	NC
2.	RS232 Receive Data (input)
3.	RS232 Transmit Data (output)
4.	NC
5.	Ground
6.	Alarm Relay - Closed on alarm (NC)
7.	Alarm Relay Common
8.	Alarm Relay - Open on alarm (NO)
9.	NC

8 Operating the Equipment

The TVG420 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 TVG420. As a general rule it is recommended to always use the latest official release of Flash Player (version 10 or newer). If the Flash Player is not installed on the administrator PC, a copy is provided on the CD delivered with the device. Alternatively, the latest Adobe Flash Player can be downloaded free of charge from <http://www.adobe.com>.



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

8.1 Accessing the graphical user interface

The default IP address of the TVG420 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 TVG420 offers two options to alter the user interface IP address; through an Ethernet connection or using a serial 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 serial 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 TVG420 using the serial 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 serial terminal interface. To reset the password list, type the following command in the terminal interface:

```
userdb factory_defaults
```



Note: The `factory_defaults` option on the `userdb` command is available without administrator privileges only when accessing the terminal via the local serial 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 TVG420 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 TVG420. Configure the PC to be on the same sub net as the TVG420. 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 TVG420 with factory default settings. The IP address/netmask

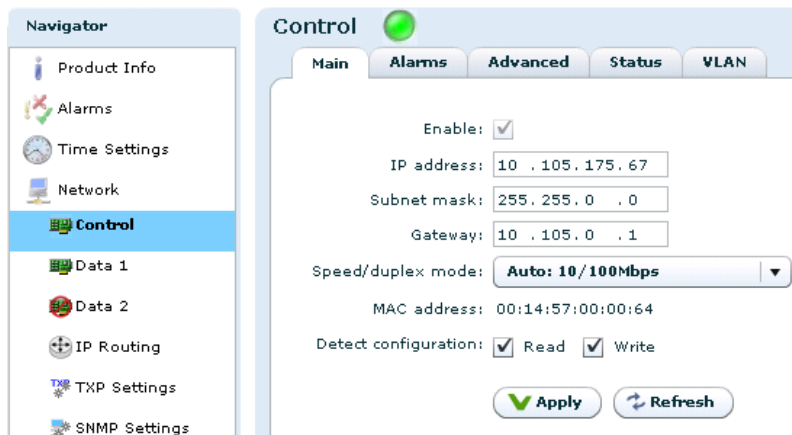


Figure 8.1 Configuring network settings via the Web GUI

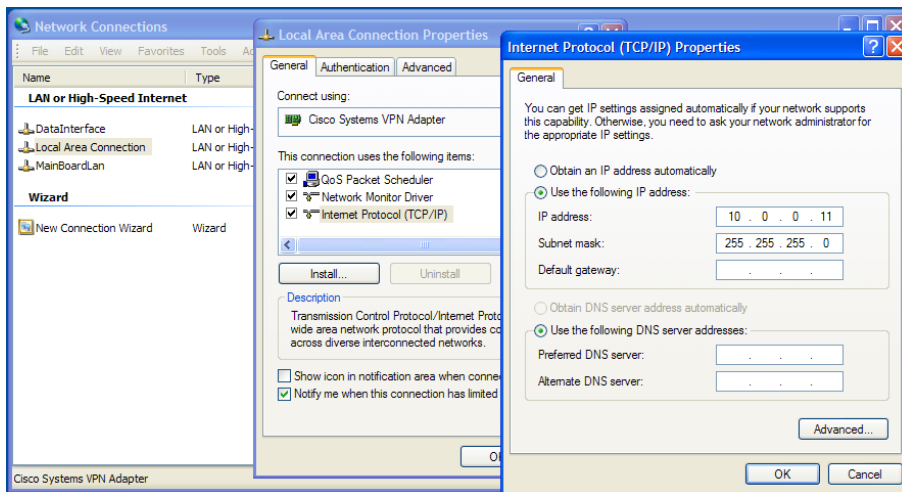



Figure 8.2 Setting static IP address 10.0.0.11 in Windows XP

is set to 10.0.0.11/255.255.255.0 which is on the same sub net as the TVG420, 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 maintenance 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. Connect your computer to the TVG420 via a null-modem cable to the RS232 port.

2. Access the terminal interface using a suitable terminal program, emulating an ANSI terminal, on your PC (e.g. HyperTerminal) Use the following serial port settings: 115200 bit/s, 8, N, 1, no flow control. Assure "scroll lock" is not on. Type <enter> and see that you have a prompt (app>).
3. 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.

9 WEB Interface

The TVG420 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.

9.1 Login

Access the TVG420 by entering its IP address in the address field of your favourite browser. When accessing the TVG420 the first time, the progress bar ([Figure 9.1](#)) should appear while the Flash application is loading from the device.

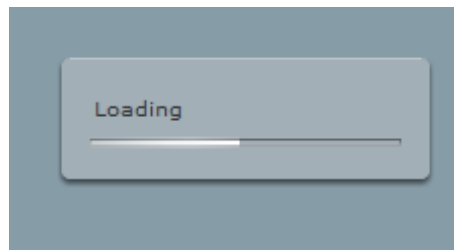


Figure 9.1 Flash application loading

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](#).

Username: admin
Password: *****
Save password
Login Clear

Figure 9.2 GUI login window

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

9.2 Status header

After successful login the start page is shown. The top part of the page (shown in figure 9.3) is called the status header.

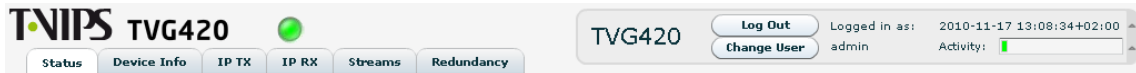


Figure 9.3 The status header

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

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

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

- The user defined device name, if entered.
- A button to log out from the GUI.
- A button to switch current user level.
- A text showing the current user name.
- The local device time.
- A button for minimising the header. Using this hides a lot of the header information and gives more space for the rest of the page.
- An activity indicator.



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

A tab bar is located beneath the status header. The exact number of tabs and tab labelling depends on the unit operational mode. Clicking a tab will open the corresponding page with a navigation pane to the left as shown in figure 9.4. This pane is used to navigate between sub-pages of the tab.



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.

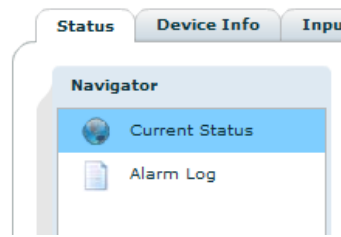


Figure 9.4 Status navigator

9.3 Status

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

There are two sub-pages within the status page.

Current Status

The current 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

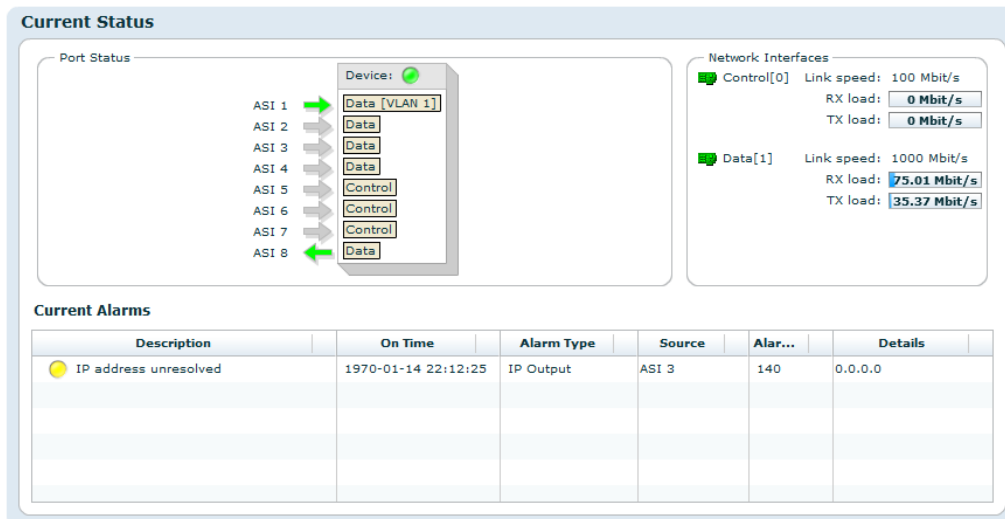


Figure 9.5 Current status

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

Block Diagram

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

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

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

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

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

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

Current Alarms

The bottom part of the page shows the currently active alarms. Some alarms, such as the PID related alarms, contain several sub-entries that are displayed by opening the folder of the entry. The severity of each alarm is represented by an error indicator (visually similar to a LED). The colour of the indicator represents the severity level configured for the specified alarm. The various severities and colours used are described in appendix C.

The Current Alarms table contains six columns:

Description

Description of the alarm condition.

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

On Time

The time when the alarm was raised.

Alarm type

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

Source

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

Subid1

Reserved for future use in multi-slot chassis and is always set to 1 in the TVG420.

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 a human readable form. The format of this string depends on the alarm type. Hovering the mouse over this field produces a tooltip which displays the full text.

A detailed overview of alarm conditions is given in appendix C.

9.3.2 Alarm log

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

Alarms in log: 8 Enable updates

Figure 9.6 Alarm log

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

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

Each row provides additional information via a tooltip shown when hovering over the row. The additional parameters are:

Sequence #

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

SubID 1

The primary numerical index to the alarm instance. This index is reserved for future use and is always set to 1 in the TVG420.

SubID 2

The secondary numerical index to 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 to 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 to provide 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 there 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 avoid scrolling of the log 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 management interface is shown in bold. See [Figure 9.7](#).

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

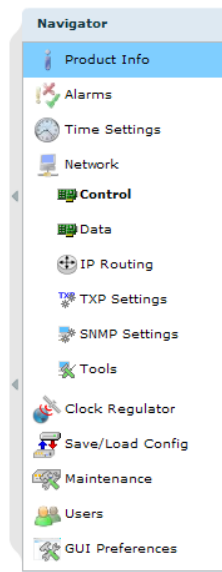


Figure 9.7 Device Info navigator

9.4.1 Product info

The product info page contains general device information.

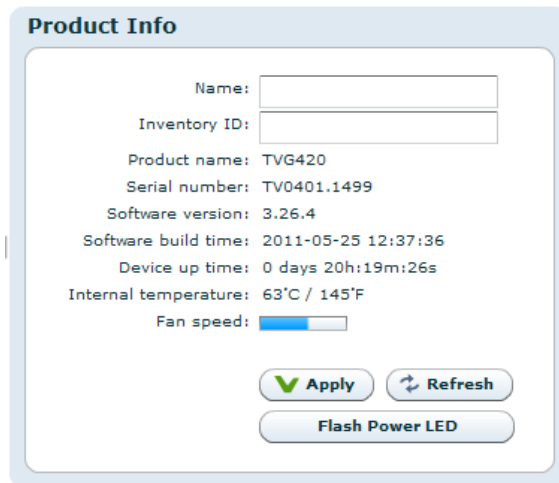


Figure 9.8 Product Information

Name

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

Product name

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

Serial number

The serial number of the device.

Software version

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

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

The convention for the SW version numbering is as follows:

major_version

Incremented for significant SW changes.

minor_version

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

patch_version

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

Software build time

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

Device up time

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

Internal temperature

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

Fan speed

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

Flash Power LED button

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

9.4.2 Alarms

The Alarms page is shown in [Figure 9.9](#):

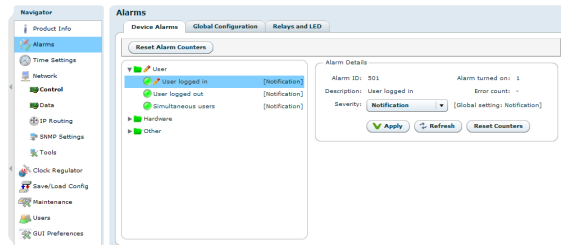


Figure 9.9 Alarm configuration

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

It gives access to the following sub pages:

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

9.4.2.1 Device alarms

The page shown in [Figure 9.9](#) provides the administrator with an interface to view the status and configure the behaviour of all alarms related to the system. At the top the Reset Alarm Counters button allows resetting all alarm counters simultaneously.

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

The right hand side of the page shows alarm details 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

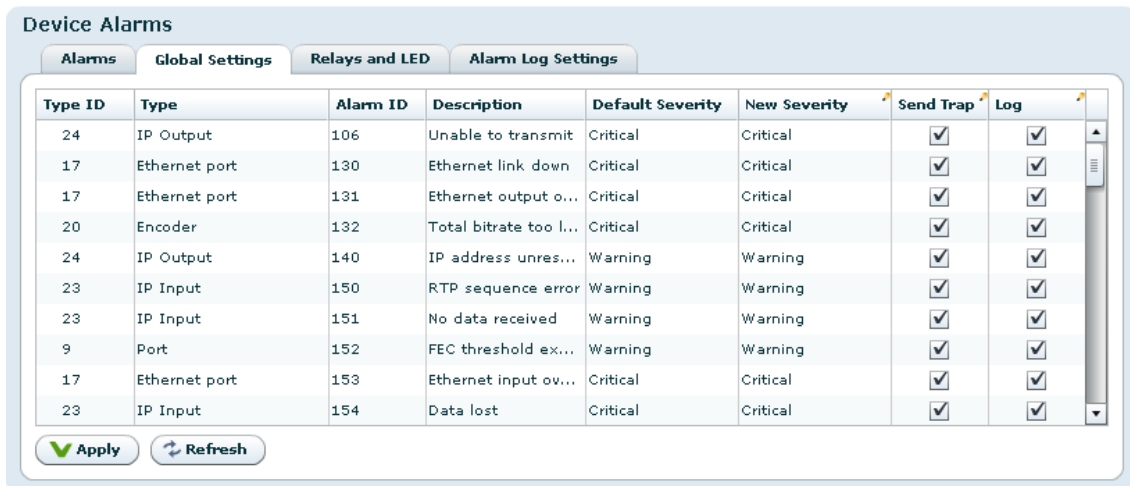
Not used.

'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



The screenshot shows the 'Device Alarms' configuration page with four tabs: 'Alarms', 'Global Settings', 'Relays and LED', and 'Alarm Log Settings'. The 'Alarms' tab is active, displaying a table with the following columns: Type ID, Type, Alarm ID, Description, Default Severity, New Severity, Send Trap, and Log. Below the table are 'Apply' and 'Refresh' buttons.

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

Figure 9.10 Global alarm configuration

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

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

Edited rows are highlighted until changes have been applied.



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

9.4.2.3 Relays and LED configuration

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

Relays and LED configuration interface showing severity level triggers and a table of virtual relays.

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

Figure 9.11 Relays and LED configuration

For further details on the physical relays refer to [Section D.4.4](#).

The Virtual Relays field shown in [Figure 9.11](#) also includes settings for the so-called *virtual relays*. These are programmable status indicators that can be set to react to any specific alarm condition. In the simplest case you may want to enable a relay in case a specific alarm ID turns up. In another case you may want to enable a relay if a specific alarm turns up on a given port. Each relay status are exported on SNMP. Activation of a virtual relay also generates a specific alarm, named "Virtual alarm relay activated" (ID=169).

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

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

2. If the expression evaluates to true, the Count value is increased by 1. You can at any time see the current count value. The Count value simply tells you how many of the current (active) alarm events in the unit that matches the expression.
3. If the count value is larger than or equal (\geq) to the Count Thresh. value the relay is activated.

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

Table 9.1 Legal field values to use in expressions

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

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

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

Table 9.2.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

Table 9.2.b Legal operators to use in expressions

Operator	Description	Sample
IN	Set operator. Returns true if left-hand part is included in set to the right.	id IN (169,200,201)
+	Addition	id + 9 = 169
-	Subtraction	id - 8 = 160
*	Multiply	id * 10 = 100
/	Divide	id / 20 = 8
>	Greater than	id > 100
<	Less than	id < 90
>=	Greater than or equal	id >= 100
<=	Less than or equal	id <= 100

Some examples are given in [Table 9.3](#).

Table 9.3 Expression examples

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

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

9.4.2.4 Alarm Log Settings

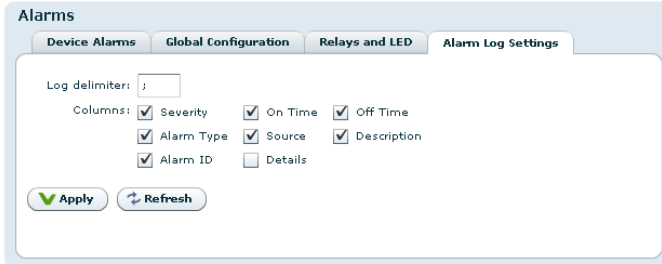
This page is used to set alarm log properties.

Log delimiter

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

Columns

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



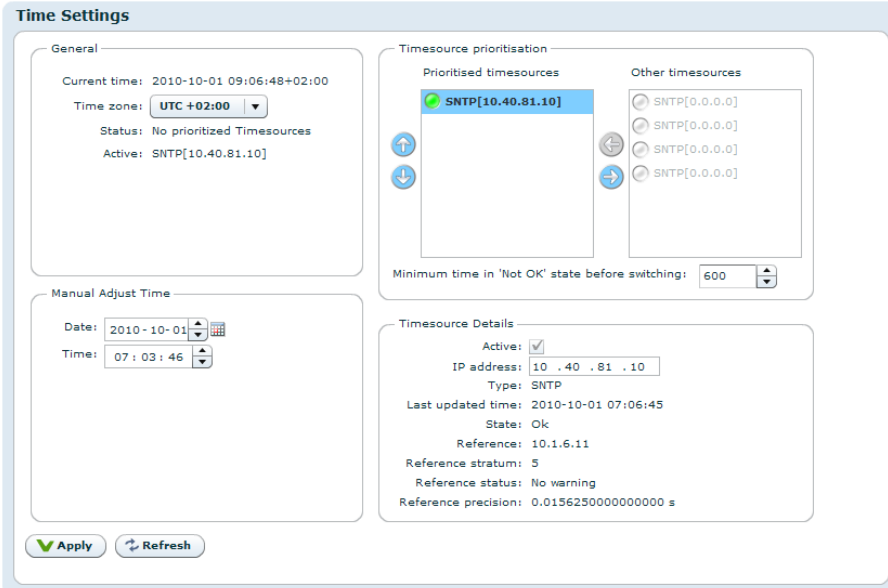
Alarms

Device Alarms Global Configuration Relays and LED **Alarm Log Settings**

Log delimiter: ;

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

Figure 9.12 Configuring the alarm log



Time Settings

General

Current time: 2010-10-01 09:06:48+02:00
Time zone: UTC+02:00
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]
Minimum time in 'Not OK' state before switching: 600

Manual Adjust Time

Date: 2010-10-01
Time: 07:03:46

Timesource Details

Active:
IP address: 10.40.81.10
Type: SNTP
Last updated time: 2010-10-01 07:06:45
State: Ok
Reference: 10.1.6.11
Reference stratum: 5
Reference status: No warning
Reference precision: 0.0156250000000000 s

Figure 9.13 Time Settings

9.4.3 Time Settings

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

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

Current time

The current time as reported by the device.

Time zone

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

Status

The status of the time synchroniser.

Active

The time source currently in use by the time synchroniser.

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

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

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

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

Active

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

IP address

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

Type

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

Last updated time

The most recent time value received from the time source.

State

The current state of the time source.

Reference

Provides the time reference source address of accessed time source.

Reference stratum

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

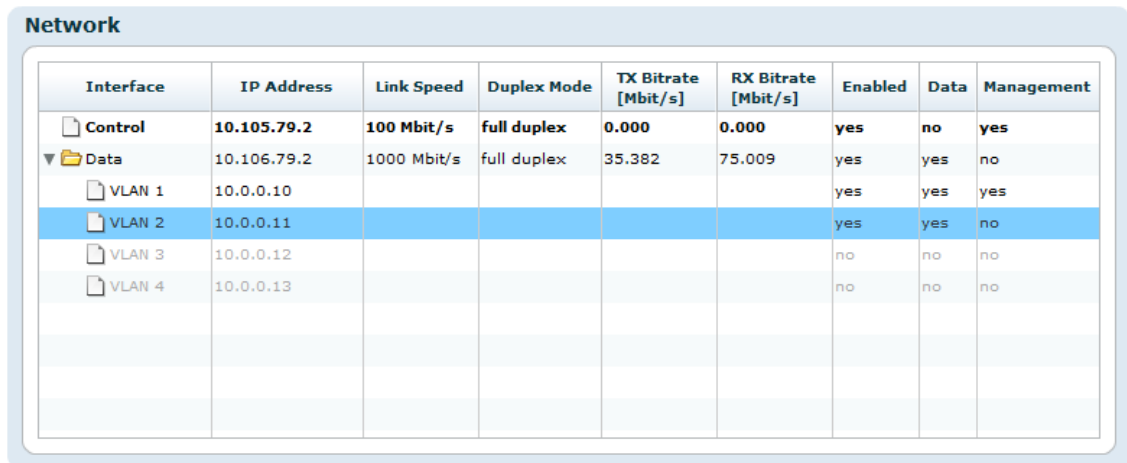
Reference status

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

Reference precision

The timing accuracy that can be expected from the current time source.

9.4.4 Network



Interface	IP Address	Link Speed	Duplex Mode	TX Bitrate [Mbit/s]	RX Bitrate [Mbit/s]	Enabled	Data	Management
Control	10.105.79.2	100 Mbit/s	full duplex	0.000	0.000	yes	no	yes
▼ Data	10.106.79.2	1000 Mbit/s	full duplex	35.382	75.009	yes	yes	no
VLAN 1	10.0.0.10					yes	yes	yes
VLAN 2	10.0.0.11					yes	yes	no
VLAN 3	10.0.0.12					no	no	no
VLAN 4	10.0.0.13					no	no	no

Figure 9.14 Network status

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

Interface

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

IP Address

The IP address configured for this interface.

Link Speed

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

Duplex Mode

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

TX Bitrate

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

RX Bitrate

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

Enabled

Shows whether the interface is currently enabled.

Data

Shows whether data traffic is currently enabled for this interface.

Management

Shows whether management traffic is currently enabled for this interface.

9.4.4.1 Interfaces

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

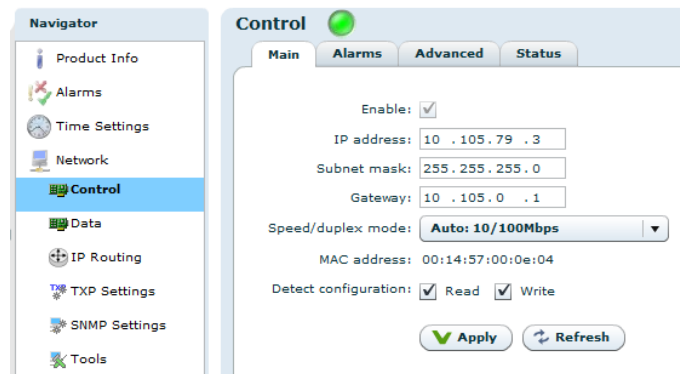
9.4.4.1.1 Main

Figure 9.15 Main IP settings

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

Enable

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

IP address

IP address of the interface.

Subnet mask

The subnet mask of the interface.

Gateway


The default gateway address for the interface.

Media Select

This field is only shown on units licensed to use the optional SFP slot. Select RJ-45 to use the Ethernet port labelled Data for data traffic. Select SFP to use the SFP module for data traffic.

Speed/duplex mode

The speed and duplex mode of the interface. The *Auto* setting enables automatic speed and mode negotiation for the Ethernet link.

 **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 article¹](#).

MAC address


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

Detect configuration

These two options enable the read and write attributes of the IP assignment server module. Only applicable if Control interface is selected.

This server is used by the T-VIPS Detect, which is a stand-alone PC application that can be used to discover T-VIPS devices on a local network and assign IP addresses to them.

Enabling the *Read* option makes the TVG420 visible for the T-VIPS Detect on the LAN. Enabling the *Write* option makes the IP address for the TVG420 configurable using the T-VIPS Detect. These options do not affect the operation of the device from the management application T-VIPS Connect.

 **Note:** Modifying the settings of the interface you are currently using for management may cause loss of contact with the unit. Make sure you will still be able to contact the unit before applying the altered settings.

9.4.4.1.2 Alarms

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

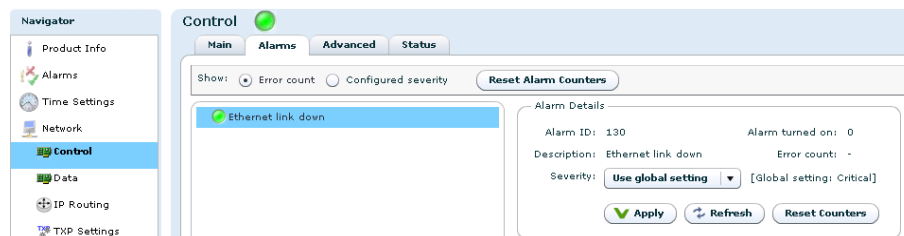


Figure 9.16 Network interface alarms

¹ http://en.wikipedia.org/wiki/Duplex_mismatch

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

9.4.4.1.3 Advanced

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

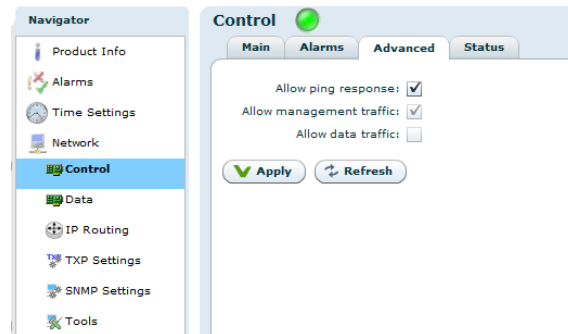


Figure 9.17 Advanced IP settings

Allow ping response

Check this box to filter incoming ICMP messages. If this option is not enabled, the device will not answer to 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 connected through.

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

The IP address of the multicast router. The address here is used in conjunction with the *Use multicast router* option on the IP TX page, see [Section 9.5.1](#).

Multicast is not applicable to the management interface.

IGMP version

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

9.4.4.1.4 Status

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

Ethernet Status

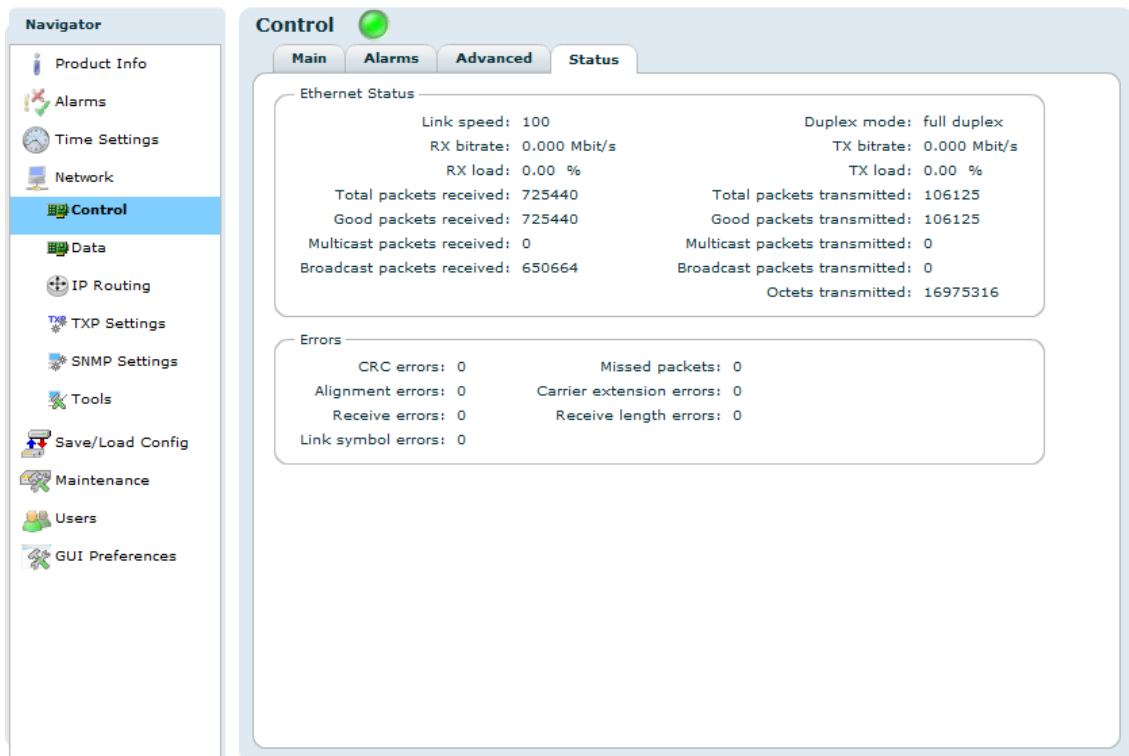


Figure 9.18 Interface Status

Link speed

The detected link speed of the interface.

Duplex mode

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

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

bitrate

The total bitrate received/transmitted.

load

Measured load on interface 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

Errors

CRC errors

Number of packets received with CRC errors.

Alignment errors

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

Receive errors

Number of erroneous packets received.

Missed packets

Number of packets missed.

Link symbol errors

Number of packets with link symbol errors.

Carrier extension errors

Number of packets with carrier extension errors.

Receive length errors

Number of packets with invalid size.

SFP Info

TBD This frame is only shown for the SFP interface. The page displays information provided by the SFP module installed.

9.4.4.1.5 VLAN

This page is only shown on interfaces with VLAN (virtual interface) support. The page allows adding, removing and editing virtual interfaces associated with the selected physical interface.

Enable	ID	Pri	IP Addr	Net Mask	GW Addr	Multicast Router	Data	Control	Ping	IGMP ver
<input checked="" type="checkbox"/>	1	0	10.0.0.10	255.255.255.0	10.0.0.1	0.0.0.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	v3
<input checked="" type="checkbox"/>	2	0	10.107.3.236	255.255.255.0	10.0.0.1	0.0.0.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	v2
<input type="checkbox"/>	3	0	10.0.0.10	255.255.255.0	10.0.0.1	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	v2
<input type="checkbox"/>	4	0	10.0.0.10	255.255.255.0	10.0.0.1	0.0.0.0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	v2

Figure 9.19 VLAN configuration

Editing is done directly in the table. Edited fields are shown with a yellow background. Pending deletions are shown with a red background. New VLANs may be edited after clicking the Add VLAN button.

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

Enable

Enable/disable the virtual interface.

VLAN id

The id of this virtual interface. Must be unique.

Priority

The priority of this virtual interface. Numbers 0 to 7 are valid. For further information on VLAN priority usage, refer to [\[7\]](#).

IP Addr

The IP address of the virtual interface.

Net Mask

The subnet mask of the virtual interface.

GW Addr

The gateway address to use for the virtual interface.

Multicast Router

The multicast router for this virtual interface.

Data

Checked box enables the virtual interface to allow data traffic.

Control

Checked box enables the virtual interface to allow management traffic.

Ping

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

IGMP ver

Provides selection of the IGMP version to use.

Below the table are four buttons. In addition to the apply and refresh buttons there are buttons for adding and removing VLANs.

9.4.4.1.6 SFP

The SFP tab, [Figure 9.20](#), is only shown if the unit is equipped with an SFP slot and when SFP is selected in the Media select pull-down list in [Section 9.4.4.1](#). Furthermore, the module configuration sub-pages are presented only if SFP configuration has been licensed [Section 9.4.7.1](#).

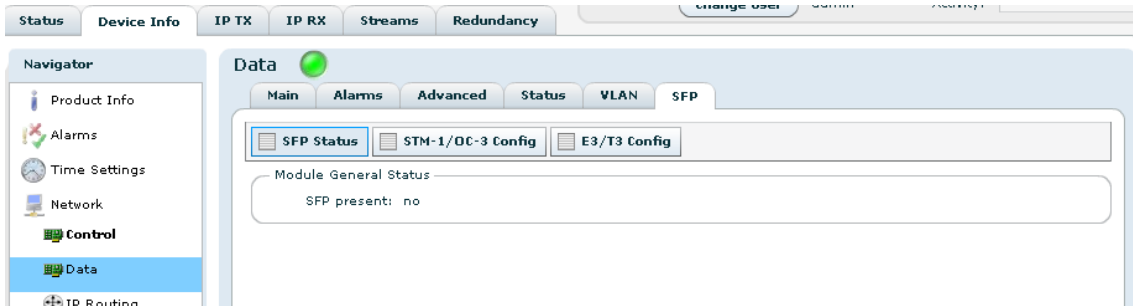


Figure 9.20 The Device info > Network > SFP tab

The **SFP Status** page, shown in figure **Figure 9.21**, presents four fields providing an overview of the module status. The appearance of the status page and the range of parameters shown depend on the type of module attached.

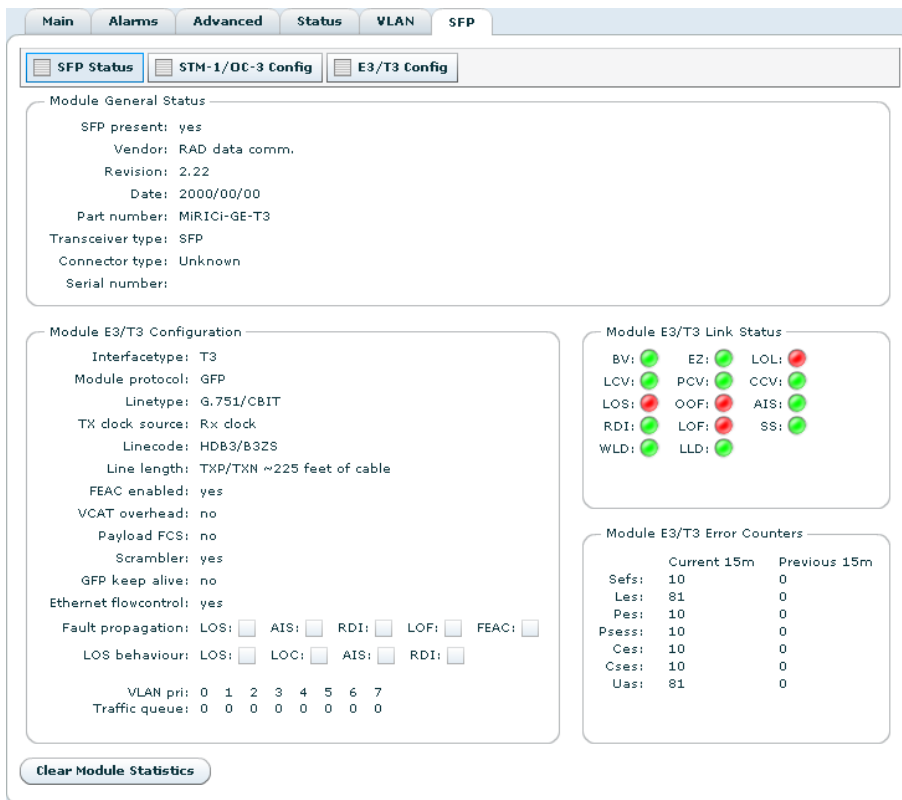


Figure 9.21 The SFP status page

The Module General Status field displays the status of the module as seen by the TVG420.

SFP Present

Indicates that the module has been detected by the TVG420.

Vendor

Shows the vendor name.

Revision

Indicates the module revision.

Date

Indicates the revision date.

Part number

The module part number.

Transceiver type

The type of transceiver inside the SFP module. Only a limited range of transceivers is compatible with the TVG420.

Connector type

Indicates the network connector type.

Serial number

The serial number of the SFP module.

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

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

TIM-P

Trace ID Mismatch (Path)

LOS

Loss of Signal

AIS_L

Alarm Indication Signal (Line)

RDI_L

Remote Defect Indication (Line)

UNEQ_P

Payload Label Mismatch (Path)

LOF

Loss of Frame

AIS_P

Alarm Indication (Path)

RDI_P

Remote Defect Indication (Path)

EED

Excessive Error Defect

LOP

Loss of Point

SD

Signal Degrade

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

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

BV

Bipolar Violation

LCV

Line Coding Violation

LOS

Loss of Signal

RDI

Remote Detection Indication

WLD

WAN Loop Detected

EZ

Excessive Zeroes

PCV

P-bit Coding Violation

OOF

Out of Frame

LLD

Lan Loop Detected

LOL

LIU Out of Lock

CCV

C-bit Coding Violation

AIS

Alarm Indication Signal

SS

System Status.

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

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

Current

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

15mins

Displays the result of the previous 15 minutes counting interval.

Section

“Section” related error counts

Line

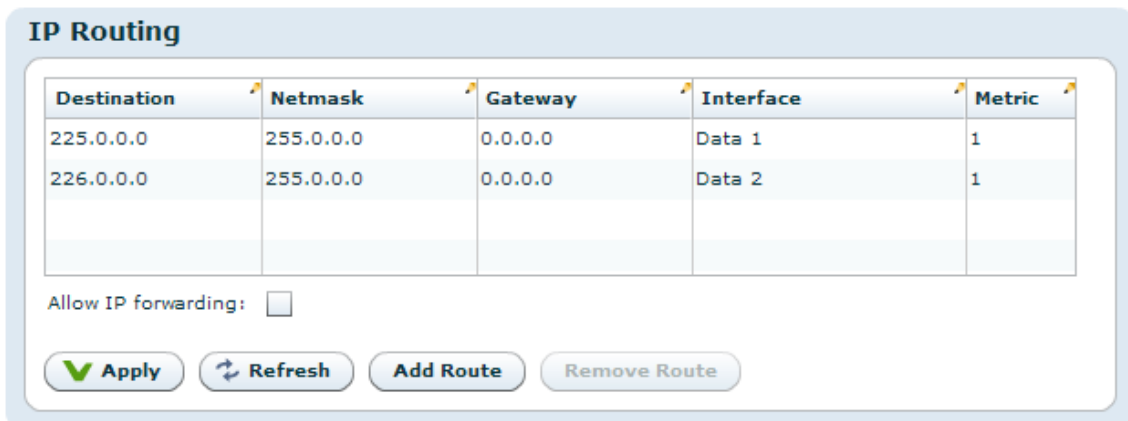
“Line” related error counts

Path

“Path” related error counts

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

9.4.4.2 IP Routing



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

Allow IP forwarding:

Figure 9.22 IP Routing

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

Destination

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

Netmask

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

Gateway

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

Interface

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

Metric

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

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

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



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

9.4.4.3 TXP Settings

The screenshot shows the 'TXP Settings' configuration page. It features a 'Mode' dropdown menu set to 'Read'. Below it is a checked checkbox for 'Anonymous read'. There are two more dropdown menus: 'Required level for read' set to 'Guest' and 'Required level for write' set to 'Operator'. At the bottom of the settings area are two buttons: 'Apply' with a green checkmark icon and 'Refresh' with a circular arrow icon.

Figure 9.23 TXP Settings

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

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

Mode

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

Anonymous read

Selects whether read accesses should be allowed without entering user credentials. This may only be edited if *Mode* is different from 'disabled'.

Required level for read

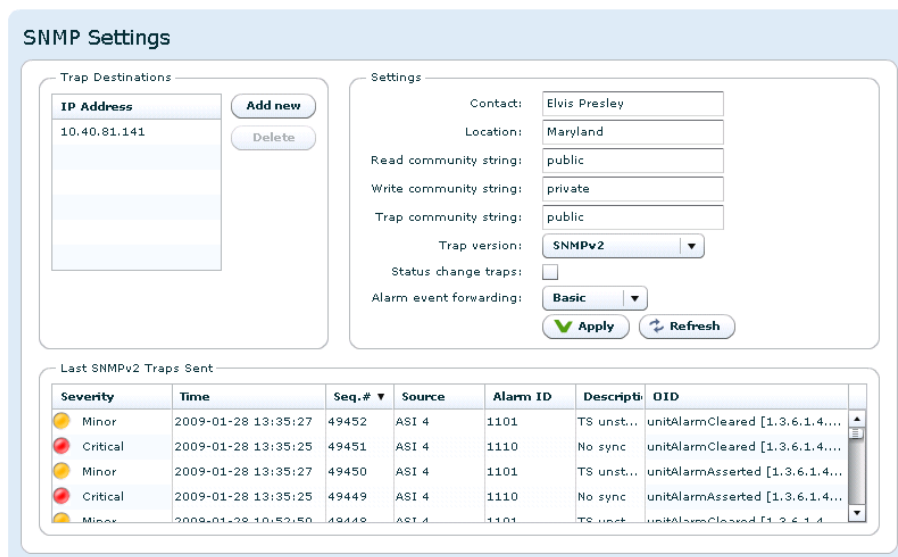
The required user level for TXP read accesses. This may only be edited if *Mode* is different from 'disabled' and 'anonymous read' is not selected.

Required level for write

The required user level for TXP write accesses. This may only be edited if *Mode* is set to 'write'.

9.4.4.4 SNMP Settings

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



Severity	Time	Seq.#	Source	Alarm ID	Description	OID
Minor	2009-01-28 13:35:27	49452	ASI 4	1101	TS unst... unitAlarmCleared [1.3.6.1.4...	
Critical	2009-01-28 13:35:25	49451	ASI 4	1110	No sync unitAlarmCleared [1.3.6.1.4...	
Minor	2009-01-28 13:35:27	49450	ASI 4	1101	TS unst... unitAlarmAsserted [1.3.6.1.4...	
Critical	2009-01-28 13:35:25	49449	ASI 4	1110	No sync unitAlarmAsserted [1.3.6.1.4...	
Minor	2009-01-28 10:52:56	49448	ASI 4	1101	TS unst... unitAlarmCleared [1.3.6.1.4...	

Figure 9.24 SNMP Settings

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

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

Status change traps

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

Alarm event forwarding

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

Disabled

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

Basic

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

Detailed

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

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

For more information about the configuration settings for SNMP, please refer to [Section 10.4](#) in [Chapter 10: SNMP](#).

9.4.4.5 Tools

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

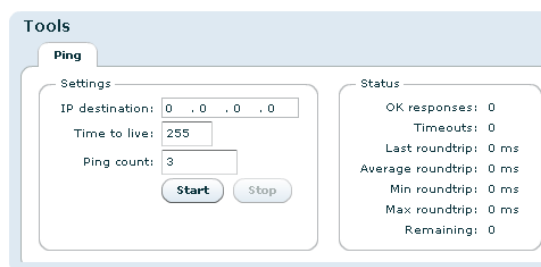


Figure 9.25 The Ping tool

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.

TTL (Time To Live)

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

Ping count

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

Start

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

OK responses

The number of ping responses received.

Timeouts

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

Last roundtrip

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

Average roundtrip

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

Min roundtrip

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

Max roundtrip

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

Remaining

The number of remaining ping requests in this session.

9.4.5 Clock Regulator

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

9.4.5.1 Main

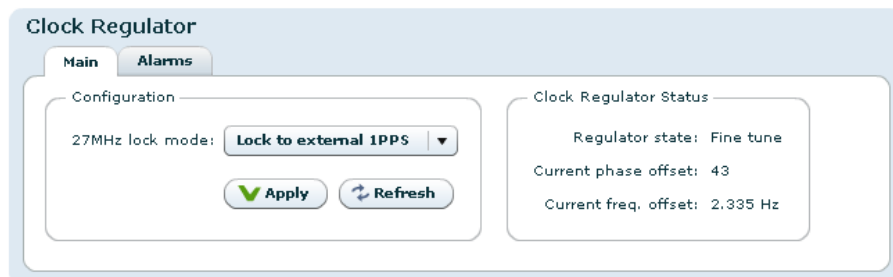


Figure 9.26 Clock regulator

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.

Lock to external 10 MHz

Configures the internal clock to use the external 10 MHz 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.

9.4.5.2 Alarms

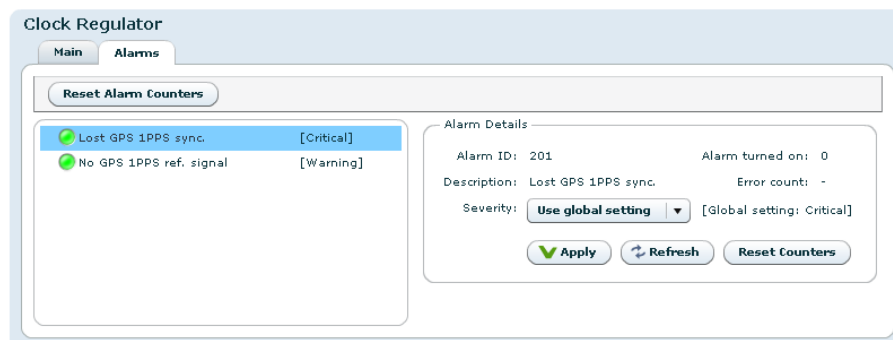


Figure 9.27 Clock regulator Alarms

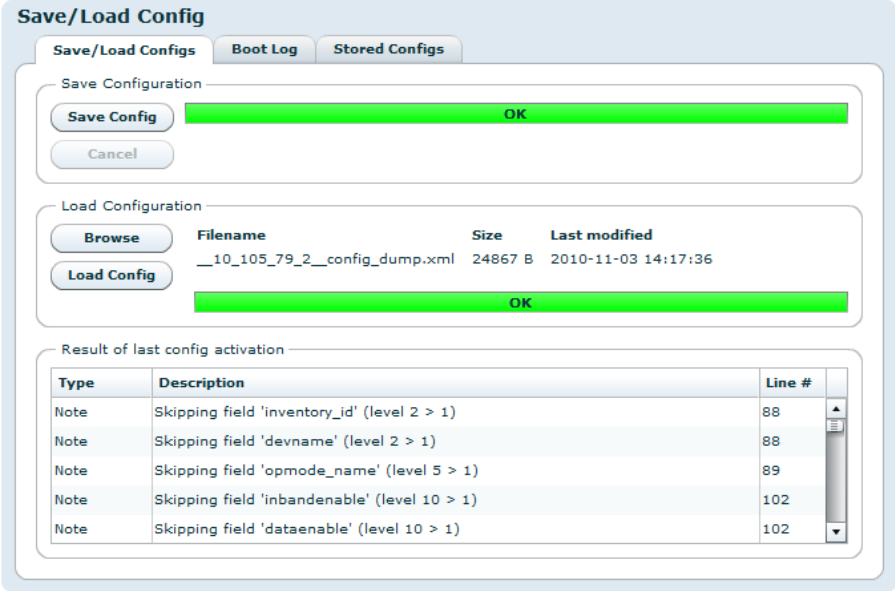
These are the Clock regulator specific alarms. Clicking an alarm opens the field to configure the alarm. Please see [Section 9.4.2](#) for alarm configuration details.

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



Save/Load Config

Save/Load Configs Boot Log Stored Configs

Save Configuration

Save Config OK

Cancel

Load Configuration

Browse Filename Size Last modified

Load Config OK

Filename	Size	Last modified
__10_105_79_2_config_dump.xml	24867 B	2010-11-03 14:17:36

Result of last config activation

Type	Description	Line #
Note	Skipping field 'inventory_id' (level 2 > 1)	88
Note	Skipping field 'devname' (level 2 > 1)	88
Note	Skipping field 'opmode_name' (level 5 > 1)	89
Note	Skipping field 'inbandenable' (level 10 > 1)	102
Note	Skipping field 'dataenable' (level 10 > 1)	102

Figure 9.28 Saving and loading of configuration files

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.

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

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

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

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

Options specific to the device, including device name and management port network configuration, are intentionally disregarded during the import process. This is a convenience feature as it allows configurations to be easily moved from one device to another and also makes management easier as the Web UI will continue to be able to communicate with the device after a new configuration has been loaded.

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

9.4.6.2 Boot Log

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

9.4.6.3 Stored Configs

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

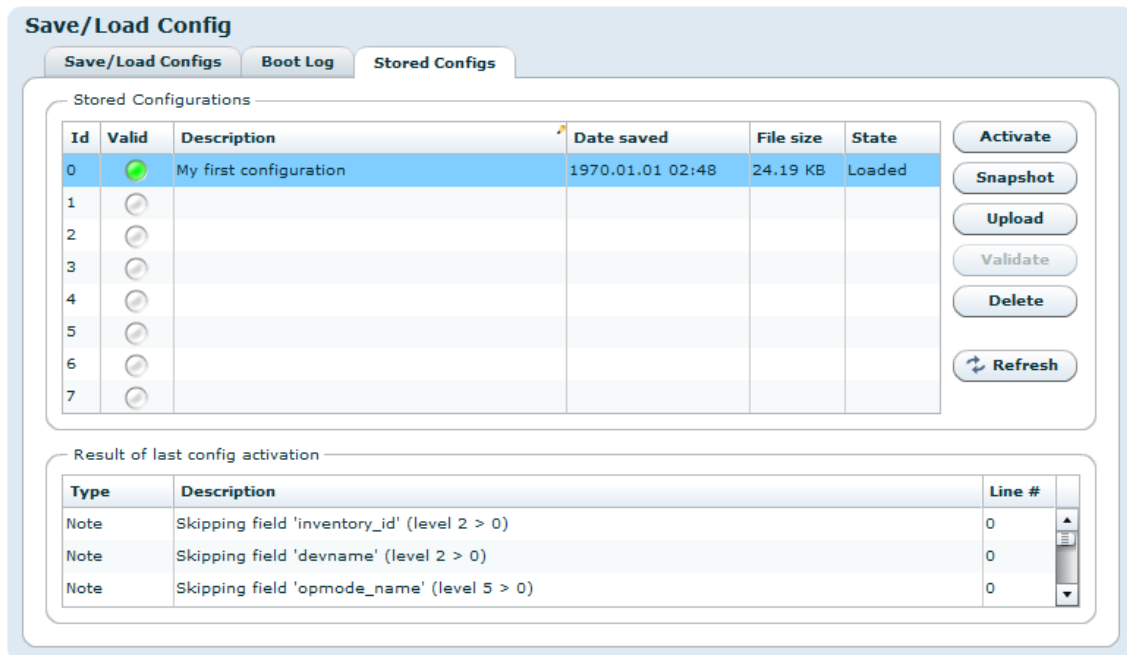
The table lists the currently stored snapshots, and columns in the table provide information specific to each snapshot as follows:

Id

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

Valid

Indicates if the uploaded config has a valid XML syntax or not. Valid syntax is indicated



The screenshot shows the 'Save/Load Config' web interface. It has three tabs: 'Save/Load Configs', 'Boot Log', and 'Stored Configs'. The 'Stored Configs' tab is active, displaying a table of configurations. The first row is highlighted in blue and has a green indicator in the 'Valid' column. The other rows have silver indicators. To the right of the table are buttons for 'Activate', 'Snapshot', 'Upload', 'Validate', 'Delete', and 'Refresh'. Below the table is a section titled 'Result of last config activation' with a table showing three notes about skipping fields.

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

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

Figure 9.29 Locally stored configuration files

by a green indicator and a invalid syntax is indicated by a red indicator. A silver indicator in this column signifies that the slot is empty and available.

Description

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

Date saved

Time stamp when the configuration was uploaded to the unit.

File size

Size of the configuration file.

State

Full

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

Loaded

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

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

Activate

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

Snapshot

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

Upload

Import a locally stored configuration file.

Validate

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

Delete

Delete the entry selected in the snapshot list.

Refresh

Reload the list.

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

9.4.7 Maintenance

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

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

9.4.7.1 General

The General tab on the maintenance page details the current software, hardware and license 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, the user is prompted after some seconds delay to reload the Web UI in the browser.

Restore Factory Defaults

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

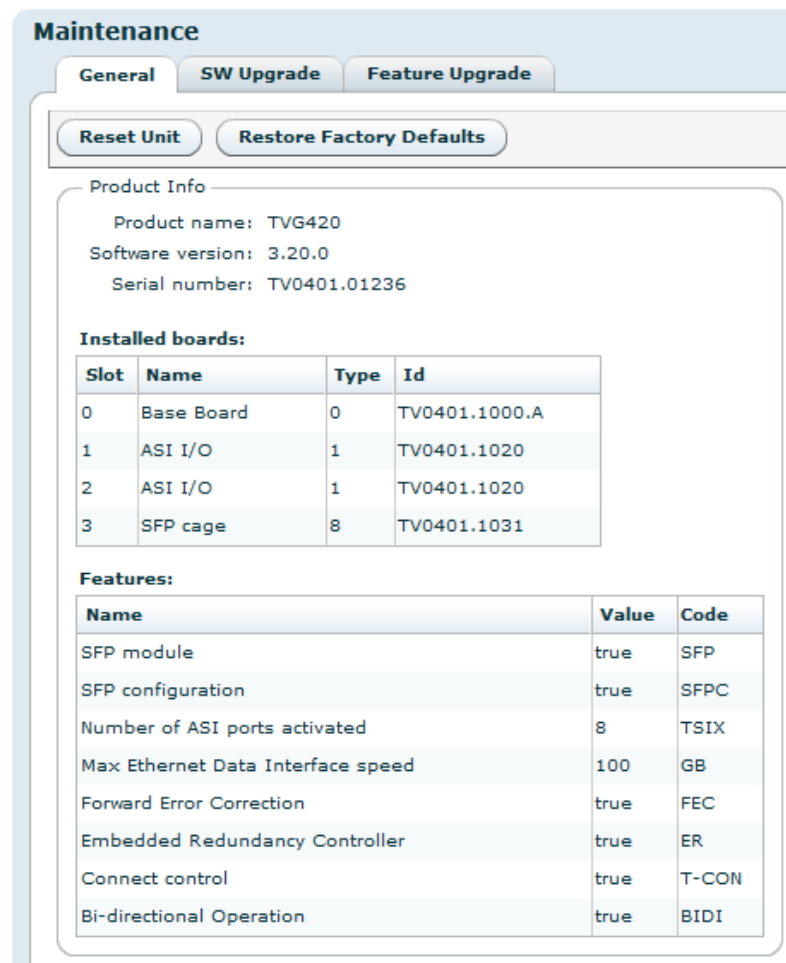
The Product info field provides the following information:

Product name

This is the product model name.

Software version

The version of the firmware image installed on the unit.



Maintenance

General SW Upgrade Feature Upgrade

Reset Unit Restore Factory Defaults

Product Info

Product name: TVG420
 Software version: 3.20.0
 Serial number: TV0401.01236

Installed boards:

Slot	Name	Type	Id
0	Base Board	0	TV0401.1000.A
1	ASI I/O	1	TV0401.1020
2	ASI I/O	1	TV0401.1020
3	SFP cage	8	TV0401.1031

Features:

Name	Value	Code
SFP module	true	SFP
SFP configuration	true	SFPC
Number of ASI ports activated	8	TSIX
Max Ethernet Data Interface speed	100	GB
Forward Error Correction	true	FEC
Embedded Redundancy Controller	true	ER
Connect control	true	T-CON
Bi-directional Operation	true	BIDI

Figure 9.30 Maintenance

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).

9.4.7.2 Software Upgrade

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

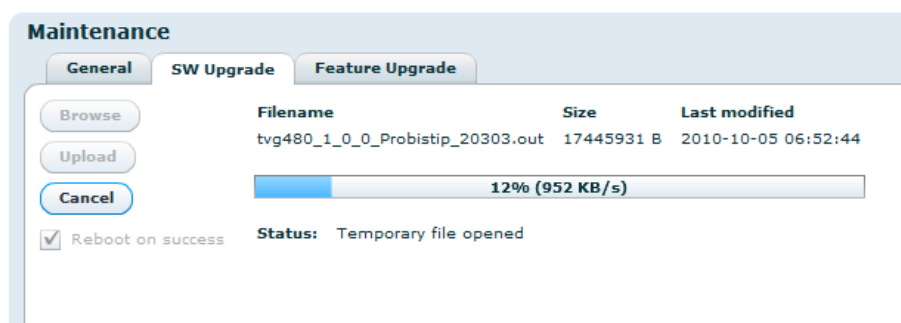


Figure 9.31 Software Upgrade

Browse

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

Upload

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

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

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

Cancel

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

Reboot on success

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

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

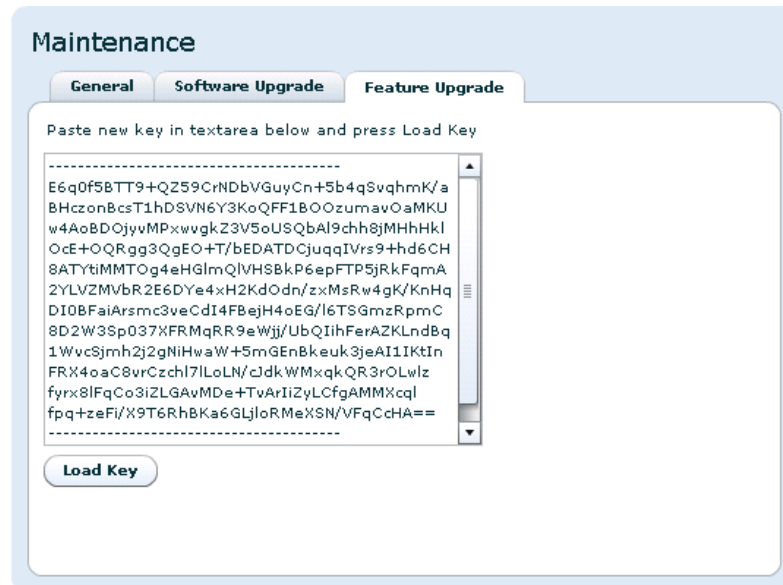
If the Reboot on success option is active the unit will automatically reboot when loading is complete, otherwise an alarm New SW pending is set to indicate that a new SW will be used on next manual reboot.

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



Note: It is recommended to verify the new software version via the “Product Info” page ([Section 9.4.1](#)) to verify that the update was successful and the latest software revision is active.

9.4.7.3 Feature Upgrade



Maintenance

General Software Upgrade **Feature Upgrade**

Paste new key in textarea below and press Load Key

```

-----
E6q0f5BTT9+QZ59CrNdbVGuyCn+5b4qSvqhmK/a
BHczonBcsT1hDSVN6Y3KoQFF1B0OzumavOaMKU
w4AoBDOjyvMPxwvgkZ3V5oUSQbAl9chh8jMHhHkI
OcE+OQRgg3QgEO+T/bEDATDCjuqqIVrs9+hd6CH
8ATYtiMMTOg4eHGlMqIVHsBkP6epFTP5jRkFqmA
2YLVZMVbR2E6DYe4xH2KdOdn/zxMsRw4gK/KnHq
D10BFaiArsmc3veCdI4FBejH4oEG/l6TSGmzRpmC
8D2W3Sp037xFRMqRR9eWjj/UbQIihFerAZKLnDbq
1WvcSjmh2j2gNiHwaW+5mGEnBkeuk3jeAI1IKtIn
FRX4oaC8vrCzchl7lLoLN/cJdkWMxqkQR3rOLwIz
fyrx8lFqCo3iZLGAvmDe+TvArIzylCfGAMMXcql
fpq+zeFi/X9T6RhBKa6GJlloRMexSN/VFqCCHA==
-----

```

Load Key

Figure 9.32 Feature Upgrade

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

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



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

9.4.8 Users

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

Auto login

Specifies the user privilege level to use for automatic login to the device. Changing this

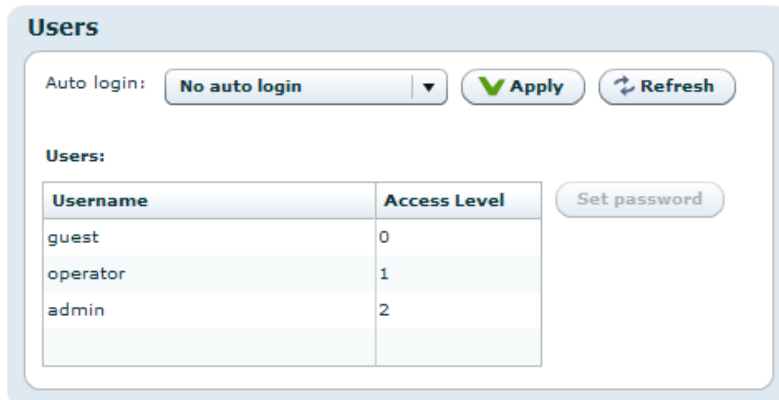


Figure 9.33 Users page

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, however each privilege level 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.

There are three user privilege levels available on the device.

guest

Can view configuration information and alarm logs

operator

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

admin

Device administrator, full access to the device.

9.4.9 GUI Preferences

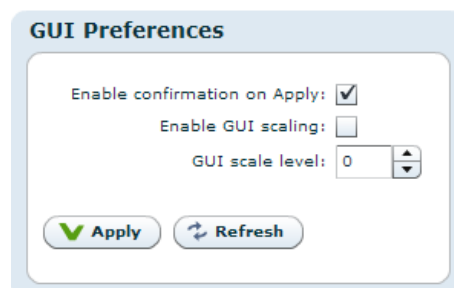


Figure 9.34 GUI Preferences page

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

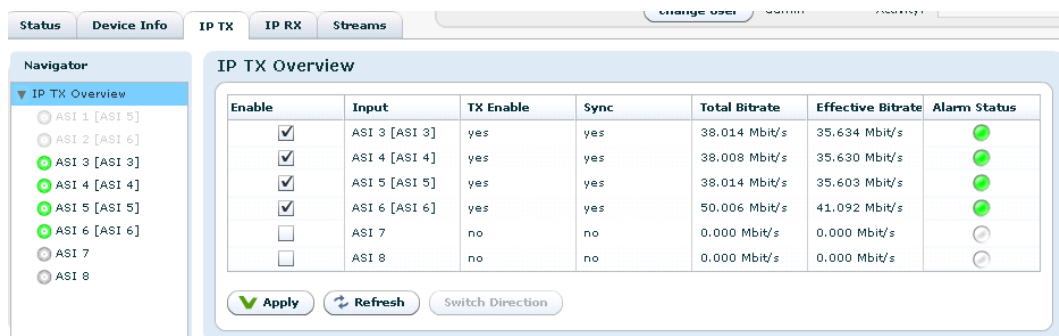
If enabled, the web interface will be shown with the currently configured GUI scale level. It also enables the use of CTRL + + and CTRL + - to change scale level. When enabling or disabling this option the web interface may hang for some seconds as it changes the font used.

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 IP TX

Figure 9.35 shows the IP TX page. The purpose of this page is to provide an interface for configuring the different streams to be sent through the unit. The left part of screen shows a tree containing all the DVB ASI input ports. To the right the page shows the IP transmission parameters for the ASI ports configured as inputs. To select a port, click that port. The bottom part of the page contains an alarm table, which shows all alarms related to the MPEG2 stream transmission. It remains visible irrespective of the tab selected. For all tabs buttons are provided to apply changes made to the settings or to discard changes prior to committing them. A third button allows changing the direction of a highlighted port. Once a port is selected this button re-appears in the top right of the page (if bidirectional mode is licenced).



Enable	Input	TX Enable	Sync	Total Bitrate	Effective Bitrate	Alarm Status
<input checked="" type="checkbox"/>	ASI 3 [ASI 3]	yes	yes	38.014 Mbit/s	35.634 Mbit/s	●
<input checked="" type="checkbox"/>	ASI 4 [ASI 4]	yes	yes	38.008 Mbit/s	35.630 Mbit/s	●
<input checked="" type="checkbox"/>	ASI 5 [ASI 5]	yes	yes	38.014 Mbit/s	35.603 Mbit/s	●
<input checked="" type="checkbox"/>	ASI 6 [ASI 6]	yes	yes	50.006 Mbit/s	41.092 Mbit/s	●
<input type="checkbox"/>	ASI 7	no	no	0.000 Mbit/s	0.000 Mbit/s	●
<input type="checkbox"/>	ASI 8	no	no	0.000 Mbit/s	0.000 Mbit/s	●

Figure 9.35 The IP TX overview page

9.5.1 Main

The IP TX main sub-page 9.36 is where you configure most of the parameters related to a stream to transmit over the IP network.

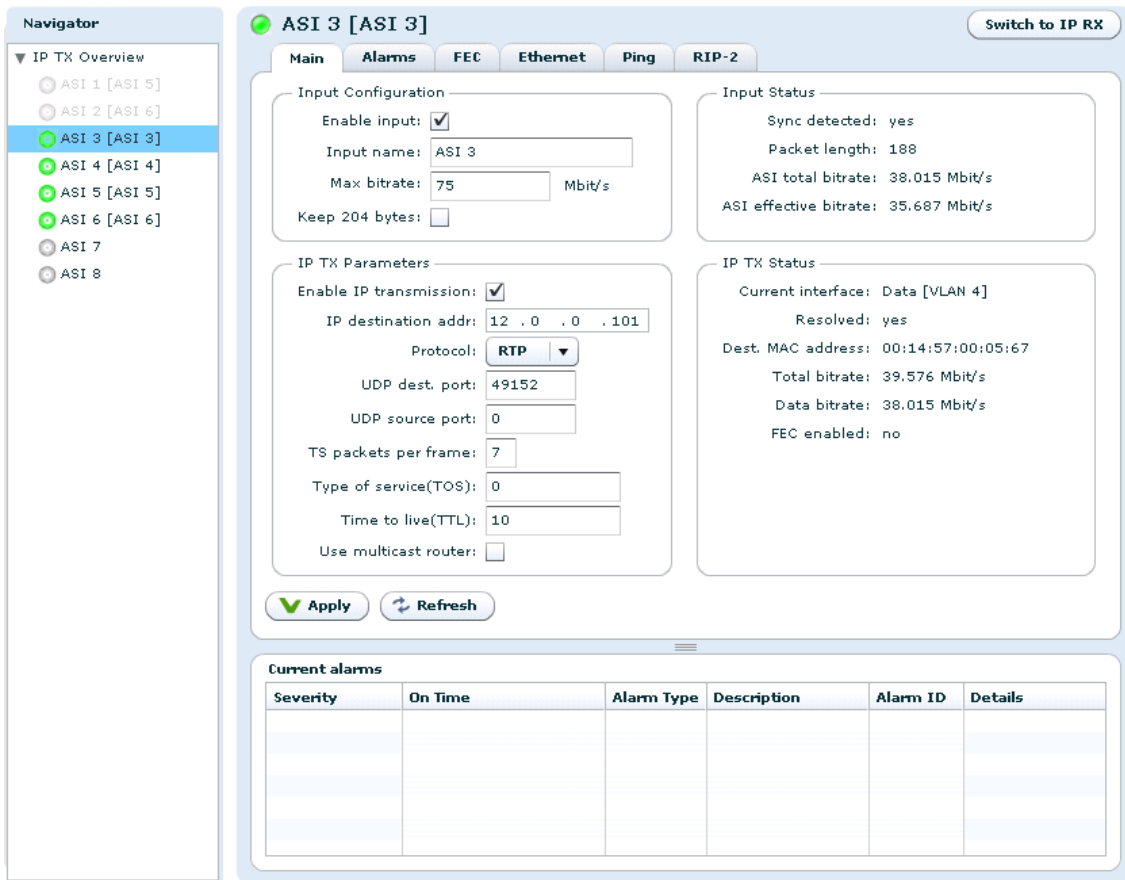


Figure 9.36 IP TX main page

The *Input Configuration* field:

Enable input

Tick this box to enable an input. If this is not ticked this ASI input will not accept an incoming MPEG-2 transport stream. The input port will be grey in the status view (see [Section 9.3.1](#)).

Input name

Enter a name reference to an ASI input stream.

Max bitrate

Enter the maximum bitrate the ASI input stream is allowed to use in the IP channel. If the actual ASI input stream exceeds this bitrate some data in this stream will be discarded to keep its bitrate within the limit. On the other hand, when set correctly this prevents one ASI stream from occupying excessive IP channel capacity, which may disrupt other streams sharing the same channel. The sum of 'Max bitrate' for all active channels should not exceed the IP channel bandwidth.

Keep 204 bytes

Tick this box to transparently transmit all 204 bytes of the incoming ASI transport stream,

if present. When only 188 byte packets are received or the box is unchecked only 188 bytes of each transport stream packet is transmitted, i.e. the 16 bytes reserved for RS error correction data are not transmitted.

The *Input Status* field:

Sync detected

Yes if the unit is receiving a valid DVB ASI stream on the ASI input interface. No if no DVB ASI stream is received.

Packet length

Shows the packet length of the MPEG2 transport stream packets received (188 or 204 bytes).

ASI total rate

Shows the bitrate of the MPEG2 transport stream on the input including NULL packets.

ASI effective rate

Shows the net bitrate of the MPEG2 transport stream on the input, i.e. bitrate excluding NULL packets.

The *IP TX Parameters* field:

Enable IP transmission

Click this box to enable the MPEG-2 transport stream on the DVB ASI input to be sent through the IP network.

Protocol

Select UDP or RTP transmission mode. See [Section 6.5.1](#) for more information on this.

IP destination addr

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

UDP dest. port

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

Note: Ensure that there is no conflict in UDP ports used. Pay special attention to the fact that if FEC data are used they are always sent on UDP ports two higher than the media port and four higher than the media port. E.g. if 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 for the current stream. UDP port numbers are in the range 1-65535. Note that the TVG420 receiver unit does not check this parameter when receiving streams. FEC streams are transmitted with the same UDP source port as the media frames.

TS packets per frame

Enter the number of 188 byte MPEG-2 transport stream packets to map into each UDP

frame. Valid values are between 1 and 7. We generally recommend using 7 when TVG420 is used both at the sender and the receiver to reduce overhead. For very low bitrate streams, less than 7 packets per frame may be used to reduce the delay through the unit.

Type of service (TOS)

Enter Type of Service parameter as a byte value to be set in the Type-of-Service (TOS) field in the IP header as specified in RFC-791. This parameter is used for Class-of-Service prioritization. It depends on the Routers honouring this field. Please refer to [Appendix A](#) "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.

Use multicast router

Click this box to force use of a particular multicast router. The address of this multicast router is the same for the entire unit and is configured in the Network sub-page of the Device Info page. When this option is enabled, the destination MAC address used when configuring a multicast destination IP address will be the MAC address resolved directly from the IP of the globally configured multicast router. If this option is left unchecked, multicast destination IP addresses automatically resolve to dedicated multicast MAC addresses – this is the default behaviour in a multicast enabled network.

The *IP TX Status* field:

Resolved

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

Destination 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 IP address. 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.

Total bitrate

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

Data bitrate

The bitrate of the IP frames containing this MPEG-2 transport stream, excluding FEC information.

9.5.2 Alarms

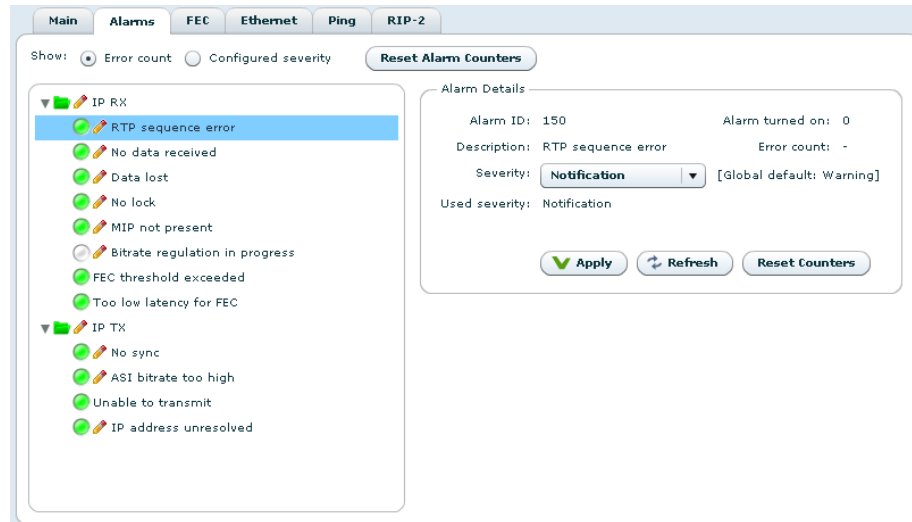


Figure 9.37 The alarms page of an IP transmitter

Each individual port has its own alarm configuration that can be used to override the global default setting. A pencil icon appears next to the alarm label when the alarm is overridden. Please see [Section 9.4.2.1](#) for details on alarm configuration.

9.5.3 FEC

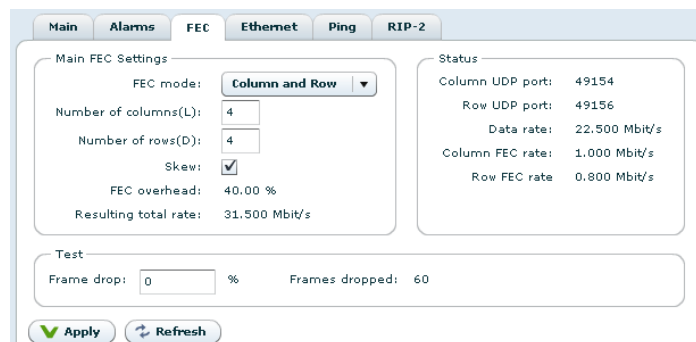


Figure 9.38 IP TX FEC page

This tab will appear only if the Forward error correction feature has been licenced.

The *Main FEC Settings* field:

FEC Mode

Select No FEC to not calculate and send any FEC data. Select Column only to calculate and send one-dimensional FEC data. Select Column and Row to calculate and send two-dimensional FEC data.

Number of columns (L)

Enter number of columns.

Number of rows (D)

Enter number of rows.



32.

Note: Please note that the maximum matrix size is 256 (L*D) and that D is in the range $4 \leq D \leq 32$. In column only mode L is in the range $1 \leq L \leq 32$, while in column and row mode $4 \leq L \leq 32$. L+D can not exceed



CoP 3.

Note: Please note that 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

Skew

Controls whether to organize the column FEC with or without skew. When enabling skew, the delay required on the receiver is less than when transmitting straight columns.

FEC overhead

This number is the overhead in percent caused by the current FEC configuration.

Resulting total rate

This is the resulting total IP bitrate including FEC overhead for this channel. The Status frame contains status parameters related to the FEC setting.

The *Status* field:**Column UDP port**

This parameter is the UDP port used for the column FEC data. The value is always Media UDP port + 2, in accordance with Pro-MPEG CoP 3.

Row UDP port

This parameter is the UDP port used for the row FEC data. The value is always Media UDP port + 4, in accordance with Pro-MPEG CoP 3.

Data rate

This parameter shows the IP data rate for this channel excluding FEC data.

Column FEC rate

This parameter shows the IP data rate for the column FEC data of this channel.

Row FEC rate

This parameter shows the IP data rate for the row FEC data of this channel.

In order to make it possible to demonstrate the function of the FEC engine, TVG420 provides a mode to drop IP packets on the transmitter.

The *Test* field:

Frame drop

Enter the percentage of packets to be dropped from this channel. This value is not stored in the unit and must be entered after each power on.

Frames dropped

This counter shows the number of frames discarded at the output of the unit.

9.5.4 Ethernet

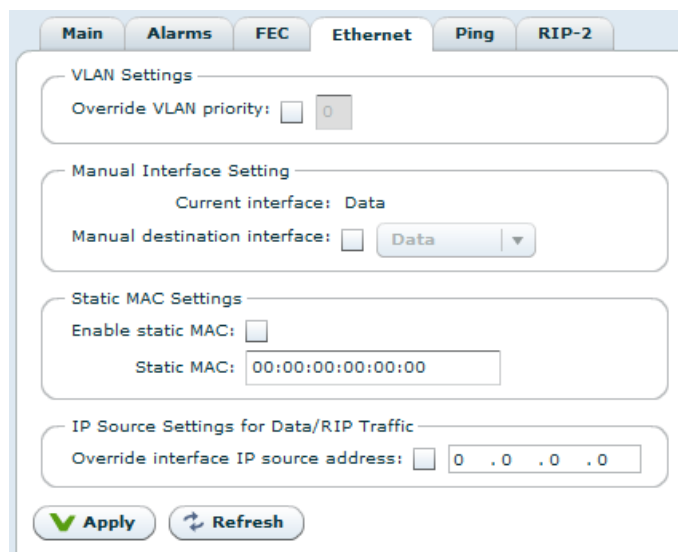


Figure 9.39 The Ethernet page of an IP transmitter

The *VLAN settings* field:

Override VLAN priority

Checking this box overrides the VLAN priority setting that may have been entered for this IP stream in the Network/Interface/VLAN page. A new priority must be entered in the field adjacent to the check box.

The *Manual Interface Setting* field:

Manual destination interface

This check box opens the possibility to use a destination interface different from the default. The destination interface must have been previously configured to be available for selection.

The *Static MAC Settings* field:

Static MAC destinations 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.

Enable static MAC

Check this box to enable insertion of the static MAC address.

Static MAC

Enter the destination MAC address.

The *IP Source Settings for Data/RIP Traffic* filed:

Override interface IP source address

Checking the box enables overriding the default unit source address with the value entered in the adjacent space.

9.5.5 Ping

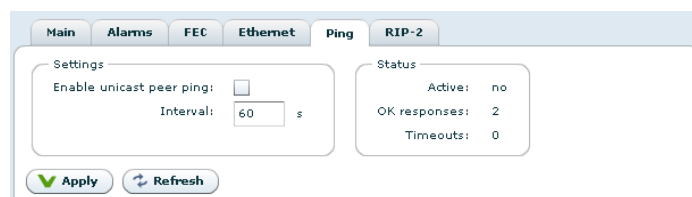


Figure 9.40 The Ping page of an IP transmitter

Ping is used to resolve network problems, avoid flooding, or where the receiver or a network component on the way to the receiver times out during MAC address lookup. This feature helps solving such issues by pushing through a ping message regularly. Also makes it possible for the sender identify if there currently is an active recipient.

Enable Unicast Peer Ping

Check this box to enable regular pingging of the peer, e.g. the receiver of the stream. This will only have effect in unicast mode.

Interval

Set the interval in seconds between each Ping.

Active

Indicates if the channel is actively sending Ping.

OK responses

Indicates how many valid Ping responses have been received.

Timeouts

Indicates how many of the sent Ping messages timed out before receiving a valid response.

9.5.6 RIP-2

The TVG420 is equipped with RIP-2 functionality. If enabled, the TVG420 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.

Figure 9.41 shows the layout of the RIP-2 page.

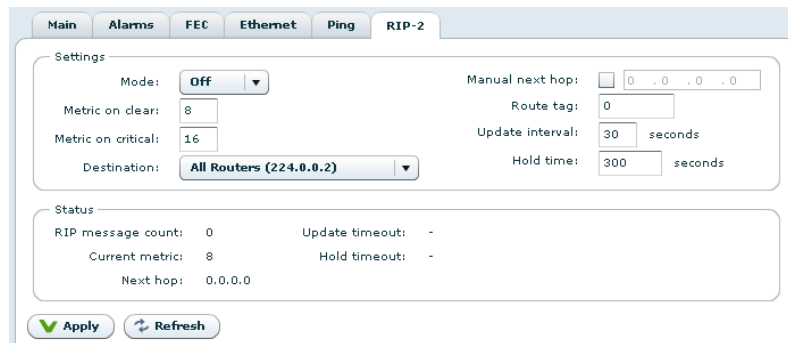


Figure 9.41 RIP-2 page

The *Settings* field allow configuring of parameters are as follows:

Mode

Controls the mode of the RIP-2 engine.

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 TVG420 adds some random delay to avoid sending messages too regularly.

The *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.

9.6 IP RX

Figure 9.42 shows the IP RX page. The purpose of this page is to provide an interface for configuring the different streams to be received by the unit. The left part of screen shows a tree containing all the DVB ASI outputs port. To the right the page shows the IP transmission parameters for the ASI ports configured as outputs. To select a port, click that port. The bottom part of the page contains an alarm table, which shows all alarms related to the MPEG2 stream transmission. It remains visible irrespective of the tab selected. For all tabs buttons are provided to apply changes made to the settings or to discard changes prior to committing them. A third button allows changing the direction of a highlighted port. Once a port is selected this button re-appears in the top right of the page (if bidirectional mode is licensed).

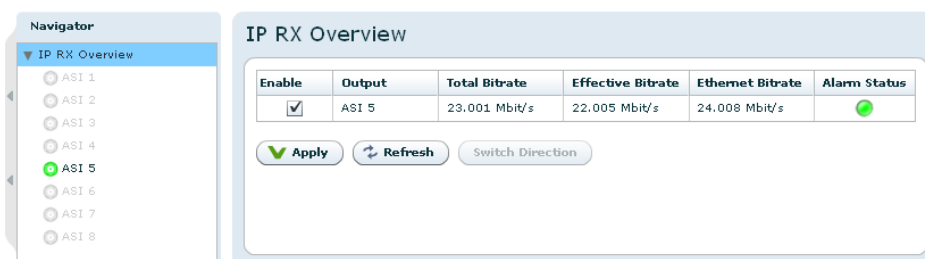


Figure 9.42 IP RX overview page

9.6.1 Main

The IP RX main sub-page is where you configure most of the parameters related to a stream to receive over the IP network.

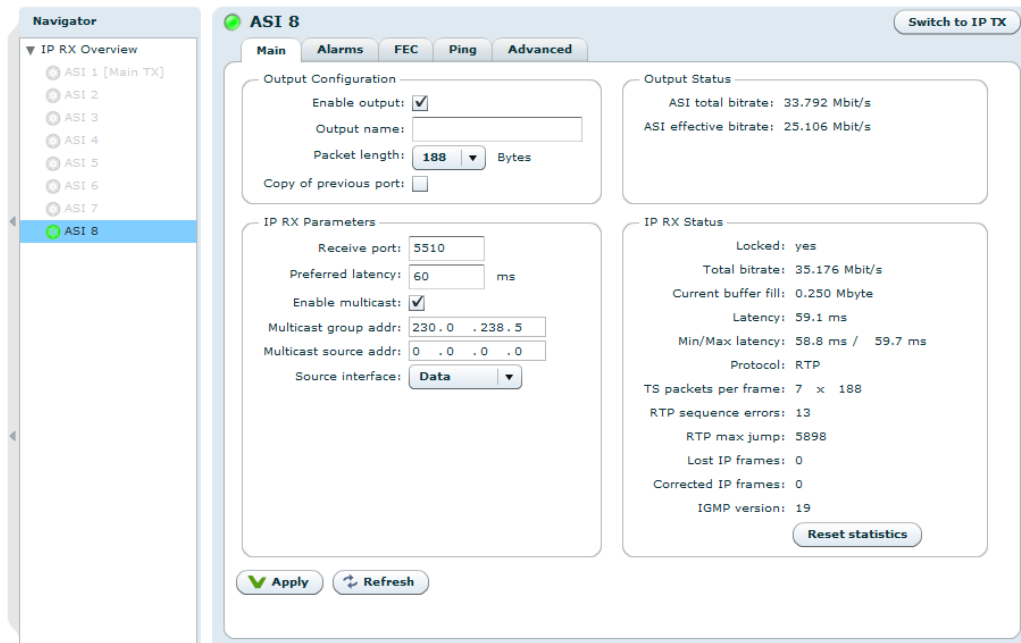


Figure 9.43 IP RX main page

The *Output Configuration* field:

Enable output

Tick this box to enable an output. If this is not ticked no MPEG-2 transport stream data will appear on this ASI output. The output port will be grey in the status view.

Packet length

This lets you configure the ASI output to transmit 188 or 204 byte transport stream packets. If incoming IP frames contain 204 byte MPEG-2 transport stream packets and the packet length is set to 188, the last 16 bytes of the 204 byte packets will be discarded. If incoming IP frames contain 188 byte MPEG-2 transport stream packets and the packet length is set to 204, 16 bytes containing the hexadecimal value FF will be appended to the 188 byte packet.

Output name

Enter a name reference to an ASI output stream.

Copy of previous port

Every even numbered output includes this option. Selecting this option makes the port output exactly the same as the previous port, and no other IP RX setting needs altering.

The *Output Status* field:

ASI total bitrate

This shows the bitrate of the MPEG-2 transport stream on the output including NULL packets.

ASI effective bitrate

This shows the effective bitrate of the MPEG-2 transport stream on the output i.e. bitrate excluding NULL packets.

The *IP RX Parameters* field:**Receive port**

Enter the UDP port number of the channel. The UDP port together with the IP address uniquely identifies the stream to receive. UDP port numbers are in the range 1-65535. This field corresponds to the UDP destination port field of the transmitter.

Preferred latency

Enter the latency in units of milliseconds. This parameter is used together with the detected bitrate to set the size of the receive buffer. The receive buffer is used to remove network jitter, and for intermediate storage to perform forward error correction.

Enable multicast

Click this box to use multicast.

Multicast group addr

This setting is only used when Enable multicast is selected. Enter the multicast IP address of the incoming stream. When enabling multicast mode, the IGMP sub-module will be activated to join the multicast group and respond to membership queries.

Multicast source addr

This setting is applicable when using IGMP version 3 (see [Section 9.7](#)). The device will join a source specific multicast group, informing the router that it is interested in receiving data from a specific transmitter only.

Source interface

The interface used is programmed by selecting from the Source interface pulldown list.

The *IP RX Status* field:**Lock**

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.

Total rate

The total IP data rate received on this channel.

Current buffer fill

Shows the number of megabyte currently in the buffer.

Latency

This parameter reflects the network jitter the unit can currently handle.

Min/Max Latency

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

TS packets per frame

The number of transport stream packets per IP frame in the incoming stream.

RTP sequence errors

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

RTP max jump

Together with Max burst loss length [Section 9.6.3](#) indicates if RTP frame have been re-ordered in the network. The Max jump figure is the largest detected difference in RTP sequence numbers received. If any frames are still missing after receiver re-ordering this is reflected by the Max burst loss length.

Lost IP frames

A counter showing the number of IP frames that is 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.

IGMP version

Shows the IGMP version that is currently active.

Reset statistics

Press this button to reset the counters: RTP sequence errors, Lost IP frames and Corrected IP frames.

9.6.2 Alarms

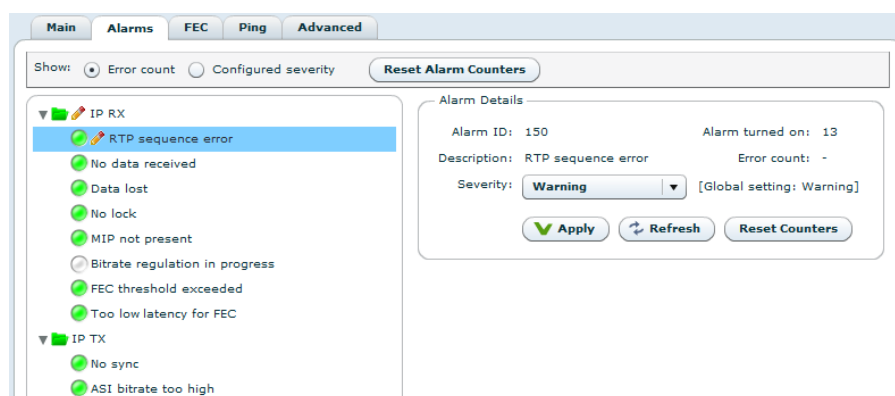


Figure 9.44 The alarms page of an IP receiver

Each individual port has its own alarm configuration that can be used to override the global default setting. A pencil icon appears next to the alarm label when the alarm is overridden. Please see [Section 9.4.2.1](#) for details on alarm configuration.

9.6.3 FEC

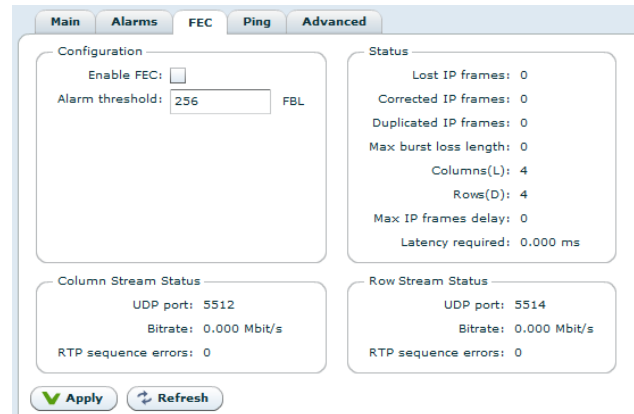


Figure 9.45 The FEC sub-page of an IP receiver

This tab will appear only if the Forward error correction feature has been licensed.

Configuration:

Enable FEC

Tick this box to enable FEC processing of the incoming data. The FEC engine automatically adjusts to the FEC mode used by the transmitter.

Alarm threshold

This parameter controls the frequency of lost frames that shall activate the 'FEC Threshold Exceeded' alarm. The threshold is configured in units of 'frames between losses', causing the alarm to be activated if the number of frames received between two losses falls below the configured number.

The *Status* frame shows the following parameters:

Lost IP frames

This counter shows the number of lost IP frames, i.e. packets that remain uncorrected.

Corrected IP frames

This counter shows the number of IP frames corrected by the FEC engine.

Duplicated IP frames

This counter shows the number of duplicated IP frames received.

Max burst loss length

The maximum number of consecutive packets lost. The number is derived from the RTP sequence number.

Columns (L)

This shows the number of columns in the incoming FEC stream.

Rows (D)

This shows the number of rows in the incoming FEC stream.

Max frames delay

This field shows the maximum number of frames delay measured for the FEC streams.

Latency required

This field is calculated from the Max frames delay field and the current total bitrate to show the minimum delay needed by the FEC engine to fully utilize the incoming FEC streams. When the delay displayed in the Latency field of the IP RX Status sub-page falls below the value of Latency required field the FEC engine may not be able to recover all lost frames that could have been corrected with a larger buffer.

In the *Column* and *Row Stream Status* fields the following parameters are shown:

UDP port

The UDP port of the stream.

Bitrate

The bitrate of the incoming FEC data.

RTP sequence error

This counter shows the RTP sequence errors in the incoming stream caused by lost IP frames or out-of-order packets.

9.6.4 Ping

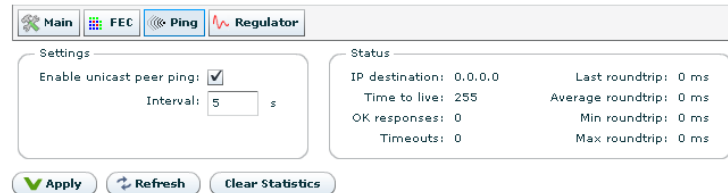


Figure 9.46 The Ping page of an IP receiver

Ping is used to resolve network problems, avoid flooding, or where the receiver or a network component on the way to the receiver times out during MAC address lookup. This feature helps solving such issues by pushing through a ping message regularly. Also makes it possible for the sender identify if there currently is an active recipient.

Enable Unicast Peer Ping

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

Interval

Set the interval in seconds between each Ping.

Active

Indicates if the channel is actively sending Ping requests.

OK responses

Indicates how many valid Ping responses have been received.

Timeouts

Indicates how many of the sent Ping messages timed out before receiving a valid response.

9.6.5 Advanced

The screenshot shows the 'Advanced' tab of a web interface. It is divided into three main sections:

- Regulator Settings:**
 - Lock to MIP bitrate (SFN):
 - Pref. init. rate mode: **PCR** (dropdown)
 - Expected PCR accuracy: ppm
 - Preferred PCR PID:
- Re-sync Conditions:**
 - Bitrate change: MIP error:
 - Latency limits (rel. to pref.):
 - + ms
- ASI Settings:**
 - Mode: **Spread (Max 72Mbit/s)** (dropdown)
 - No lock mode: **Idle** (dropdown)
 - Max bitrate: Mbit/s
 - Pad with NULL packets:

At the bottom, there are 'Apply' and 'Refresh' buttons.

Figure 9.47 Advanced Tab

Under the Advanced tab it is possible to control and inspect the status of the buffer regulator for a port.

Lock to MIP bitrate (SFN)

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

Regulator Settings:

Pref. Init. Rate Mode

This parameter is used to select the preferred algorithm to use to find an initial bitrate for a received data stream.

PCR

The default mode is PCR in which a number of consecutive TS packets on the first PCR PID encountered are used to calculate the bitrate. If no PCR PID is found Coarse mode is automatically 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. If no MIP PID is found, "Coarsemode is automatically used.

COARSE

In this mode, a simple 2 second measurement is used to estimate the bitrate. This

method is sensitive to network jitter and does not give as good results as PCR and MIP modes.

VBR

In this mode, the unit attempts to transmit data at the rate entered in the Max bitrate input. If the incoming rate is lower than this, the unit will either pad with idle bytes (resulting in a VBR output stream) or with NULL packets, according to whether the Pad with NULL packets checkbox is checked. In this mode, no PCR adjustment is performed.

Expected PCR accuracy

The expected clock accuracy on the PCR on the input signal. The configured value affects how far off from the initial bitrate value (measured by PCR) that the buffer regulator is allowed to configure the output bitrate while regulating the latency. The default value (25ppm) should be sufficient for handling of signals from professional DVB equipment and at the same time guaranteeing that the output bitrate is not moved 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 out and avoid buffer over-/under runs.

Preferred PCR PID

When enabled, the IP RX regulator will use the configured PID if it is present. If it is not present it will fall back to the first other PCR PID it finds.

The *Re-sync Conditions:* field allows setting the conditions when to perform re-synchronisation of the output transport stream. Three boxes may be ticked:

Bitrate change

Re-sync occurs if the unit detects a change in the bitrate.

MIP error

Re-sync occurs if the clock recovery based on MIP detection fails.

Latency limits

Re-sync occurs if the latency exceeds the preferred value by the time values entered in the boxes provided.

ASI Settings:

Mode

Configure the unit to transmit ASI data using burst or spread mode. Note that spread mode only works for bitrates up to 72 Mbit/s. If you choose spread mode and transmit a higher bitrate, the signal will become a burst/spread hybrid.

No lock mode

This parameter lets you choose what the unit should transmit on the ASI port when it is unable to lock to the incoming signal. Options are to send idle bytes or to turn the port completely off.

Max bitrate

If VBR rate mode is chosen in the Pref. init. rate mode pull-down Max Bitrate tells the unit at what bitrate it should attempt to transmit.

Pad with NULL packets

Checking this means that the unit, when in VBR rate mode, will pad the output stream with NULL packets to achieve Max bitrate.

The *Regulator Status* field:

Init. Rate Mode

This parameter shows the initial bitrate mode that was used at last re-sync. If PCR mode was selected and this parameter shows Coarse mode the device has not been able to find a valid PCR PID on the signal.

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 has been found, the regulator enters the Rate Estimation state, where the signal is analysed to check if a better estimation of the bitrate can be made. 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.

Selected PCR PID

The PID of the transport stream containing PCR time stamps used for bitrate estimation.

Initial bitrate

Displays the exact initial bitrate found.

Current bitrate

This parameter shows the exact bitrate currently played out on the ASI port.

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 is highly inaccurate and depends on IP network jitter. After a few minutes of operation the value gets more accurate, and can be compared to the current bitrate to see how far off the bitrate target the regulator is operating.

Regulator output

Regulator output expressed in ppm offset from the initial bitrate.

Regulator operation range

Operation range for the regulator expressed in ppm offset from the initial bitrate. The operation range is affected by the Expected PCR accuracy setting and is typically configured slightly wider to give headroom for buffer regulation.

Number of re-synchs

Number of times the buffer has been re-synchronised.

Channel uptime

Time since channel was last re-synchronised.

9.7 Streams

Figure 9.48 shows the Streams page of a unit configured for bi-directional operation of the Ethernet interface. The purpose of this page is to provide network related information.

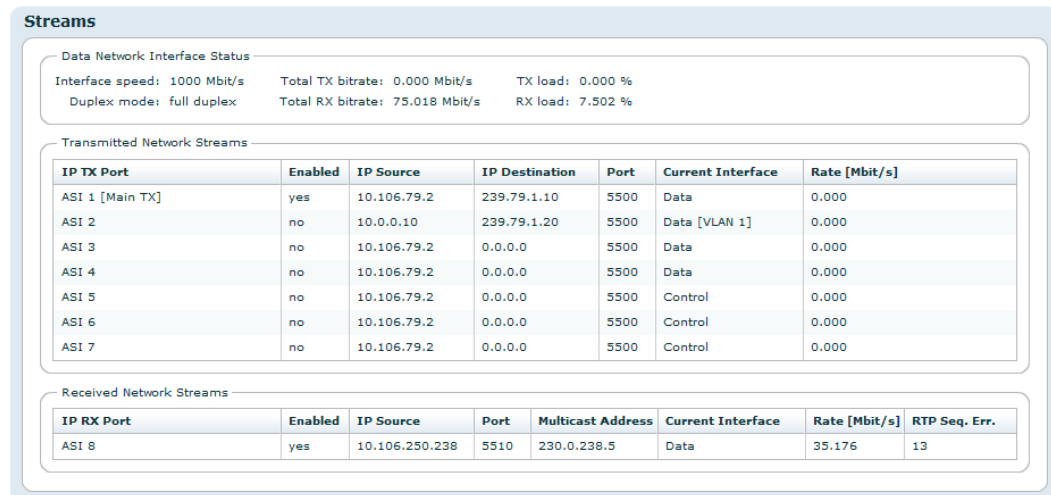


Figure 9.48 Streams page for unit in IP TX mode

The *Data network interface status* field:

Interface speed

Shows the rate in Mbit/s of the data network interface.

Duplex mode

Full duplex or half duplex dependent on the configuration of the port.

Total RX bitrate

The total bitrate of IP frames received over the network data interface.

RX load

The percentage of the total interface speed used by the IP frames received over the network data interface.

Total TX bitrate

The total bitrate of IP frames sent over the network data interface.

TX load

The percentage of the total interface speed used by the IP frames sent over the network data interface.

The *Transmitted Network Streams* table:

This table lists all ASI inputs providing transport streams that shall be transmitted over the network. For each individual ASI port the table shows the name of the port, if the port is enabled (Yes/No), the IP destination or source address, the UDP port number, the current interface and the total bitrate of the interface (in Mbit/s).

The *Received Network Streams* table:

This table lists all ASI outputs delivering transport streams that have been received over the network. For each individual ASI port the table shows the name of the port, if the port is enabled (Yes/No), the IP source address, the UDP port number, the multicast address (if appropriate), the current interface, the total bitrate of the interface (in Mbit/s) and a counter showing RTP sequence errors.

9.8 Redundancy

9.8.1 Redundancy Controller

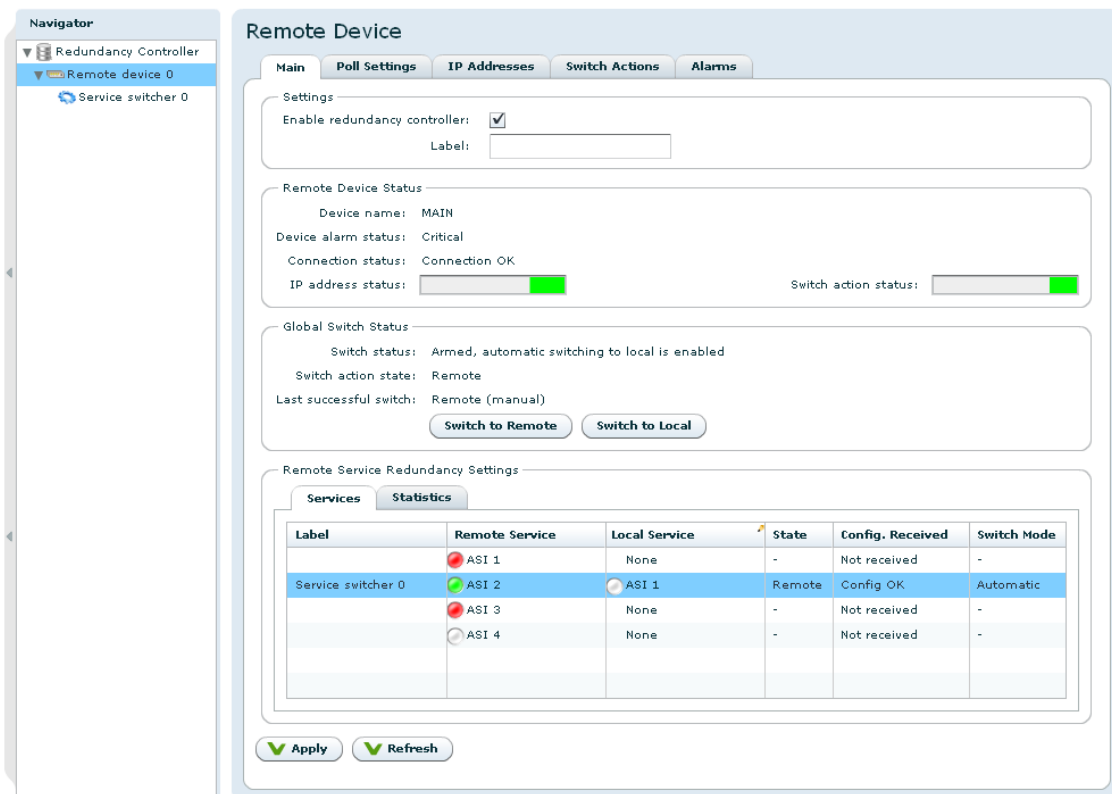


Figure 9.49 The user interface

Figure 9.49 shows the user interface. The page is divided into four sections: Settings, Remote Device Status, Global Switch Status and Remote Service Redundancy Settings.

Settings

allows the user to label this specific redundancy controller and also to enable or disable it.

Remote Device Status

shows the remote device name and alarm status. It also shows the status of the connection

to the remote device. Additionally two status bars show the status of the last poll towards each configured IP Address and Switch action. The status bar is divided into a number of parts according to the number of IP addresses or Switch actions. For instance if three IP addresses are configured and their status is no contact, disabled and contact ok, then the bar is divided into three equally sized parts with the colours red, gray and green.

Global Switch Status

shows the status of the global redundancy controller. The information shown in this section changes when a global switch is performed, either by an automatic switch to local or a manual switch. The Switch Action State attribute reflects the combined state of the configured switch actions. If all switch actions are configured to remote value the Switch Action State is Remote. If all switch actions are configured to local value the Switch Action State is Local. Otherwise the Switch Action State is Unknown.

Remote Service Redundancy Settings

This section shows a table of the remote and local services. For each remote service the user can configure a local replacement by using the select box on each row in the Local service column. When a local replacement is configured a service switcher is added to the redundancy controller. The service switcher parameters state, Configuration received and mode is shown in the table. Refer to [Section 9.8.2](#) for detailed information on service switchers.

9.8.1.1 Global redundancy controller switching

A global switch can be performed either manually or automatically. Figures 9.50 and 9.51 show redundancy controller state diagrams when switching to local or remote services respectively.

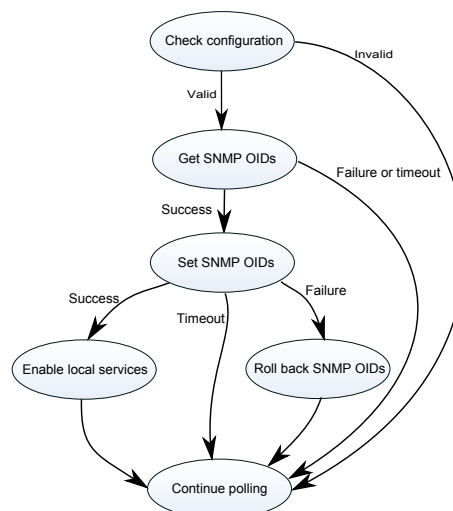


Figure 9.50 The actions performed when the redundancy controller loses contact with the remote device.

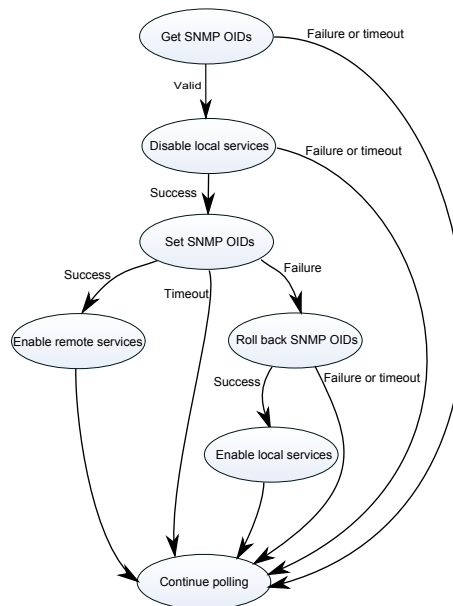


Figure 9.51 The actions performed when a manual redundancy controller switch to remote services is forced.

9.8.1.2 Poll settings

The remote device is polled through a set of IP addresses. Loss of contact towards any of these addresses causes an alarm.

During normal operation the redundancy controller alternates between two states, poll and sleep. When entering the poll state a series of polls are made towards the configured IP addresses and SNMP OIDs. When all poll responses are received the redundancy controller switches to sleep state. If not all responses are received before the poll state timeout the remaining IP addresses and OIDs will be flagged as no contact before switching to sleep. The redundancy controller will wait a number of seconds in sleep before doing a new poll. The sleep state timeout is configurable for both link up (contact with remote) and link down (no contact with remote) scenarios.

If an authorization error towards any address occurs the redundancy controller cannot resolve the state of the remote device. In this case the redundancy controller assumes the remote device is healthy and will not switch to local.

All IP addresses should be to the same device, otherwise a configuration alarm will be raised.

If no contact can be made to any of the IP addresses configured for a device, each service switcher will be informed that the remote device is down. In addition, a set of SNMP actions will be performed.

Figure 9.52 shows the poll settings of the redundancy controller. The timeouts used in the sleep and poll states are configured here. The username and password to use when logging in on the remote device is also configurable.

Figure 9.52 The poll settings page

9.8.1.3 Remote device IP addresses

Enable	IP Address	Timeout [s]	Polls OK	Polls Fa...	RTT [s]	Status	Device
<input checked="" type="checkbox"/>	12.0.0.13	8	1771	1	0.12	Contact ok	TV0401.01289

Figure 9.53 The IP Addresses to the remote (main) device

Figure 9.53 shows the IP address configuration. The individual poll timeout per address should not be higher than the poll state timeout.

9.8.1.4 SNMP switch actions

#	Enabled	IP Address	Poll OID	Read Value	State	RTT [s]	Polls OK	Polls Failed	Status
0	yes	12.0.0.4	1.3.6.1.2.1.2.2.1.7.15	1	Remote	0.79	1874	0	Ok

SNMP Action #0

Switch Action Settings:

Enable:

IP address: 12.0.0.4

UDP port: 161

Value to set when switching to remote: 1

Value to set when switching to local: 2

OID type: Integer32

Set OID: 1.3.6.1.2.1.2.2.1.7.15

Poll mode: GET

Other read OID: 1.3.6.1

Read community string: public

Write community string: private

Figure 9.54 The SNMP switch actions

Figure 9.54 shows the SNMP switch action configuration. Note that these OIDs are only set after a loss of contact with the remote device or when manually switching the entire redundancy controller between remote and local services, i.e. during a global switch. The OIDs are not set when switching a single service switcher between remote and local.

The SNMP OIDs are polled during normal operation to discover potential problems as soon as possible. Three modes are available for this poll: set oid, get oid or get other oid request.

The set oid sets the oid to remote value if the link to the remote device is up and local value if the link is down. The get oid mode just reads the oid. The get other oid reads the Other read OID.

9.8.2 Service switchers

A service switcher is assigned to each pair of remote and local services. As long as the Redundancy Controller has contact with the remote device, the service switcher will acquire the current status and configuration.

The service switcher does not perform a switchover unless it has received a valid configuration. Switching from the local to the remote service is not performed automatically, only manually.

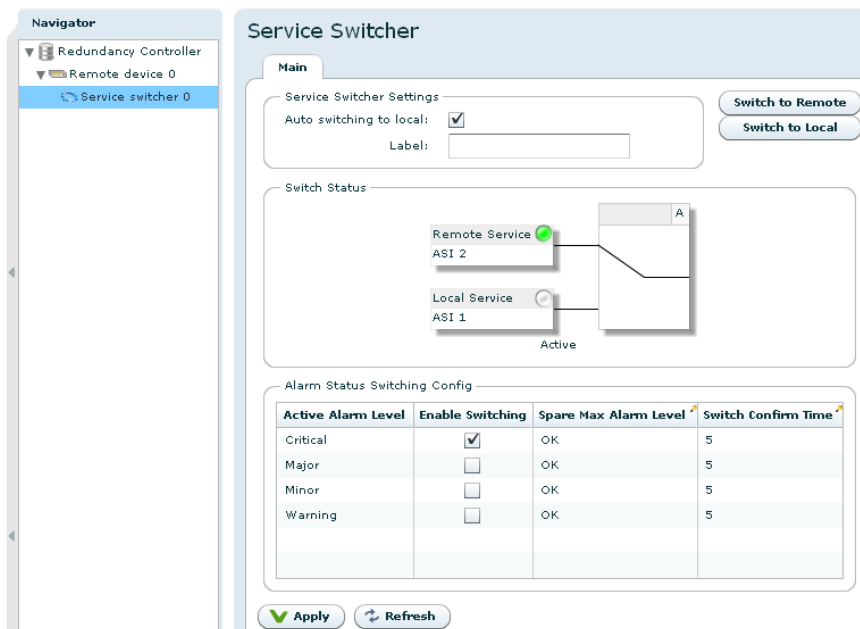


Figure 9.55 The service switcher configuration page

The service switcher page shows the current state of this service pair. The label and the alarm status is shown in the graphical representation in addition to the current switch state.

The service switcher controller only relates to alarm levels for the two corresponding services. It is up to the user to configure appropriate alarm levels for each of the alarms a service is able to generate. The switching criteria are configured as follows:

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

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

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

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

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

In “auto” state, the switch controller is “armed” and continuously listens to change in the alarm status for each service. For each change event, the controller evaluates the levels and checks if the switching criteria is met. If the answer is “yes”, the controller jumps to a `wait_confirm` state to actually confirm that the switch criteria still is met after the configured time. If the criteria is still met, the controller performs a switch. If the criteria is no longer met, the controller does no switching and jumps back to the auto state.

10 SNMP

The product supports SNMP – Simple Network Management Protocol – for remote control and supervision. SNMP uses an extensible design, where management information bases (MIBs) describe the structure of the management data of a device subsystem. The primary purpose of SNMP is to export alarm and status information, but a range of MIBs related to configuration settings are also supported.

10.1 SNMP agent characteristics

The SNMP agent supports the SNMPv2c (Community based SNMPv2) protocol. All custom MIBs are written in SMIV2 format. The SNMP agent will accept both SNMPv1 and SNMPv2 messages. The SNMP agent uses the normal UDP sockets for communication and listens for requests at UDP port 161.

Both legacy SNMPv1 traps and SNMPv2 notifications are supported. It is however recommended to use the new SNMPv2 notification types for new deployments.

10.2 MIB naming conventions

All custom MIB files start with the prefix VIGW. MIBs that defines data structures that are not connected to one specific product start with VIGW-PLAT. Most MIBs are of generic type and therefore starts with this prefix.

Some MIB-files are very custom and corresponds to a specific product only. These MIBs start with the prefix VIGW-PROD.

10.3 MIB overview

This section describes the different MIBs. Detailed description of MIBs is included later on in this document.

10.3.1 Supported standard MIBs

RFC1213-MIB

MIB-II according to RFC1213.

10.3.2 Custom MIBs

VIGW-TC-MIB

Describes common textual conventions (data types etc.) used throughout the entire MIB set. For example, definition of alarm status numbers are defined in this MIB.

VIGW-BASE-MIB

Defines the top level MIB structure including the enterprise specific root node for device control (1.3.6.1.4.1.22909).

VIGW-UNIT-MIB

This is a generic MIB module that defines parameters supported by all products. It is the main source for alarm and status related information. The following objects are examples of contents in this MIB:

- Top level alarm status
- Table of current alarms
- History of last transmitted TRAP messages
- Trap destination list
- Force reset of the unit
- TRAP/NOTIFICATION definitions
- Other, general product information:
 - Serial number
 - SW version



Note: When setting values in the unitAddressTable it is important to send all values for one interface in the same request. This is to prevent the unit from entering an undefined intermediate state.

VIGW-PLAT-TS-MIB

This MIB contains Transport Stream related information for each of the transport stream inputs. It is supported by transport stream related products that are able to analyse incoming transport streams. For each input transport stream, the following information is available:

- Transport stream sync status and total/effective bitrate.
- Present PIDs with information about bit rates and CC errors.
- Present services with information about service name and service ID.

VIGW-PLAT-TSOUT-MIB

This MIB is supported by products that can generate an outgoing transport stream. Parameters include:

- Control of output bitrate and other ASI parameters (spread/burst mode).
- Control of MIP insertion (if enabled in the product)
 - OFDM modulation parameters
 - Enable/disable of MIP insertion
- Control of PSI/SI table playout

VIGW-PLAT-SWITCH-MIB

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

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

VIGW-PLAT-IPTRANSPORT-MIB

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

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

VIGW-PLAT-VIDEO-MIB

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

Examples of included information are:

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

10.4 SNMP related configuration settings

The SNMP related configuration parameters are located on the Device Info/SNMP settings page in the GUI.

10.4.1 Community strings

The community strings are used to provide simple password protection for SNMP read and write requests. The strings can be configured from the GUI. It is also possible to configure the community strings to be used for trap messages.

10.4.2 Trap destination table

The Trap Destination table lets the user configure the external entities that should receive SNMP traps from the device. The table is both accessible via VIGW-UNIT-MIB and the product GUI (Device Info/SNMP settings). A maximum of 8 different destinations are supported.

10.4.3 Trap configuration

All supported traps are currently defined in the VIGW-UNIT-MIB. Via the GUI you can control the trap forwarding. For detailed information about each trap and the corresponding variable bindings, please see [Section 10.5](#).

Trap version

This parameter controls the TRAPs that will be sent from the device in case of alarm conditions.

SNMPv1 (Legacy)

If this option is selected, the unit will send the traps located under the `vigwLegacyTraps` MIB node. These traps are included mostly for historical reasons and it is not recommended to use these for new deployments.

SNMPv2

This is the recommended setting. The traps defined under the node `unitNotifications` will be used while the traps under the node `vigwLegacyTraps` will be disabled.

Status change traps

If enabled, the unit will transmit `unitAlarmStatusChanged` traps whenever the top level alarm status is changed for the unit.

Alarm event forwarding

This setting controls how internal alarm event will be forwarded as TRAP messages. Adjust this value if you want to control the number of traps sent from the unit. The settings are only used when SNMPv2 is selected as TRAP version. The settings are:

Disabled

No specific event traps are transmitted when alarms are raised or cleared. (The `unitAlarmStatusChanged` trap may however be transmitted).

Basic

The device forwards alarms as traps on a basic level. No information about `subid3` will be transmitted.

Detailed

The device forwards alarms as traps. If there are sub-entries that are using the `subid3` value, each sub.entry will be transmitted in separate trap messages.

10.5 Alarm/status related SNMP TRAPs

All TRAP messages are defined in VIGW-UNIT-MIB. This section describes each trap message.

10.5.1 The main trap messages

The main (SNMPv2) trap messages are defined under the `unitNotifications` node in `VIGW-UNIT-MIB`. The messages are described briefly in [Table 10.1](#).

Table 10.1 List of SNMPv2 traps

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

10.5.2 Severity indications

All alarm event traps (i.e. all traps defined in [Table 10.1](#) except `unitAlarmStatusChanged`) contain a severity field which is encoded according to the definition below:

Severity	Description
1	Cleared
2	Indeterminate
3	Warning
4	Minor
5	Major
6	Critical

10.5.3 Alarm event fields

A description of the fields in the alarm event traps is presented in [Table 10.2](#). Most of the fields are entries from the `unitEventHistoryTable`. The instance identifier for each variable binding corresponds to the index in this table. This index is of kind `CircularLog` and will wrap around at 2^{32} .

Table 10.2 Variables in SNMPv2 traps and their meanings

Field	Description
<code>unitEventSeverity</code>	This field indicates the severity of the alarm, 2-6. 1 will never be used, as this condition is indicated by transmitting a <code>unitAlarmCleared</code> message.
<code>unitEventAlarmType</code>	This is an integer that describes the alarm type. Please refer to alarm documentation for description. From this type, one can extract the actual meaning of the <code>subid1</code> and <code>subid2</code> values in the message.
<code>unitEventAlarmId</code>	A unique identifier for this alarm type. Refer to alarm documentation in the user manual for values.
<code>unitEventAlarmName</code>	A fixed name corresponding to the alarm id.
<code>unitEventRefNumber</code>	This field is provided to easily match asserted/cleared alarms. In the cleared alarm it is set to the same number as in the asserted alarm.
<code>unitEventSubId1</code>	The first subidentifier to identify the source of the alarm. For products with single base boards it is typically set to a fixed value (0 or 1) and can be ignored.
<code>unitEventSubId2</code>	This field's purpose is dependent on the alarm type (alarm id). For some alarms it is not used and set to zero. For other alarms, it may e.g. indicate the channel/port number for the entity that generated the alarm.
<code>unitEventSubId3</code>	This field provide an even more detailed description of the alarm source. This field is only present in the "detailed" type of trap messages (<code>unitDetailedAlarmAsserted</code> , <code>unitDetailedAlarmEvent</code>). It's usage is dependent on the alarm ID. For example, in transport stream related alarms, <code>subid3</code> is used to indicate the PID value that caused the alarm.
<code>unitEventSourceText</code>	A textual description of the source of the alarm. This is typically a textual description of the <code>subid1</code> and <code>subid2</code> fields. For example, for transport stream related alarms, the text indicates the name (with label) of the port that generated the alarm.
<code>unitEventSubId3Label1</code>	This field is fixed and indicates the label (meaning) of the <code>subid3</code> field, contained in the <code>unitEventSubId3</code> variable. It is intended to make it easy to log the alarm.
<code>unitEventDetails</code>	This is a generic text string that contains more details related to the alarm event. It's usage and content is dependent on the alarm ID.
<code>unitAlarmStatus</code>	This variable contains the new, top level alarm status of the unit <i>after</i> the condition leading to this trap message. It may be used to quickly update the top level status for the device after receiving the trap message.

10.5.4 Matching of on/off traps

As mentioned previously, a `unitAlarmCleared` message is sent after a `unitAlarmAsserted` message and a `unitDetailedAlarmCleared` message is sent after a `unitDetailedAlarmAsserted` message.

The “cleared” event contains exactly the same identifiers as the “asserted” trap. This includes the alarm ID, `subid1`, `subid2` and `subid3` fields. This set of four identifiers uniquely identifies the source of an alarm.

A more easy way to match the traps is by using the `unitEventRefNumber` field. This is a simple integer that is the same in an “asserted” trap and in a “clear” trap.

10.5.5 Legacy trap messages



Note: The information in this section relates to trap definitions that are marked as deprecated in VIGW-UNIT-MIB. They are included for backwards compatibility with earlier product versions and should not be used for new deployments.

The legacy traps are defined under the `vigwLegacyTraps` node. Transmission of these traps is specified by selecting “SNMPv1 (Legacy)” for the trap version field. The format of these traps follow the SNMPv1 trap format.

In contrast to the SNMPv2 alarm messages, the SNMPv1 messages has its severity implicitly encoded in the trap type.

The trap messages are defined in [Table 10.3](#).

Table 10.3 List of legacy (SNMPv1) traps

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

All these trap messages contain variable bindings from the `unitTrapHistoryTable`. This table is filled up with historical trap messages, only when SNMPv1 mode is selected.

The fields in these traps are fetched from the `unitAlarmTrapHistoryTable`. The meaning of these fields correspond to the fields in the `unitEventHistoryTable` for SNMPv2 traps and are not described in more detail here.

11 Preventive Maintenance and Fault-finding

This chapter provides the schedules and instructions, where applicable, for routine inspection, cleaning and maintenance of the TVG420, 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 TVG420 with a soft cloth dampened with a mixture of mild detergent and water.
- Make sure that the unit is completely dry before reconnecting it to a power source.

11.1.3 Servicing



Warning: Do not attempt to service this product as opening or removing covers may expose dangerous voltages or other hazards. Refer all servicing to service personnel who have been authorised by T-VIPS.

In case of equipment failure unplug the unit from the power and refer servicing to qualified personnel with information of the failure conditions:

- The power supply cord or plug is damaged
- Liquid has been spilled or objects have fallen into the product
- Product has been exposed to rain or water
- Product does not operate normally when following the operating instructions
- Product has been dropped or has been damaged
- Product exhibits a distinct change in performance

11.1.4 Warranty

The TVG420 is covered by standard T-VIPS warranty service for a period of 24 months following the date of delivery.

The warranty covers the following:

- All defects in material and workmanship (hardware only) under normal use and service.
- All parts and labour charges
- Return of the repaired item to the customer, postage paid.
- Customer assistance through T-VIPS Customer Service Help Line

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

11.2 Fault-finding

The objective of this chapter is to provide sufficient information to enable the operator to rectify apparent faults or else to identify where the apparent fault might be. It is assumed that fault-finding has already been performed at a system level, and that the fault cannot be attributed to other system components.

This manual does not provide any maintenance information or procedures which would require removal of covers.



Warning: Do not remove the covers of this equipment. Hazardous voltages are present within this equipment and may be exposed if the covers are removed. Only T-VIPS trained and approved service engineers are permitted to service this equipment.



Caution: Unauthorised maintenance or the use of non-approved replacement parts may affect the equipment specification and will invalidate any warranties.

If the following information fails to clear the abnormal condition, please contact your local reseller or T-VIPS customer care.

11.2.1 Preliminary checks

Always investigate the failure symptoms fully, prior to taking remedial action. The operator should not remove the cover of the equipment to carry out the fault diagnosis. The following fault-finding tasks can be carried out:

- Check that the PSU LED is lit. If this is not lit, replace external equipment, power source and cables by substitution to check that these are not defect.

- Confirm that the equipment hardware configuration is suitable for the purpose and that the unit has been correctly connected.
- Confirm that inappropriate operator action is not causing the problem, and that the equipment software set-up is capable of performing the required functionality.
- Check that the fans are unobstructed and working correctly.

When the fault condition has been fully investigated, and the symptoms are identified, proceed to fault-finding according to the observed symptoms. If the fault persists, and cannot be rectified using the instructions given in this manual, contact T-VIPS Customer Support. Switch off the equipment if it becomes unusable, or to protect it from further damage.

11.2.2 PSU LED not lit / power supply problem

Power fault-finding

1. Check the Power LED.
 - Is the LED unlit, but the unit still working properly?
 - Yes
The Power LED itself is probably at fault - Call a Service Engineer.
 - No
Proceed to next step
2. Check the Power Source.
 - Connect a piece of equipment known to work to the power source outlet. Does it work?
 - Yes
The problem lies within the TVG420 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 TVG420. 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 TVG420 to T-VIPS, contact your local T-VIPS reseller or T-VIPS directly for additional advice.

1. Write the following information on a tag and attach it to the TVG420.
 - Name and address of the owner
 - Model number
 - Serial number
 - Description of service required or failure indication.
2. Package the TVG420.
 - The original shipping containers or other adequate packing containers must be used.
3. Seal the shipping container securely, and mark it FRAGILE.

Appendix A 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

A.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.

A.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.

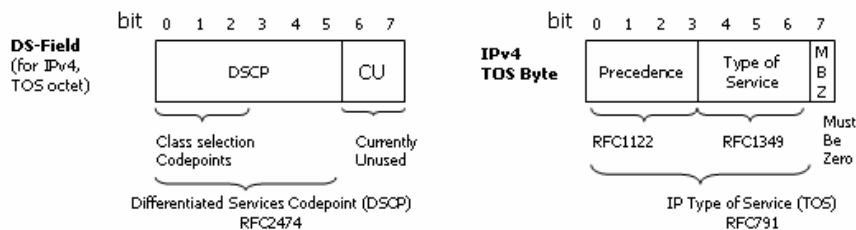


Figure A.1 Differentiated services (Diff-serve) and precedence bits (TOS)

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.

A.2.1 TVG420 configuration

The number entered into the Type of service (TOS) field in TVG420 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.

A.3 Layer 2 priority

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

A.3.1 TVG420 configuration

The COS priority is entered in the VLAN configuration page in the TVG420 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 B 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, horizontally and vertically, giving clearer and more detailed TV pictures.

HTTP

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

ICMP

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

IGMP

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

JPEG2000

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

Meta-data

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

MPEG-2

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

MPLS

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

MPTS

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

Multicast

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

MXF

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

NMS

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

PCR

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

PID

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

PSI/SI

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

QAM

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

QoS

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

QPSK

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

RIP2

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

RSVP

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

RTP

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

SD-SDI

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

SDI

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

SDP

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

SDTI

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

SDTV

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

SFP

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

SIP

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

SNDU

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

SNMP

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

SNTP

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

SPTS

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

TCP

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

TCP/IP

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

ToS

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

Transport Stream (TS)

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

UDP

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

Unicast

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

VLAN

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

Watermarking

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

XML

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

Appendix C Alarms

The TVG420 indicates alarm or failure status to the user in four ways:

- WEB interface
- Alarm LED on the front and on the rear
- SNMP trap messages to Network Management System
- Alarm relay

The user can define the severity level of the different alarm events. There are five levels, and each level is also indicated by a colour on the alarm severity indicator:

Table C.1 Alarm severity levels

Severity	Level	Colour
Notification	2	Blue
Warning	3	Yellow
Minor	4	Amber
Major	5	Orange
Critical	6	Red

In addition it is possible to set an alarm to filtered, so that there will be no alarm events generated for this alarm.

The WEB interface gives the most detailed alarm information as all active alarms and warnings are listed with time of occurrence

The unit sends an SNMP trap message to all registered trap receivers when an alarm condition arises. A critical alarm will have severity level 6 and a Notification will have severity level 2. When the alarm is cleared, a new message is sent to indicate that the alarm condition is cleared.

Finally, the red alarm LED will be lit when an unmasked critical alarm condition arises. At the same time the alarm relay will be set to alarm state.

Table C.3 shows the possible alarms that can be signalled by the TVG420. For each alarm type, essential information is presented. The different fields are described in **Table C.2**.

Table C.2 Fields in the alarm description table

Field	Description
Alarm ID	Unique identifier (number) for this alarm. There are no duplicates in the table, e.g. a specific alarm number always maps to a specific alarm.
Text	A short text describing the alarm
Description	A longer text describing the cause of the alarm
Def. severity	The default severity of the alarm
Type	Alarms are grouped together into different <i>types</i> . This field contains a textual description of the type.
Type ID	Each alarm type has a corresponding number (ID).
Clear event	Set to Yes if an “off/cleared” alarm is expected after an “asserted” alarm. In most cases the value is Yes. For “stateless” alarms, e.g. the event that a user has logged into the system, no explicit clear events are expected.
Subid2	This field is present if the Subid2 value of the alarm type is used. The text in the table describes the usage of the Subid2 value.
Subid3	This field is present if the Subid3 value of the alarm type is used. The text in the table describes the usage of the Subid3 value.

Table C.3.a Alarms

Alarm ID	Text	Details
100	No sync	<p><i>Description:</i> No valid ASI input stream detected.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Port</p> <p><i>Type ID:</i> 9</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
101	ASI bitrate too high	<p><i>Description:</i> The ASI input bitrate has exceeded the configured maximum value.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Port</p> <p><i>Type ID:</i> 9</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
106	Unable to transmit	<p><i>Description:</i> Channel not able to transmit any data, or only part of the data is transmitted.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> IP Output</p> <p><i>Type ID:</i> 24</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP output channel identifier</p> <p><i>Subid3:</i> Dest</p>
121	Bitrate regulation in progress	<p><i>Description:</i> The regulation algorithm is estimating the incoming bitrate to compensate for the difference in PCR clocks on the source encoder and the IP receiver. While this alarm is active, the output bitrate may be tuned beyond the limits of the ASI specifications.</p> <p><i>Def. severity:</i> Filtered</p> <p><i>Type:</i> Port</p> <p><i>Type ID:</i> 9</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
130	Ethernet link down	<p><i>Description:</i> No link on Ethernet layer.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Ethernet port</p> <p><i>Type ID:</i> 17</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>

Table C.3.b Alarms

Alarm ID	Text	Details
131	Ethernet output overflow	<p><i>Description:</i> The total bitrate of the streams to transmit is too high compared to the available ethernet bitrate.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Ethernet port</p> <p><i>Type ID:</i> 17</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>
133	Generic SFP alarm	<p><i>Description:</i> Generic SFP alarm for Mipot and SFF-8472 based modules.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Ethernet port</p> <p><i>Type ID:</i> 17</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>
140	IP address unresolved	<p><i>Description:</i> IP address is not resolved into physical MAC address.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> IP Output</p> <p><i>Type ID:</i> 24</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP output channel identifier</p> <p><i>Subid3:</i> Dest</p>
150	RTP sequence error	<p><i>Description:</i> Analysis of the sequence number of the RTP layer indicates that IP frames have been lost or that they have been received out of order.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> IP Input</p> <p><i>Type ID:</i> 23</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
151	No data received	<p><i>Description:</i> No data received on Ethernet input for stream.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> IP Input</p> <p><i>Type ID:</i> 23</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>

Table C.3.c Alarms

Alarm ID	Text	Details
152	FEC threshold exceeded	<p><i>Description:</i> The frequency of lost frames is higher than the configured value. Threshold values are configured per stream.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> Port</p> <p><i>Type ID:</i> 9</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>
153	Ethernet input overflow	<p><i>Description:</i> The total bitrate of the IP input streams is too high.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Ethernet port</p> <p><i>Type ID:</i> 17</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Ethernet port ID</p>
154	Data lost	<p><i>Description:</i> The data stream received for a channel is incomplete, and if running FEC, the FEC engine is not able to recover all the lost frames.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> IP Input</p> <p><i>Type ID:</i> 23</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
155	No lock	<p><i>Description:</i> The incoming packet stream is absent or incompatible with the expected format.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> IP Input</p> <p><i>Type ID:</i> 23</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
156	MIP not present	<p><i>Description:</i> No MIP frames are received.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Port</p> <p><i>Type ID:</i> 9</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>

Table C.3.d Alarms

Alarm ID	Text	Details
157	Too low latency for FEC	<p><i>Description:</i> The preferred latency is set lower than the latency required to fully utilize the current FEC.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> IP Input</p> <p><i>Type ID:</i> 23</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> IP input channel identifier</p>
160	SNTP server unreachable	<p><i>Description:</i> The unit is not receiving answers from the SNTP server.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
161	Too high temperature	<p><i>Description:</i> Internal temperature of unit is too high.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
162	Defective fan	<p><i>Description:</i> One or more fans are not spinning.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
163	Time reference unreachable	<p><i>Description:</i> No selected timesources are OK.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
164	Illegal board configuration detected	<p><i>Description:</i> A board configuration that is incompatible with this product has been detected.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
165	Time source not OK	<p><i>Description:</i> One or more time sources are not OK.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>

Table C.3.e Alarms

Alarm ID	Text	Details
166	Time source switch	<p><i>Description:</i> Device started using a new time source.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> No</p>
167	Time adjusted	<p><i>Description:</i> The real time clock of the device was adjusted significantly.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> No</p>
168	Power failed	<p><i>Description:</i> One or more power supplies have failed, or are out of regulation.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Power supply ID</p>
169	Virtual alarm relay activated	<p><i>Description:</i> A virtual alarm relay has been activated.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid3:</i> Relay ID</p>
200	No GPS 1PPS ref. signal	<p><i>Description:</i> The 1PPS reference signal is lost (The regulator has however not lost synchronization).</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
201	Lost GPS 1PPS sync.	<p><i>Description:</i> The clock synchronization mechanism has been resynchronized due to too large phase error.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>

Table C.3.f Alarms

Alarm ID	Text	Details
210	Emergency switch active	<i>Description:</i> A user has activated the remote emergency switch. <i>Def. severity:</i> Notification <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> Yes
211	Emergency switch unreachable	<i>Description:</i> The device is not able to communicate with the remote emergency switch. <i>Def. severity:</i> Warning <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> Yes
212	Emergency switch rule config error	<i>Description:</i> An error has been detected in the configuration of the emergency switch. <i>Def. severity:</i> Warning <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> Yes
501	User logged in	<i>Description:</i> This event is generated when a user logs on to the system. <i>Def. severity:</i> Notification <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> No
502	User logged out	<i>Description:</i> This event is generated when a user logs out from the system. <i>Def. severity:</i> Notification <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> No
503	System started	<i>Description:</i> The system has booted. <i>Def. severity:</i> Notification <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> No
505	Config changed	<i>Description:</i> A modification has been made to the configuration of the device. <i>Def. severity:</i> Notification <i>Type:</i> System <i>Type ID:</i> 13 <i>Clear event:</i> No

Table C.3.g Alarms

Alarm ID	Text	Details
517	Alarm log cleared	<p><i>Description:</i> Alarm log was cleared, user in details</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> No</p>
518	System is starting up	<p><i>Description:</i> This alarm is set when the system is starting. Once booted correctly, the alarm is cleared.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
519	Forced reset initiated	<p><i>Description:</i> A reset of the device was forced by the operator.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> No</p>
520	SW loading in progress	<p><i>Description:</i> Loading of an embedded SW image is in progress</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
521	New SW pending	<p><i>Description:</i> A SW image has been successfully loaded, but manual reboot is needed for SW to be activated.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
524	Simultaneous users	<p><i>Description:</i> Multiple users with administrator or operator access level are logged in.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> System</p> <p><i>Type ID:</i> 13</p> <p><i>Clear event:</i> Yes</p>
601	No contact	<p><i>Description:</i> The redundancy controller could not contact the remote unit.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>

Table C.3.h Alarms

Alarm ID	Text	Details
602	Authorization error	<p><i>Description:</i> The redundancy controller got response from the remote unit but authorization failed.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
603	Switchover performed	<p><i>Description:</i> The redundancy controller has performed a switchover.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
604	Switchover failed	<p><i>Description:</i> The redundancy controller failed to perform a switchover.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
605	Rollback failed	<p><i>Description:</i> The redundancy controller failed to perform a switchover and the rollback failed as well.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> No</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
606	SNMP error	<p><i>Description:</i> This alarm is triggered if a redundancy controller SNMP request fails.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
607	Illegal configuration	<p><i>Description:</i> This alarm is triggered if the redundancy controller configuration is invalid.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>

Table C.3.i Alarms

Alarm ID	Text	Details
608	Switchover performed	<p><i>Description:</i> A switchover has been performed by the redundancy controller service switcher.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
609	Automatic switchover is disabled	<p><i>Description:</i> The redundancy controller service switcher is in manual mode, no automatic switchover will be performed.</p> <p><i>Def. severity:</i> Warning</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
610	Local service alarm level too high	<p><i>Description:</i> The redundancy controller alarm level switching criteria are met, but the local service has a too high alarm level.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
611	Illegal configuration	<p><i>Description:</i> The redundancy controller service switcher has either never received a configuration from the remote service or received an invalid configuration.</p> <p><i>Def. severity:</i> Notification</p> <p><i>Type:</i> Redundancy</p> <p><i>Type ID:</i> 18</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Redundancy Controller ID</p>
1500	Input overflow	<p><i>Description:</i> The total bit rate of the input stream is too high.</p> <p><i>Def. severity:</i> Critical</p> <p><i>Type:</i> Port</p> <p><i>Type ID:</i> 9</p> <p><i>Clear event:</i> Yes</p> <p><i>Subid2:</i> Port identifier</p>

Appendix D Technical Specification

D.1 Physical details

D.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

D.1.2 Full-width (dual power) version

Height	43 mm, 1U
Width	444 mm excluding fixing brackets
Overall width	485 mm including fixing brackets
Depth	320 mm excluding connectors
Overall depth	340 mm including connectors
Approximate weight	5 kg
Rack-mount case	19 inch width, 1 U height

D.2 Environmental conditions

Table D.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

D.3 Power

D.3.1 AC Mains supply

Table D.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

D.3.2 DC supply

Table D.3 DC Power
Supply Specification

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

Table D.4 Physical details

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

D.4 Input/output ports

D.4.1 DVB ASI port

Table D.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

D.4.2 Ethernet management port

Table D.6 Ethernet Management Port Specification

Type	10/100Base-T
Connector type	RJ45

D.4.3 Ethernet data port

Table D.7 Ethernet Data Port Specification

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

Table D.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).
-------------	---

D.4.4 Alarm relay and maintenance port specification

Table D.9 Alarm Relay and Reset Port Specification

Connector type	9-pin DSUB Male
RS232 baud rate	115.2 kBd
RS232 framing	8 bits, no parity, 1 stop bit (8N1)
RS232 handshake	None
Relay rating	0.1 A max, 50 VDC max
Relay minimum load	10 μ A at 10 mVDC
Reset activation time	8 seconds

Table D.10 Alarm Relay and Reset Port Pin Out

PIN	Connection
1	(NC)
2	RS232 Receive Data (input)
3	RS232 Transmit Data (output)
4	(NC)
5	Earth
6	Alarm on
7	Alarm relay common
8	Alarm off
9	(NC)

D.5 External reference

D.5.1 10MHz/1 PPS input

Connector type	BNC 50 Ω socket
-----------------------	------------------------

D.5.2 10 MHz input

Connector type BNC 50 Ω socket

D.6 Compliance

D.6.1 Safety

The equipment has been designed to meet the following safety requirements: [Table D.11](#).

Table D.11 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.

D.6.2 Electromagnetic compatibility - EMC

The equipment has been designed to meet the following EMC requirements:

EN 55022 and AS/NZS 3548 (European, Australian and New Zealand)

Emission Standards Limits and methods of measurement of radio frequency interference characteristics of information technology equipment - Class A.

EN 61000-3-2 (European)

Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions.

EN 50082-1 (European)

Generic Immunity Standard Part 1: Domestic, commercial and light industry environment.

FCC (USA)

Conducted and radiated emission limits for a Class A digital device, pursuant to the Code of Federal Regulations (CFR) Title 47-Telecommunications, Part 15: radio frequency devices, sub part B -Unintentional Radiators.

D.6.3 CE marking

The CE mark indicates compliance with the following directives:

89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to electromagnetic compatibility.

73/23/EEC of 19 February 1973 on the harmonisation of the laws of the Member States relating to electrical equipment designed for the use within certain voltage limits.

1999/5/EC of March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity.

D.6.4 Interface to “public telecommunication system”

The equipment is not constructed for electrical connection directly to a “public telecommunication system”. None of the signals shall be connected directly from the unit to a “public telecommunication system” leaving the building without using some kind of interface in between such as a telecom terminal, switch or similar unit. Such kind of buffer is required to achieve a protective electrical barrier between the “public telecommunication system” and the unit. This electrical barrier is required to achieve protection against lightening or faults in nearby electrical installations.

Appendix E References

- [1] ISO13818-1, 2 and 3; MPEG-2 Video and Audio and Systems
- [2] ETSI EN 300 468: Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB Systems.
- [3] ETSI TR 101 211: Digital Video Broadcasting (DVB); Guidelines on Implementation and Usage of Service Information.
- [4] ETSI EN 300 744. Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television.
- [5] ETSI TS 101 191. Digital Video Broadcasting (DVB); DVB mega-frame for Single Frequency Network (SFN) synchronisation.
- [6] ETR 154 Digital Video Broadcasting (DVB); Implementation Guidelines for the Use of MPEG-2 Systems, Video and Audio in Satellite and Cable Broadcasting Applications. ETSI Technical Report ETR 154, European Telecommunications Standards Institute ETSI.
- [7] IEEE 802.1Q-2005 802.1QTM, Standards for Local and metropolitan area networks, Virtual Bridged Local Area Networks
- [8] RFC 1889 - RTP; A Transport Protocol for Real-Time Applications.
- [9] RFC 3550 - RTP; A Transport Protocol for Real-Time Applications.
- [10] RFC 2733 - RTP; An RTP Payload Format for Generic Forward Error Correction.
- [11] RFC 2250 - RTP; RTP Payload Format for MPEG1/MPEG2 Video
- [12] RFC 3497 - RTP; Payload Format for Society of Motion Picture and Television Engineers (SMPTE) 292M Video
- [13] RFC 3376 - IGMP; Internet Group Management Protocol, Version 3

-
- [14] RFC 2236 - IGMP; Internet Group Management Protocol, Version 2
 - [15] RFC 0791 - IPv4; Internet Protocol
 - [16] RFC 0793 - TCP ; Transmission Control Protocol
 - [17] RFC 0792 - ICMP; Internet Control Message Protocol
 - [18] RFC 0768 - UDP ; User Datagram Protocol
 - [19] RFC 0959 - FTP; File Transfer Protocol
 - [20] RFC 2068 - HTTP; Hypertext Transfer Protocol – HTTP/1.1
 - [21] RFC 0764 - Telnet; Telnet Protocol specification
 - [22] RFC 1157 - SNMP; Simple Network Management Protocol (SNMP)
 - [23] RFC 2030 - SNTP; Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
 - [24] RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets; MIB-II
 - [25] RFC 4326 - Unidirectional Lightweight Encapsulation for Transmission of IP Datagrams over an MPEG-2 Transport Stream
 - [26] Pro MPEG Forum Code of Practice #3 version 2; Transmission of Professional MPEG-2 Transport Streams over IP Networks
 - [27] Pro-MPEG Code of Practice #4 release 1 July 2004; Transmission of High Bit Rate Studio Streams over IP Networks

