BRIDGE TECHNOLOGIES™



VB330-SW 10G Software Probe User's Manual

Applies to software release v5.5

July 2019

Current documents are always found in the log-in area of the **www.bridgetech.tv** site.
Refer to section 1.2 of this document for more information.

10G Software Probe User's Manual
Revision 71a3a3f (2019-07-01)

Copyright © Bridge Technologies Co AS. Bentsebrugata 20, NO-0476, Oslo, Norway.
All rights reserved.

This publication can contain confidential, proprietary, and confidential trade secret information. No part of this document may be copied, photocopied, reproduced, translated, or reduced to any machine-readable or electronic format without prior written permission from Bridge Technologies Co AS. CE-marked in accordance to low voltage directive (LVC) 73/23/EEC and EMC directive 89/336/EEC. Compliant to requirements for US and Canada. Designed for CSA approval. Bridge Technologies Co AS continuously improves on products and reserves the right to modify the specifications without prior notice. Information in this document is subject to change without notice and Bridge Technologies assumes no responsibility or liability for any errors or inaccuracies.

The BRIDGE, BRIDGE TECHNOLOGIES and BRIDGETECH name, logo and all other related logos are registered trademarks of BRIDGE TECHNOLOGIES Co AS.

All other products or services mentioned in this document are identified by the trademarks, service marks, or product names as designated by the companies who market those products. Inquiries should be made directly to those companies. This document may also have links to third-party web pages that are beyond the control of Bridge Technologies. The presence of such links does not imply that Bridge Technologies Co AS endorses or recommends the content on those pages. Bridge Technologies acknowledges the use of third-party open source software and licenses in some products.

This product can include software developed by the following people and organizations with the following copyright notices:

- Curl. Copyright © Daniel Stenberg and many contributors. All rights reserved.
- Dropbear. Contains software copyright © 2008 Google Inc. All rights reserved.
- OpenSSL Project for use in the OpenSSL Toolkit. (https://www.openssl.org/).
  Copyright © 1998-2017. The OpenSSL Project. All rights reserved.
- Webmin. Copyright © Jamie Cameron.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Contents

Contents 3

1 INTRODUCTION 7
1.1 About the 10G Software Probe . . . 7
1.1.1 VB330-SW – Overview . . . 7
1.1.2 10G Software Probe – Functionality . . . 7
1.2 How to Use This Manual . . . 8

2 PRINCIPLE OF OPERATION 10

3 INSTALLATION AND INITIAL SETUP 12
3.1 System Requirements . . . 12
3.2 First-time Installation . . . 13
3.3 Deploying in a Virtualized Environment . . . 14
3.4 Verifying Correct Initial Setup and Software Activation . . . 14
3.5 Initial Setup Troubleshooting . . . 16
3.6 Upgrading From a Previous Version . . . 17
3.6.1 Upgrading by Re-Installing the System . . . 17
3.6.2 Upgrading From Version 5.3.0 or later . . . 18
3.7 Upgrading To a Maintenance Release . . . 18
3.8 Accessing the User Interface . . . 18
3.9 Accessing Software Activation interface . . . 18
3.10 Deactivating . . . 19

4 QUICK SETUP GUIDE 20
4.1 Basic Setup . . . 20
4.2 Input Signal Definitions . . . 20
4.2.1 Multicasts . . . 20
4.2.2 OTT Input (OTT Engine Option Only) . . . 20
4.3 Monitoring . . . 21
4.4 Adjusting Alarm Thresholds . . . 21

5 THE SOFTWARE PROBE GRAPHICAL USER INTERFACE 23
5.1 Main . . . 25
5.1.1 Main — Summary . . . 25
5.1.2 Main — CPU usage . . . 27
5.1.3 Main — Thumb overview . . . 28
5.1.4 Main — Eii graphing . . . 29
5.2 Alarms . . . 32

5.2.1 Alarms — All Alarms . . . 33
5.2.2 Alarms — Alarm setup . . . 34
5.3 OTT (Option) . . . 40
5.3.1 OTT — Active testing . . . 40
5.3.2 OTT — Details . . . 41
5.3.2.1 OTT — Details — Profiles . . . 42
5.3.2.2 OTT — Details — Manifest . . . 44
5.3.2.3 OTT — Details — Alarms . . . 46
5.3.2.4 OTT — Details — Thumbnails . . . 47
5.3.2.5 OTT — Details — Alignment . . . 48
5.3.3 OTT — Latency . . . 49
5.3.4 OTT — Channels . . . 50
5.3.5 OTT — Settings . . . 53
5.3.6 OTT — Thresholds . . . 54
5.4 Multicasts . . . 56
5.4.1 Multicasts — Parameters . . . 56
5.4.2 Multicasts — Parameters — Fields . . . 65
5.4.3 Multicasts — Summary . . . 66
5.4.4 Multicasts — History . . . 67
5.4.5 Multicasts — Detect . . . 68
5.4.6 Multicasts — SAP . . . 68
5.4.7 Multicasts — Join . . . 69
5.4.8 Multicasts — Streams . . . 70
5.4.9 Multicasts — Ethernet thresh. . . . 74
5.5 MW (Media Window) . . . 76
5.5.1 Media Window — Selected channel . . . 78
5.5.2 Media Window — Bandwidth graph . . . 79
5.5.3 Media Window — Inter Arrival Time graph . . . 79
5.6 RDP (Return Data Path) . . . 79
5.6.1 RDP — Control . . . 80
5.6.2 RDP — Setup . . . 80
5.7 Traffic . . . 82
5.7.1 Traffic — Protocols . . . 82
5.7.2 Traffic — Detect . . . 84
5.7.3 Traffic — Filter statistics . . . 85
5.7.4 Traffic — Filter setup . . . 87
5.7.5 Traffic — Microbitrate . . . 89
5.8 Ethernet . . . 90
5.8.1 Ethernet — FSM . . . 90
5.8.1.1 Ethernet — FSM — Monitor . . . 91
5.8.1.2 Ethernet — FSM — Setup . . . 92
5.8.1.3 Ethernet — FSM — Syslog . . . 94
5.8.2 Ethernet — IGMP . . . 95
5.8.3 Ethernet — PCAP . . . 96
5.9 ETR 290 (Option) . . . 97
5.9.1 ETR 290 — ETR Overview . . . 97
5.9.2 ETR 290 — ETR Details . . . 98
5.9.3 ETR 290 — PIDs . . . 100
5.9.4 ETR 290 — Services . . . 102

5.9.5 ETR 290 — Bitrates . . . 105
5.9.6 ETR 290 — Tables . . . 106
5.9.7 ETR 290 — PCR . . . 109
5.9.8 ETR 290 — T2MI (requires T2MI-OPT) . . . 110
5.9.9 ETR 290 — SCTE 35 (requires SCTE35-OPT) . . . 114
5.9.10 ETR 290 — Status . . . 116
5.9.11 ETR 290 — Compare . . . 116
5.9.12 ETR 290 — ETR threshold . . . 120
5.9.13 ETR 290 — PID thresholds . . . 131
5.9.14 ETR 290 — Service thresh. . . . 133
5.9.15 ETR 290 — Gold TS thresholds . . . 136
5.10 Setup . . . 141
5.10.1 Setup — Params . . . 141
5.10.2 Setup — Pages . . . 142
5.10.3 Setup — Colors (requires EXTRACT-OPT) . . . 143
5.10.4 Setup — Ethernet . . . 143
5.10.5 Setup — VBC . . . 144
5.10.6 Setup — Login . . . 144
5.10.7 Setup — ETR . . . 146
5.10.8 Setup — VBC thresh. . . . 148
5.10.9 Setup — Scheduling . . . 150
5.10.10 Setup — Routing . . . 151
5.10.11 Setup — Security . . . 152
5.10.11.1 Setup — Security — Ports . . . 152
5.11 Data . . . 153
5.11.1 Data — Configuration . . . 153
5.11.2 Data — Software . . . 154
5.11.3 Data — Table Descriptors . . . 155
5.11.4 Data — Eii . . . 155
5.12 About . . . 156
5.12.1 About — Release info . . . 156
5.12.2 About — License . . . 156
5.12.3 About — Technologies . . . 158
5.12.4 About — Credits . . . 158
5.12.5 About — System . . . 158

A Appendix: VB330-SW Versus VBC Alarms 160

B Appendix: Monitoring Practices 162
B.1 RTP Monitoring . . . 162
B.2 Default Multicast Monitoring . . . 162
B.3 Strategy for MediaWindow Analysis . . . 163
B.3.1 IAT Before and After Router . . . 164
B.3.2 Identifying UDP Packet Loss . . . 165
B.4 Multicast Thresholds . . . 166
B.5 Dedicated interface for OTT . . . 166
B.6 OTT descrambling with Verimatrix . . . 166
B.7 OTT Bandwidth requirements . . . 166



C Appendix: OTT Profile Health 167
C.1 OTT Profile Health Bar . . . 167
C.2 OTT Profile Health Timeline . . . 167

D Appendix: Network configuration 169
D.1 Web-based configuration . . . 169
D.2 Command-line based configuration . . . 169

E Appendix: Enabling HTTPS 174

F Appendix: Enabling NTP time synchronization 177

G Appendix: On-line License Verification 178
G.1 Introduction . . . 178
G.2 Requirements . . . 178

H Appendix: Software Maintenance 181

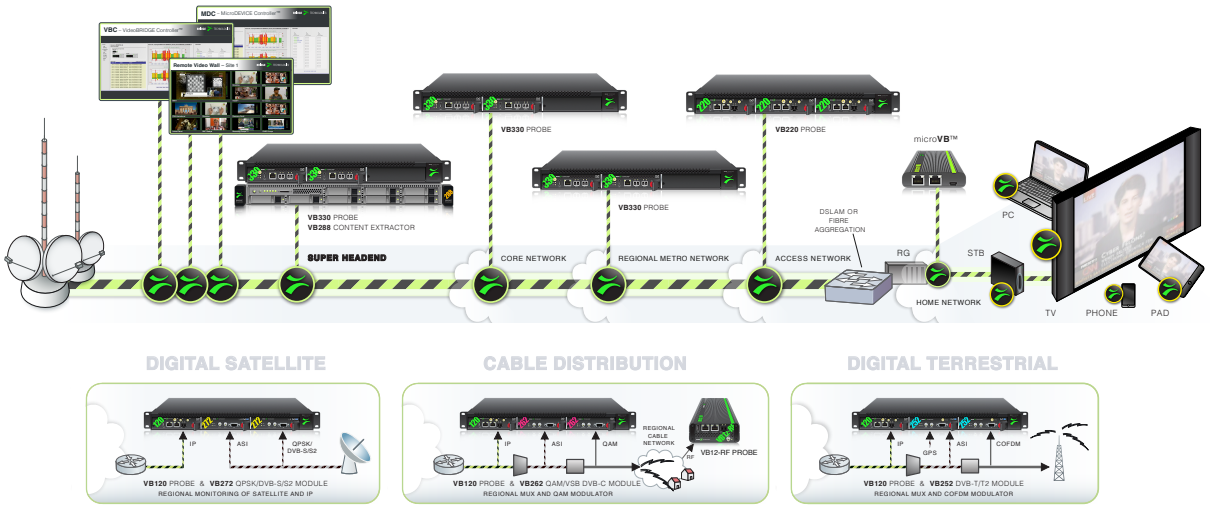
I Appendix: Software Upload 182
I.1 Obtain the software image . . . 182
I.2 Export and save the probe configuration . . . 182
I.3 Transfer the image to the probe and save . . . 182
I.4 Wait while the software is being saved . . . 184
I.5 Verify the new image . . . 184
I.6 Software upload troubleshooting . . . 185

1 INTRODUCTION

1.1 About the 10G Software Probe

1.1.1 VB330-SW – Overview

The VB330-SW 10G Software Probe was made specifically for IPTV backbone network monitoring. With support for 10 Gbit/s Ethernet inputs, the 10G Software Probe provides detailed IP packet monitoring of a very high number of Ethernet streams, suitable for core networks carrying extreme amounts of media signals.



The OTT software option is available on the VB330-SW and enables monitoring of up to 500 adaptive bitrate channels in steps of 5 or 50 (Bulk OTT option) OTT engines depending on licensing.

A built-in web server in the VB330-SW allows remote signal monitoring using a standard web browser. This can be managed either through a separate Ethernet network, or by using the regular video/data network – both IPv4 and IPv6 are supported.

The VB330-SW 10G Software Probe can also be managed via the VBC Controller. The VBC Controller will add management features like alarm aggregation and report functionality.

The 10G Software Probe is a server appliance, that can be installed onto any server that meets the minimum requirements specified in chapter 3.

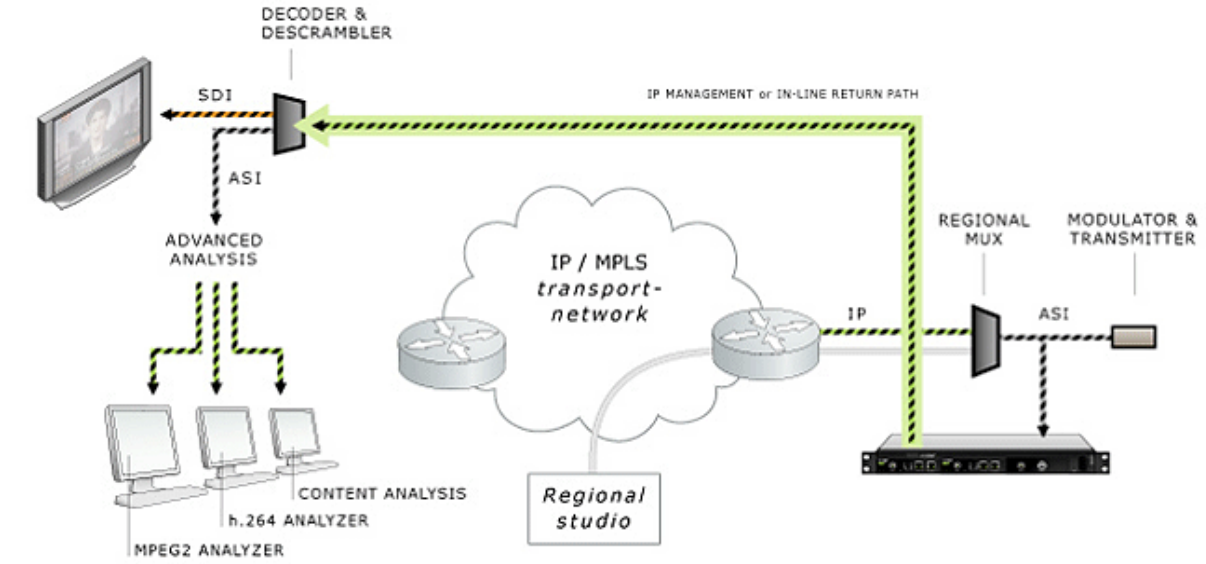
1.1.2 10G Software Probe – Functionality

An IP-based network is fully transparent with respect to signal contents quality, provided that the IP packets arrive, and provided that they arrive in time. The 10G Software Probe therefore uses the patented MediaWindow to allow monitoring at-a-glance of packet loss and errors in inter-packet arrival time. This way the operator can conveniently ensure correct signal quality at IP-level.

The advanced Ethernet protocol analysis tool automatically detects all protocols carried over Ethernet past the port the 10G Software Probe is connected to, and it displays statistics like percentage utilization of the interface and percentage of the different transported protocols. This gives the 10G Software Probe a real-time sniffer capability.

The 10G Software Probe allows the user to define a Return Data Path (RDP), using the regular video/data network or the management network to return a stream. A faulty signal can then be further analyzed at the studio premises, when necessary.

The recording functionality allows the user to record a stream, either triggered manually by the user or triggered by a user defined alarm.



RDP™
RETURN DATA PATH

Full Service Monitoring (FSM) checks that vital system components like CA-servers are active.

Optional Ethernet TR 290 monitoring allows the operator to check parameters like transport stream sync and PSI/SI standards conformity. This option also performs further PSI/SI analysis, making it possible to view PSI/SI contents. PID and service bitrates are also continuously measured.

Optional OTT monitoring allows the operator to set up active testing of Over-the-top type signals as found in adaptive bitrate streaming architectures. Formats supported include Apple ™ HLS, Microsoft ™ Smoothstream, RTMP, MPEG DASH, Adobe ™ HDS and Nullsoft SHOUTcast™.

The 10G Software Probe can be expanded through license options to monitor the T2MI protocol layer as found in DVB-T2 networks.

The 10G Software Probe can also be licensed with an SCTE 35 option that allows monitoring and logging of splice time codes embedded in the transport streams.

1.2 How to Use This Manual

This User's Manual is valid for software version 5.5 of the VB330-SW 10G Software Probe.

Throughout this manual the term stream is often used rather than unicast or multicast. One stream may consist of one or more services, and refers to one IP uni- or multicast.

Chapter 2 **PRINCIPLE OF OPERATION** provides a simplified block-diagram overview of the probe.

Chapter 3 **INSTALLATION AND INITIAL SETUP** explains how to install the software on a server.



Chapter 4 **QUICK SETUP GUIDE** contains a quick setup guide; a step-by-step description of how to setup the 10G Software Probe once the initial setup has been performed.

Chapter 5 **THE SOFTWARE PROBE GRAPHICAL USER INTERFACE** describes the graphical user interface (GUI) as seen when pointing a web browser to the 10G Software Probe's IP address.

A **Appendix: VB330-SW Versus VBC Alarms** describes the alarm handling in the 10G Software Probe versus the VBC Controller.

B **Appendix: Monitoring Practices** explains some useful monitoring practices.

C **Appendix: OTT Profile Health** explains the OTT profile health bar and timeline.

D **Appendix: Network configuration** gives a brief introduction to the server OS network configuration.

F **Appendix: Enabling NTP time synchronization** provides some basic information about setting up time synchronization.

G **Appendix: On-line License Verification** outlines the on-line license verification procedure.

H **Appendix: Software Maintenance** briefly describes software maintenance licenses and how they are used.

I **Appendix: Software Upload** explains how to upgrade the software on the 10G Software Probe.

Note that current version of the User's Manual can be found on the `https://www.bridgetech.tv/` website. Log in as end user: **customer** with password: **xmas4u**. Additional technical documentation is also found at the same location.

2 PRINCIPLE OF OPERATION

The VB330-SW 10G Software Probe can utilize all the network interfaces on the host system. The user selects which interface to be used by the monitoring engine. Management of the 10G Software Probe is configured in the operating system web server setup[1].

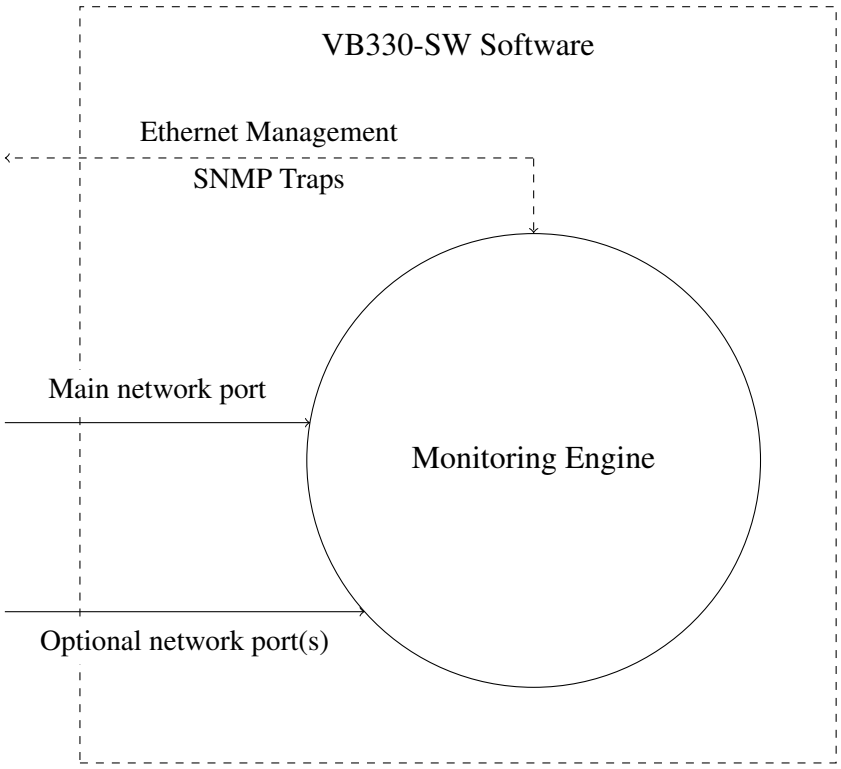


Figure 2.1: The VB330-SW Software – Principle of Operation

A simplified diagram of the alarm handling mechanisms of the 10G Software Probe is shown in figure 2.2. The input signals are continuously analyzed, and measured data are checked against user defined threshold values. If the data do not comply with the threshold values alarms will be generated. The overall alarm settings further make it possible to enable and disable alarms, thus defining which alarms should be reported in the 10G Software Probe alarm list and sent as SNMP traps to an external management system.

[1] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/ch-Web_Servers.html

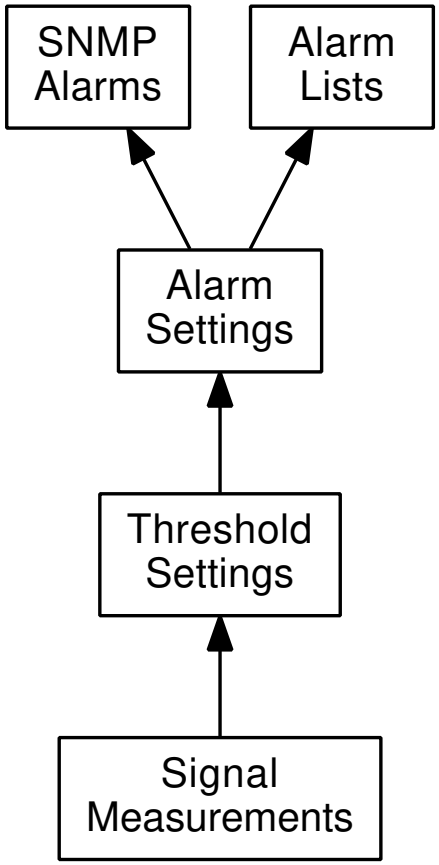


Figure 2.2: Simplified Diagram of the Alarm Handling in the 10G Software Probe



3 INSTALLATION AND INITIAL SETUP

3.1 System Requirements

The minimum hardware requirements for virtualized or natively running Software Probe with performance similar to or better than VB330:

- Intel XEON D-1537 1.7 GHz, 12 Mbyte Cache, 8 cores
- 8 Gbyte RAM
- 100 Gbyte HDD
- 10 Gbit/s Network Interface card for data: Intel X550/X552/X557
- Additional 10/100/1000T Ethernet Network Interface card with support for CentOS Linux 7 or Red Hat Enterprise Linux 7 for management
- Note that there are motherboards with the 10Gbit/s NICs referred to above built-in. The XEON D family of CPUs has built-in support for these 10 Gbit/s NICs.

The Software Probe can be license upgraded to a higher bitrate independently of the hardware. It may thus be useful to obtain better hardware which allows for future license upgrade.

Recommended NICs

Interface	NIC	Notes
1G BASE-T	Intel I340 and Intel I350	RJ45 connector. Dual or single input.
10G BASE-T	Intel X550-T2 (dual)	RJ45 connector. Dual or single input. Supports 100Mb/1GbE/2.5GbE/5GbE/10GbE.
10G SFP28	Mellanox ConnectX-4 Lx 10gbe	SFP+ compatible connector. Dual or single input. Supports 1/10GbE.
25G SFP28	Mellanox ConnectX-4 Lx 25gbe	Dual or single input. Also available for OCP with Host Management. Supports 1/10/25GbE.
100G QSFP28	Mellanox ConnectX-5 Ex 100gbe PCIe 4.0	Dual or single input. Supports 1/10/25/40/50/100GbE.

Supported platforms:

- CentOS Linux release 7 (7.3–7.6) for x86_64
- Red Hat Enterprise Linux Server release 7 (7.3–7.6) for x86_64

If the system is upgraded to an unsupported operating system release, an error message will be displayed in the Application notification menu upon accessing the user interface. Check the release notes available for the currently installed software version before updating to a new operating system release.

3.2 First-time Installation

Make sure that the server hardware matches the requirements listed above. Download the appropriate installation image from the end-user area on `https://www.bridgetech.tv/` and then follow the procedure outlined below.

1. Obtain the latest installation kickstart image.

   Installation media is provided both for CentOS Linux and Red Hat Enterprise Linux. If you install the Red Hat Enterprise Linux version, you will need an active subscription for Red Hat Enterprise Linux server.

2. Insert the installation medium into the server:

   - For DVD-based installations, burn the downloaded ISO image to a DVD and insert into the server.
   - For USB-based installation, transfer the downloaded image to a USB mass storage device using a tool such as **dd** (Mac, Unix, Linux) or **USBWriter**[1] (Windows).
   - For installation in a virtualized environment, attach the downloaded ISO image to a virtual DVD-ROM unit.

     Note: Please read the advice on how to configure the virtual machine in section 3.3 to ensure optimal performance.

3. Boot the server and make sure that the primary boot device is set appropriately. If the system fails to boot from the medium, you may need to configure the boot loader for 'legacy BIOS mode'.

4. The installer will run, please follow the on-screen prompts to install the system, taking note of the following:

   - **IMPORTANT:** Leave 'Software selection' at 'Custom software selected'.
   - **IMPORTANT:** In the 'Installation Destination', the default partitioning will create a large `/home` partition, which is unused. To avoid this, use the 'I will configure partitioning' option. Then use the 'Click here to create them automatically' and manually reduce the size of (or remove) the `/home` partition, instead giving that space to the `/` partition.
   - We recommend that you configure network settings (IP address, gateway, DNS) within the installer. Post-installation network configuration can be performed using the **nmtui** utility, please refer to D Appendix: Network configuration for details.
   - The default installation does not provide any graphical user interface environment. This can be installed later if desired, please refer to the CentOS Linux[2] or Red Hat Enterprise Linux[3] documentation for more details.

5. At the end of the installation procedure, the server is rebooted. Remove the installation media and ensure that the system boots up properly.

[1] `https://sourceforge.net/projects/usbwriter/`
[2] `https://wiki.centos.org/Manuals/ReleaseNotes/CentOS7`
[3] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/index.html`



6. If you installed the Red Hat Enterprise Linux server flavor, make sure you follow the instructions on how to subscribe the system to the Red Hat Customer Portal[4].

   If you install the CentOS Linux flavor, you may want to enable the Continuous Release repository[5] to be able to get access to security updates as quickly as possible.

7. Enter the selected IP address in your web browser to access the Software Activation page. If your host is using dynamic addressing, you can log in to the account created during installation and issue the command **ip addr** to display the address assigned to the system.

   Continue to chapter 3.4 for details on how to enable the 10G Software Probe system.

The kickstart will install CentOS Linux 7 or Red Hat Enterprise Linux 7 on the server. The disks will be formatted and all contents lost. Make sure that any important data on the server has been backed up before beginning the procedure.

3.3 Deploying in a Virtualized Environment

It is also possible to deploy the software in a virtualized environment. For optimal performance, check the processor configuration of **cores per socket** on your host server and use the same configuration setting of cores per virtual sockets on the virtual machine.

For accurate measurements, you must configure the data network interface card(s) in **pass-through mode** on the host server.

Please follow the steps from chapter 3.2 when installing the software in the virtualized environment. We recommended **disabling** any 'Easy install' or similarly worded option, and *not* selecting the operating system type when initially creating the new virtual machine instance in your virtualization environment. These options may override the installation instructions included in the provided installation image, causing an incomplete installation.

Pre-built images for VMware (vSphere/Workstation/Player) are provided in `OVA` (Open Virtualization Format Archive) format. These images contains a system already installed according to the steps described in the previous chapter, with VMware Tools already installed and activated.

To deploy the image, you need to import it to the virtualization host, please refer to the documentation of your virtualization environment for more details on how to do this.

If installed in a VMware vSphere environment, the machine should report back its network configuration to the host environment. Please allow some time for it to do so, and then continue with point 6 as described in the previous chapter.

When logging in to the console of the pre-built images, the default password for the **root** user is **elvis**. The same password is also used for logging in remotely using Secure Shell (ssh). **Please change the password for the root user after finishing the install**, log in and use the `passwd` command to do this.

3.4 Verifying Correct Initial Setup and Software Activation

Once the software has been installed and restarted all further configuration takes place through the web interface.

[4] `https://access.redhat.com/solutions/253273`
[5] `https://wiki.centos.org/AdditionalResources/Repositories/CR`

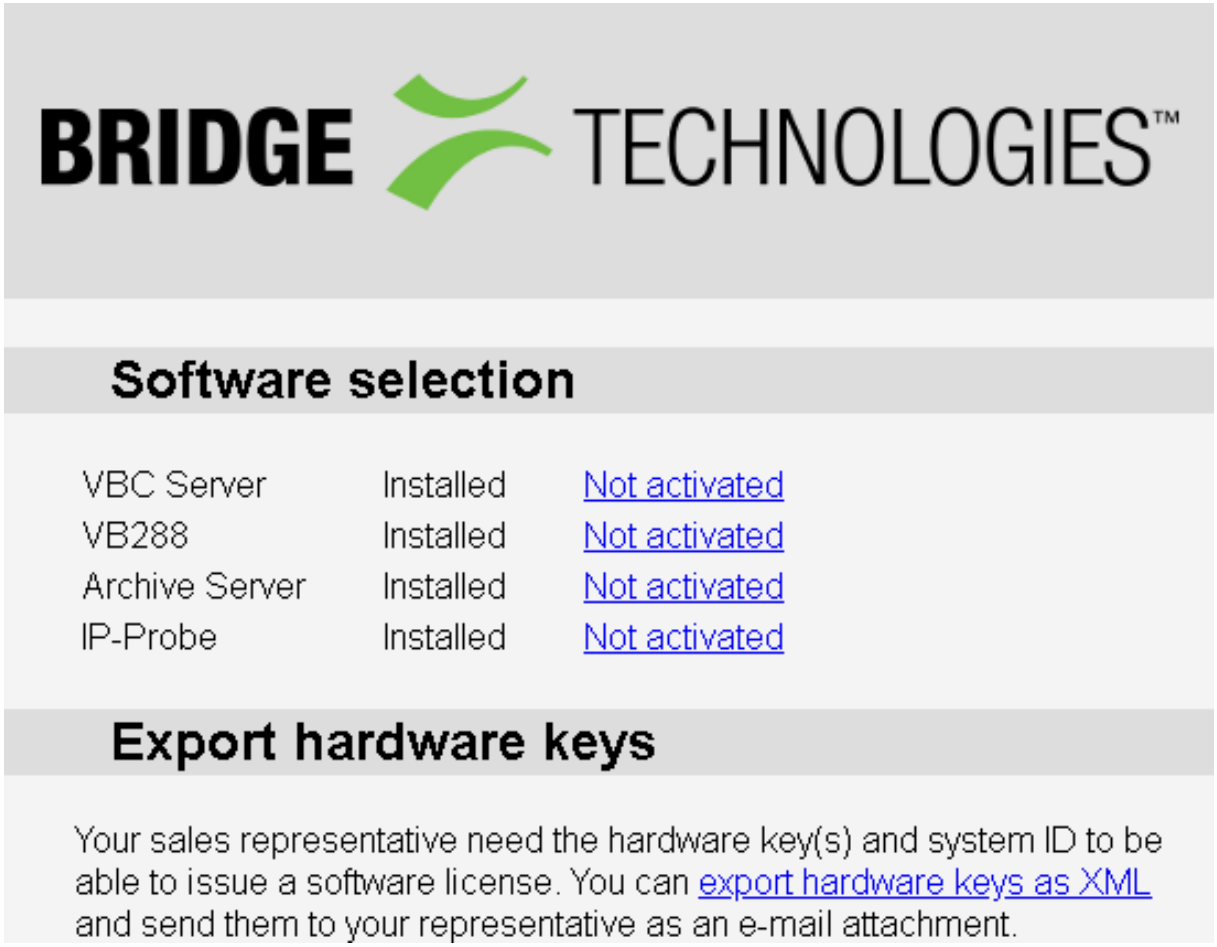


Figure 3.1: Software Activation

1. Launch a web browser application on the management system.

   Any web browser with support for JavaScript can be used to access the Software Activation interface, one of the following are recommended:

   - Google Chrome
   - Mozilla Firefox
   - Microsoft Edge
   - Microsoft Internet Explorer 11 or higher
   - Apple Safari

2. Type the IP address of the server in the browser URL field and press Enter.

   The network settings should have been set when the operating system was installed. If the web browser is unable to reach the web server, check the server's network settings in the operating system.

3. The Software Activation view should be displayed inside the browser. Software Activation is password-protected, the user name is **admin** and the default password is **elvis**. The page displayed should look similar to figure 3.1.



The password should be changed from the default. Expand the **More options** heading and follow the instructions under **Change password**[6].

4. If you already have an XML file with license keys for your system, click on the **More options** heading and upload this file under the **Import license keys** option. If you have the license key written down or in an e-mail, instead use the product page described below.

5. If this is a new server, and you need to obtain license keys for the purchased products, please click the link labeled **export hardware keys as XML** and send the downloaded file to your sales representative as an e-mail attachment.

6. The 10G Software Probe is not enabled by default on the newly installed server. To enable it, use the link labeled **Not activated** next to its name. This will take you to a page giving you the details of the installed software, such as the installed version and the hardware key. If you have a license key that you want to enable and have not yet done so, enter the key in the field labeled **Apply license key** and click the **Add license** button.

7. Click the button labeled **Activate software** and wait for it to finish. If successful, the 10G Software Probe should now be activated, and you will be presented with a link to the user interface. The next time you access the server using a web browser, you should be taken automatically to the enabled software.

   Please note that it may take some additional time before the user interface of the activated product becomes available. If you receive an error trying to access it, please wait for a few minutes before trying again.

   Note that it is not possible to activate the Software Probe and the VB288 Objective QoE Content Extractor on a single system at the same time.

To return to the Software Activation view to make changes, open the **About — License** tab in the 10G Software Probe user interface and click the link labeled **Manage installed software**.

By default, all web communication to and from the host running the 10G Software Probe is using unencrypted HTTP communication. Please refer to E Appendix: Enabling HTTPS for information on how to enable HTTPS.

It is **strongly recommended** that the system time is configured to be synchronized against an external NTP server. Please refer to F Appendix: Enabling NTP time synchronization for more information on configuring time synchronization.

3.5 Initial Setup Troubleshooting

If you are having trouble bringing up the Software Activation interface, or the 10G Software Probe web based management interface, verify the following:

- Verify that the client machine and the 10G Software Probe are configured on the same subnet and that they have different addresses, or, if you use different subnets, verify that the routing and gateways are set correctly on both the client machine and the 10G Software Probe.
- Make sure that the IP address of the gateway and the network interface are not the same.

[6] If you forget the Software Activation password, you can reset it by logging in as root and issuing the command `/opt/btech/ssg/bin/reset_web_password`



- Verify that the appropriate Ethernet link indicators of the PC and the 10G Software Probe are lit.
- Verify that web browser proxy settings are not interfering.
- Verify that local firewall settings on the PC are not interfering.
- Try rebooting the server and make sure all services start as expected.
- Clear the browser's cache.
- Verify that the web server is running, by entering the command

```
systemctl status httpd
```

  on the server's command line. If it is not running properly, or you are seeing **DNS lookup failure** errors, try issuing the command

```
echo "ServerName localhost" >> /etc/httpd/conf/httpd.conf
```

  and then restart the server by issuing the command

```
systemctl restart httpd
```

- If you can reach Software Activation but the 10G Software Probe GUI is not working, enter the command `probehello` on the server's command line to verify that the VB330-SW services are running. If services are not running, try re-installing the VB330-SW.

Please refer to D Appendix: Network configuration for more information on server network configuration.

3.6 Upgrading From a Previous Version

You can either re-install the system as mentioned below, or by using one of the provided upgrade images.

Download the appropriate installation image from the end-user area on `https://www.bridgetech.tv/` and then follow the procedure outlined below.

3.6.1 Upgrading by Re-Installing the System

If you want to re-install the system from scratch, please follow these steps:

1. Backup the system configuration (**Data — Configuration — Full configuration**).
2. Export the current license (**About — License — Export current license and software maintenance keys**).
3. Possibly back up the system network configuration by logging in to the machine and copying any files matching the wildcard `/etc/sysconfig/network-scripts/ifcfg-*` to a safe location (off the system).
4. Re-install the system as described above.
5. Using the Software Activation page import the previous license key (under **More options**); or re-enter it using the activation page) and activate the software.
6. Import the configuration from **Data — Configuration — Import configuration XML**.

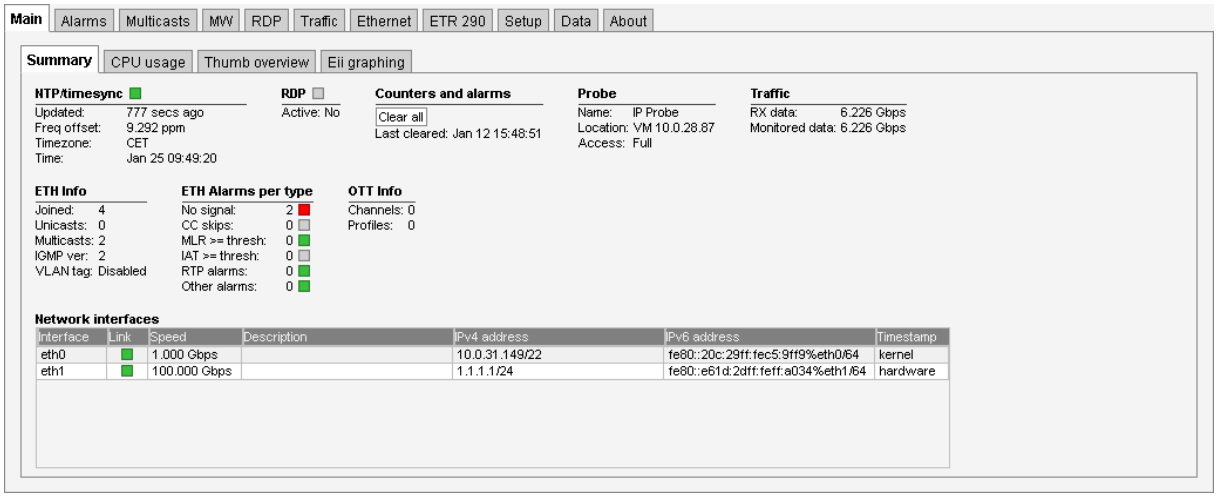


Figure 3.2: The VB330-SW Graphical User Interface

3.6.2 Upgrading From Version 5.3.0 or later

Please refer to chapter 5.11.2 and I Appendix: Software Upload for details on how to install the upgrade image.

3.7 Upgrading To a Maintenance Release

Please refer to chapter 5.11.2 and I Appendix: Software Upload for details on how to upgrade to maintenance releases.

3.8 Accessing the User Interface

Once the software has been installed and activated all further configuration takes place through HTTP.

The following web browsers are supported for the management interface:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11 or higher
- Apple Safari

The default management view should look similar to figure 3.2. If you have problems accessing the user interface, refer to chapter 3.5 for troubleshooting.

3.9 Accessing Software Activation interface

To return to the Software Activation view after activating the 10G Software Probe, you can either navigate to the **About — License** view and follow the **Manage installed software** link, or navigate your web browser to the address `http://<IP>/ssg`, where `<IP>` is the IP address (or host name, if using DNS) of the server.



3.10 Deactivating

To deactivate 10G Software Probe, you must first access the Software Activation interface (see the previous section) and make sure that it is not set to the default. Expand the **More options** heading and change the setting under **Set default software**.

Once this is done, access the 10G Software Probe user interface and de-activate it from the **About — License** view.



4 QUICK SETUP GUIDE

This quick setup guide is intended to provide a step-by-step explanation of how to setup a probe once the initial setup has been performed (as described in chapter 3).

More detailed instructions are found in chapter 5 of this manual.

The Return Data Path and Full Service Monitoring features are not covered by this quick setup guide.

4.1 Basic Setup

1. Set appropriate parameters in the **Setup — Params** view.
2. Enabling Time synchronization is strongly recommended. Please see F Appendix: Enabling NTP time synchronization for further details on how to configure the date and time.
3. If access control is required, define a password in the **Setup — Login** view.

   Note: it is important to read the instructions in the associated section of this manual, see chapter 5.10.6.

4.2 Input Signal Definitions

4.2.1 Multicasts

1. Define multicasts using the **Multicasts — Streams** view. You can also import multicast lists from another probe using the **Data — Configuration** view, or add them automatically, either by using the multicast detect feature in the **Multicasts — Detect** view, or from SAP announced streams using the **Multicasts — SAP** view.

   Note: Often upstream equipment will not transmit multicasts unless join messages have been received, and in this case it will usually not be possible to detect multicasts automatically.

   Select predefined threshold templates that seem appropriate for the signal.

   Note: The sequence of the multicast definitions will be reflected in monitoring, so order the multicasts correctly if required. Also note that ETR 290 monitoring for Ethernet streams is disabled by default, so if this is required, it will have to be enabled by the user (on a per-stream basis).
2. Define stream page name(s) in the **Setup — Pages** view (not strictly necessary).
3. Join multicasts in the **Multicasts — Join** view or in the **Multicasts — Streams** view.

4.2.2 OTT Input (OTT Engine Option Only)

1. Define the OTT channel manifest URLs and channel names in the **OTT — Channels** view. Leave the Threshold and VBC threshold settings at default values for now. Remember to tick the Enable box in the dialog box. If you have multiple OTT engines installed (1 to 50 are allowed) then select which engine to assign to the channel. Any number of OTT channels can be assigned to each OTT engine. Each engine works in parallel to each other.

   Note: When monitoring both multicast (UDP) and OTT (TCP) traffic, we recommend using different network interfaces. Mixing the two traffic types on the same network can have unwanted impact on the monitored signals. The interface used for OTT traffic is controlled using the **Setup — Routing** view.

2. Inspect the OTT monitoring progress using the **OTT — Active testing** dialog. Useful information on OTT monitoring can be found in Appendix C.

4.3 Monitoring

When input signal parameters have been set, the signals may be monitored.

For Ethernet multicasts the relevant monitoring views are **Main**, **Alarms**, **Multicasts**, **MW**, **Traffic** and **Ethernet**. If the probe is equipped with the ETR 290 and/or the OTT option then the views **ETR 290** and **OTT** are of relevance as well.

Ethernet monitoring hints are found in B Appendix: Monitoring Practices.

4.4 Adjusting Alarm Thresholds

When the probe inputs and streams have been defined using default thresholds, the result will usually be a number of more or less permanent alarms, some which may not be relevant under the current circumstances. In order for the user to get rid of unwanted alarms, the probe provides alarm filtering functionality in the form of alarm thresholds and alarm on/off selection.

Multicasts

By default Ethernet thresholds are set to raise alarms when service affecting errors occur, that are caused by the network. There may however be reasons for these thresholds to be altered, for instance to reflect receiver robustness in the case of IAT, or to reflect a TS into IP mapping different from the default (7TS/UDP). Creating a new threshold template is done either by copying an existing one and altering the copy, or by creating a new threshold template from scratch. The Ethernet thresholds are defined in the **Multicasts — Ethernet thresh.** view. These thresholds are associated with streams in the **Multicasts — Streams** view.

In addition to the miscellaneous thresholds, that affect only the streams with which they are associated, the **Alarm — Alarm setup** view allows the user to enable and disable alarms on an overall basis. You can also define the alarm severity levels for different alarms in this view.

OTT

When an OTT channel is defined the default OTT threshold template is assigned to it. To change threshold values create one or more new templates in the **OTT — Thresholds** view and assign them to OTT channels in the **OTT — Channels — Edit** view.

ETR 290

By default the streams configured in the probe will be set up to use the ETR 290 threshold named **Default**. This has the most important alarms enabled but have been adjusted to match real world systems and only alarm on more severe problems. The threshold named **ETSI TR 101 290** is based on the ETSI TR 101 290 guidelines and are fairly strict generating more alarms. The ETR 290 thresholds should be changed if there are tables that are not relevant for a system, or if the user requires alarm functionality that exceeds the ETR 290 guidelines. The ETR engines has a lot of powerful functionality not enabled by default, for instance the ability to raise alarms if the number of services present in a signal is lower than a preset limit.

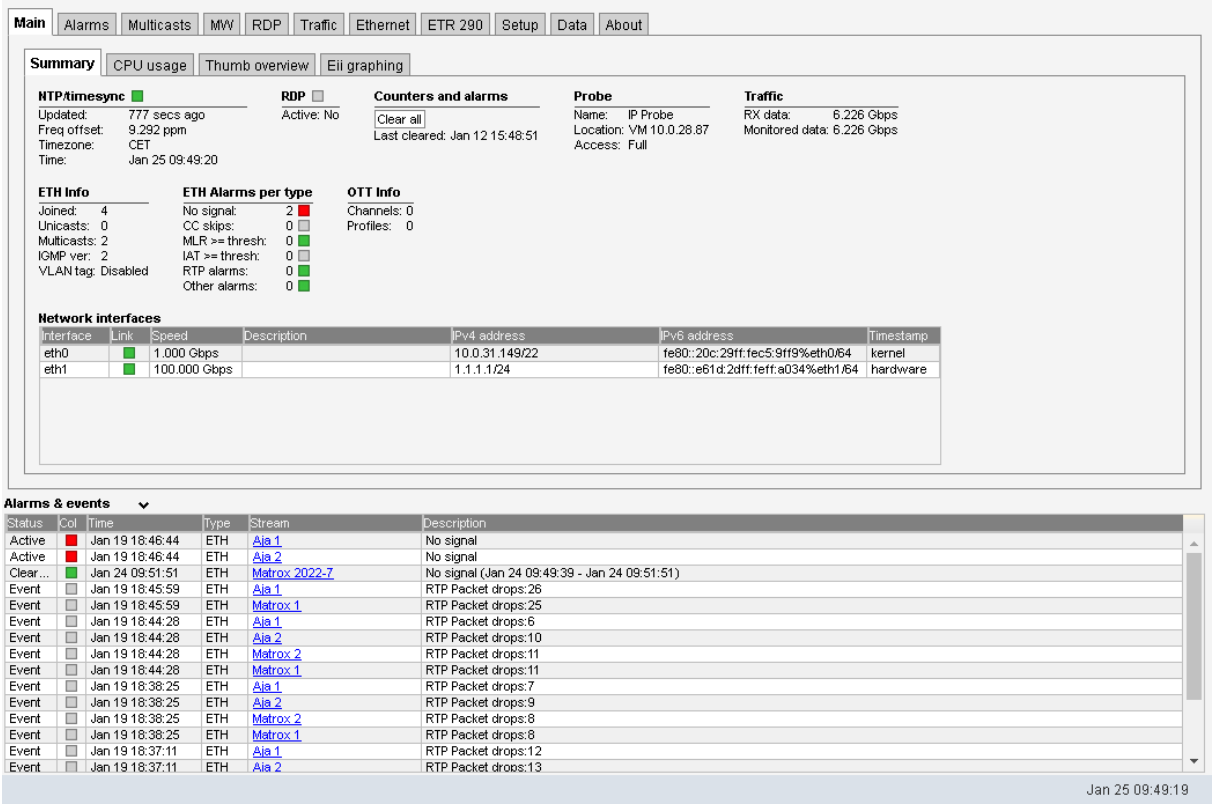
The default PID and service thresholds do not affect alarming at all, they are completely transparent. The thresholds may be altered for instance in order to mask an alarm generated by an unreferenced PID or to ensure an alarm is raised if a service or PID bitrate is outside preset limits.



Creating a new threshold template is done either by copying an existing one and altering the copy, or by creating a new threshold template from scratch. The thresholds are defined in these views: **ETR 290 — ETR thresh.**, **ETR 290 — PID thresh.**, **ETR 290 — Service thresh.**

The thresholds are associated with streams in the **Multicasts — Streams — Edit** view.

5 THE SOFTWARE PROBE GRAPHICAL USER INTERFACE



The VB330-SW web interface is reached by pointing a web browser to the IP address of the 10G Software Probe as shown in the screenshot above. The following web browsers are recommended:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Microsoft Internet Explorer 11 or higher
- Apple Safari

Note that different web browsers behave differently with respect to memory leaking, and if the VB330-SW GUI should be available at all times the browser should be selected carefully. A browser memory leak manifests itself as the browser responding more and more slowly, and this is corrected by closing down the application and restarting.

The interface is easy and intuitive to use. Navigate by clicking on the tabs just below the 10G Software Probe logo. Some of the pages have their own tabs for accessing nested pages. The bottom frame of the



interface is always the Alarms & events list, usually referred to as the **alarm list**. The alarm list can be displayed or hidden by clicking the **Toggle** link, which is displayed as an arrow head.

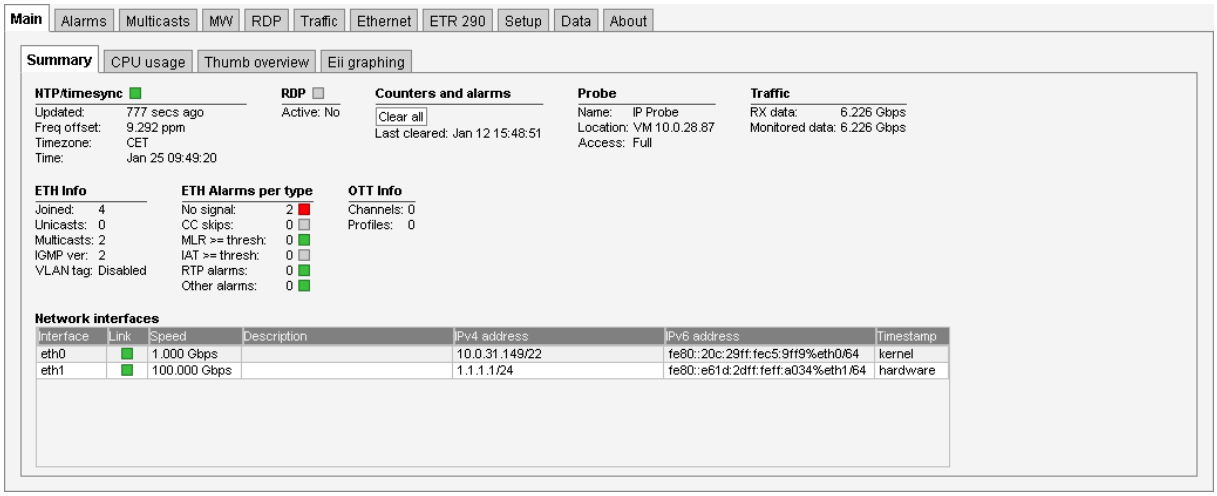
The web interface has been designed to be resizable in both vertical and horizontal directions with a minimum screen resolution of 1280×800 pixels.

Tool-tips are available for most buttons and labels. To access tool-tip information simply navigate the mouse pointer towards a button or a label and leave it hovering for a second or two.

In this manual the term stream is generally used instead of the terms multicast and/or unicast. A stream may thus contain a single service or multiple services.

5.1 Main

5.1.1 Main — Summary



The intention of this page, together with the **alarm list**, is to provide enough information for the operator to immediately see if there is anything seriously wrong with one or more input streams.

The following parameters are shown:

NTP/timesync	
(Bulb):	The NTP/timesync bulb indicates whether the VB330-SW clock is locked to an external time reference signal. Green indicates that the VB330-SW is locked to an external reference whereas grey indicates that the VB330-SW runs in unlocked mode or the status is unknown.
Updated:	The time since the last time synchronization update.
Freq offset:	Indicates the measured frequency offset for the system clock.
Timezone:	The time zone relative to UTC. Configured in the OS.
Time:	The current local time.

We recommend using the standard operating system tools for configuring the system clock. Please refer to the operating system instructions[1] for further details on how to configure the date and time.

RDP	
(Bulb):	The RDP bulb indicates whether RDP is active or not. Green indicates RDP active whereas grey indicates that RDP is currently not active.
Active:	The RDP active state is either *yes* or *no, yes* indicating that RDP relaying or alarm triggered recording mode has been selected by the operator in the **RDP** view.

Counters and alarms

[1] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Configuring_the_Date_and_Time.html



Clear all:	Click the **Clear all** button to reset all counters, graphs and alarms. All VB330-SW measurement and alarm history is cleared. Note that it is not possible to undo this operation.
Last cleared:	The time the **Clear all** button was last clicked. If no time is indicated the counters have not been cleared since VB330-SW startup/reboot time.

Probe	
Name:	The VB330-SW name as defined by the operator in the **Setup — Params** view.
Location:	The VB330-SW location as defined by the operator in the **Setup — Params** view.
Access:	The access rights of the current user. Access rights are either full access or read only access, and are defined by the operator in the **Setup — Login** view.

Traffic	
RX data:	The total bitrate of received data traffic
Monitored data:	The total bitrate of multicasts and unicasts monitored (analyzed) by the probe

ETH info	
Joined:	The number of joined streams (multicasts and unicasts)
Unicasts:	The number of unicasts currently being joined/monitored by the probe
Multicasts:	The number of multicasts currently being joined/monitored by the probe
IGMP ver:	The IGMP version currently used by the probe. IGMPv2 is used unless the operator has selected source specific multicasts (**Setup — Params** view), in which case IGMPv3 is used.
VLAN tag:	The VLAN tag currently used by the probe. If no VLAN tag has been specified by the operator (**Setup — Params** view), the VLAN tag value will read disabled.

ETH alarms per type	
No signal:	The number of currently active Ethernet 'No signal' alarms
CC skips:	The number of currently active Ethernet 'CC skips' alarms
MLR>=thresh:	The number of currently active Ethernet MLR alarms, i.e. the total number of 'MLR>= warning-threshold' and 'MLR>= alarm-threshold' alarms
IAT>=thresh:	The number of currently active Ethernet IAT alarms, i.e. the total number of 'IAT>= warning-threshold' and 'IAT>= alarm-threshold' alarms
RTP alarms:	The number of currently active RTP alarms, i.e. the total number of 'RTP packet drop', 'RTP duplicates' and 'RTP out of order' alarms
Other alarms:	The total number of currently active Ethernet alarms not included in the alarm figures specified above

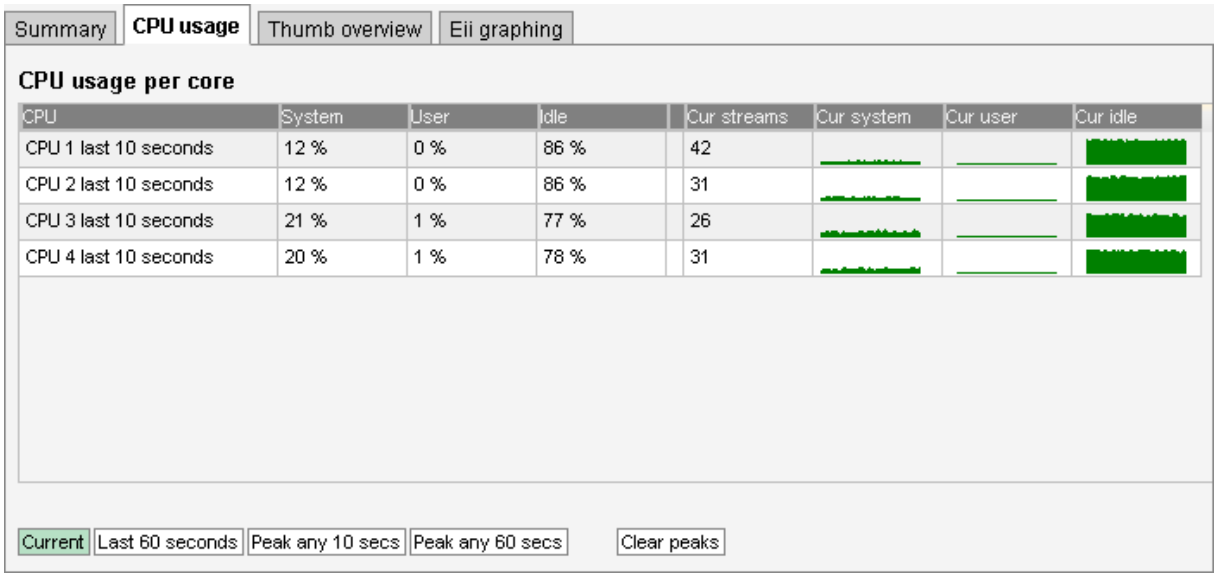
OTT info

Channels:	The number of enabled OTT channels.
Profiles:	The total number of profiles in the enabled OTT channels.

At the very bottom of the Summary page, an overview of the Ethernet network interfaces on the VB330-SW are displayed.

Network interfaces	
Interface:	The ID of the selected network interface.
Link:	Indicates whether the interface is connected.
Description:	Provides a human-readable description of the interface, if available[2].
IPv4 address:	Lists the IPv4 address and netmask of the network interface, if set.
IPv6 address:	Lists the IPv6 address and netmask of the network interface, if set.
Timestamp:	Indicates whether the network interface supports hardware timestamping for precise measurements, or if kernel timestamping is used.

5.1.2 Main — CPU usage



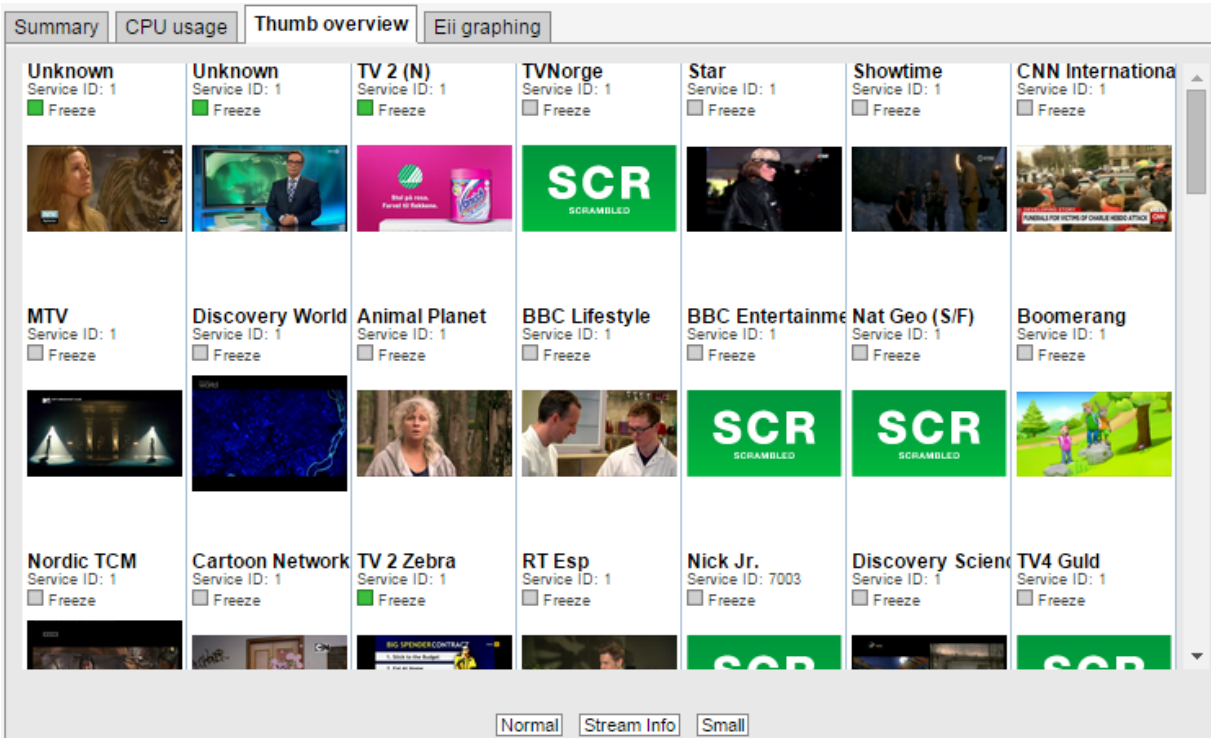
The **CPU usage** view is meant for troubleshooting performance issues in case of excessively high traffic load.

Three internal performance indicators (System, User and Idle) are displayed as percentage numbers and also graphed for the last minute. Issues can potentially arise if the System indicator becomes high (>80%).

The **CPU usage** view displays CPU usage of the 10G Software Probe. To view the CPU usage averaged over the last 10 seconds click the **Current** button. To view the usage averaged over the last 60 seconds click the **Last 60 seconds** button. Clicking the **Peak any 10 secs** or **Peak any 60 seconds** button will display the historical maximum value for an averaging period of 10 s and 60 s respectively. To clear peak values click the **Clear peaks** button.

[2] A description can be set using the command `ip link set` *interfacename* `alias "`*Description*`"`

5.1.3 Main — Thumb overview



The **Thumb overview** view displays a mosaic of all decoded thumbnails. By default the **Normal** mode is used. Placeholder images will be displayed if thumbnailing has not been enabled in the **Setup — Params** view, indicating the type of stream being received.

If the **Small** button is clicked the **Thumb overview** view will display service names and thumbs only, allowing more thumbnails to be displayed in a view. To display the stream address and name (as defined in the **Multicasts — Streams** and **OTT — Channels** views) click the **Stream info** button.

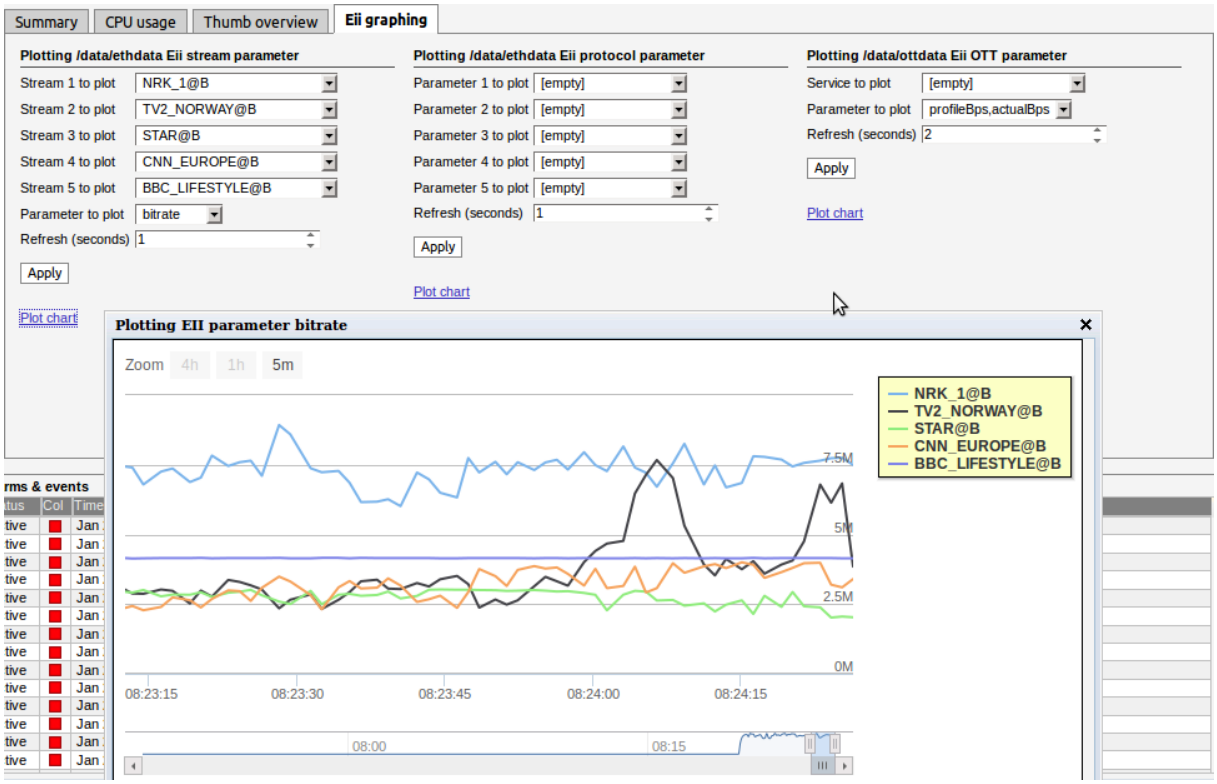
The following information is displayed for each stream:

Thumb overview	
Service name:	Shows the name defined for the TV service in the SI service descriptor. If no SI is present in the stream the service id will be shown.
Service id:	For TS services, the ID of the selected service within a transport stream.
Type:	For non-TS services, the service type is displayed.
Freeze-frame status:	If the probe has been licensed with the Content Extraction and Alarming option, status bulbs are displayed indicating the current freeze-frame and color-freeze status for the streams. **White:** Unknown (typically due to the VB330-SW being unable to decode video) **Grey:** freeze-frame detection is disabled. **Green:** freeze-frame detection is enabled, no freeze-frame is detected. **Yellow:** freeze-frame detection is enabled. Two consecutive equal frames have been detected, but the freeze-frame error timeout value has not been exceeded. **Red:** freeze-frame is enabled. Freeze-frame has been detected and the freeze-frame error timeout value has been exceeded, thus resulting in an alarm.

The **Thumbs Details** pop-up view is accessed by clicking a thumb in the **Thumb overview** view. For more information about the details displayed in the **Thumbs Details** pop-up see chapter 5.4 for multicast streams, and chapter 5.3.2 for OTT channels. Note that thumbnails are only decoded automatically if the **Extract thumbnails** option has been enabled in the associated OTT or multicast setup, or if content check alarming (Content Extraction and Alarming option) has been enabled in the ETR threshold template. To decode the thumbnail manually, open the **Thumbs Details** view. The same pop-up details are displayed as when opened from the **ETR 290 — Services** view.

Clicking the **Close** button will close the view.

5.1.4 Main — Eii graphing



Eii is short for External Integration Interface and constitutes a set of XML files accessible through the VB330-SW web server interface for machine access to measurement data.

Portions of the Eii interface are available in this view for simple trend graphing over arbitrary long time by the web browser.

The screenshot shows the bandwidth of two IP streams being graphed by sampling the Eii interface every 2 seconds. The graph is stored in the client web browser for as long as the graph window remains open. The graph starts again with zero history if the window is closed and then opened again.

Eii stream parameter

Using the **Eii stream parameter** plot, it is possible to plot parameters from up to five IP streams. Select the streams in the **Stream N to plot** (where N is 1 through to 5) drop-downs and the parameter in the **Parameter to plot** dropdown.



Eii stream parameters	
bitrate:	Bitrate (bits per second)
rtp_drops:	Number of dropped IP frames due to network errors
iat_avg:	Average Inter-Arrival Time
cc_errs:	The number of discontinuities detected

Refresh (seconds) selects how often samples are read and plotted on the graph. Click **Apply** to store the parameters and then click the **Plot chart** link to open the chart.

Eii protocol parameter

Using the **Eii protocol parameter** plot, it is possible to plot up to five network interface parameters. Select the parameters in the **Parameter N to plot** (where N is 1 through to 5) drop-downs.

Eii protocol parameters	
vlanTaggedPerc:	Percentage of frames being VLAN tagged
ipFragPerc:	Percentage of frames being IP fragmented
eth0txBitr:	Total TX bitrate including units on first data interface
eth0rxBitr:	Total RX bitrate including units on first data interface
udpUnicastBitr:	Bitrate of the unicast traffic
udpMulticastBitr:	Bitrate of the multicast traffic
udpUnicastStreams:	Number of UDP unicast streams present
udpMulticastStreams:	Number of UDP multicast streams present
copPayloadBitr:	Bitrate of FEC protected payload
copFec1Bitr:	Bitrate of the FEC columns
copFec2Bitr:	Bitrate of the FEC rows
copCorrected:	IP packets correctable by the FEC
copUncorrected:	IP packets not correctable by the FEC
copErrors:	FEC packets with errors

Refresh (seconds) selects how often samples are read and plotted on the graph. Click **Apply** to store the parameters and then click the **Plot chart** link to open the chart.

Eii OTT parameter

Using the **Eii OTT parameter** plot, it is possible to plot analysis parameters from any of the monitored OTT channel. Select the channel in the **Service to plot** drop-down and the parameter in the **Parameter to plot** dropdown.

Eii OTT parameters	
profileBps,actualBps:	Plots both the **profileBps** and **actualBps** parameters
profileBps:	Bitrate of this profile as listed in meta-data (bits per second)

actualBps:	Bitrate of this profile calculated from downloaded chunk (bits per second)
chunkDur:	Last chunk length (seconds)
firstByte:	Time to first byte (milliseconds)
downloadDur:	Time to download chunk (seconds)
chunkSize:	Size of downloaded chunk (bytes)

Refresh (seconds) selects how often samples are read and plotted on the graph. Click **Apply** to store the parameters and then click the **Plot chart** link to open the chart.

Please refer to the separate Eii documentation on the customer area of the Bridge Technologies website for further details.

5.2 Alarms

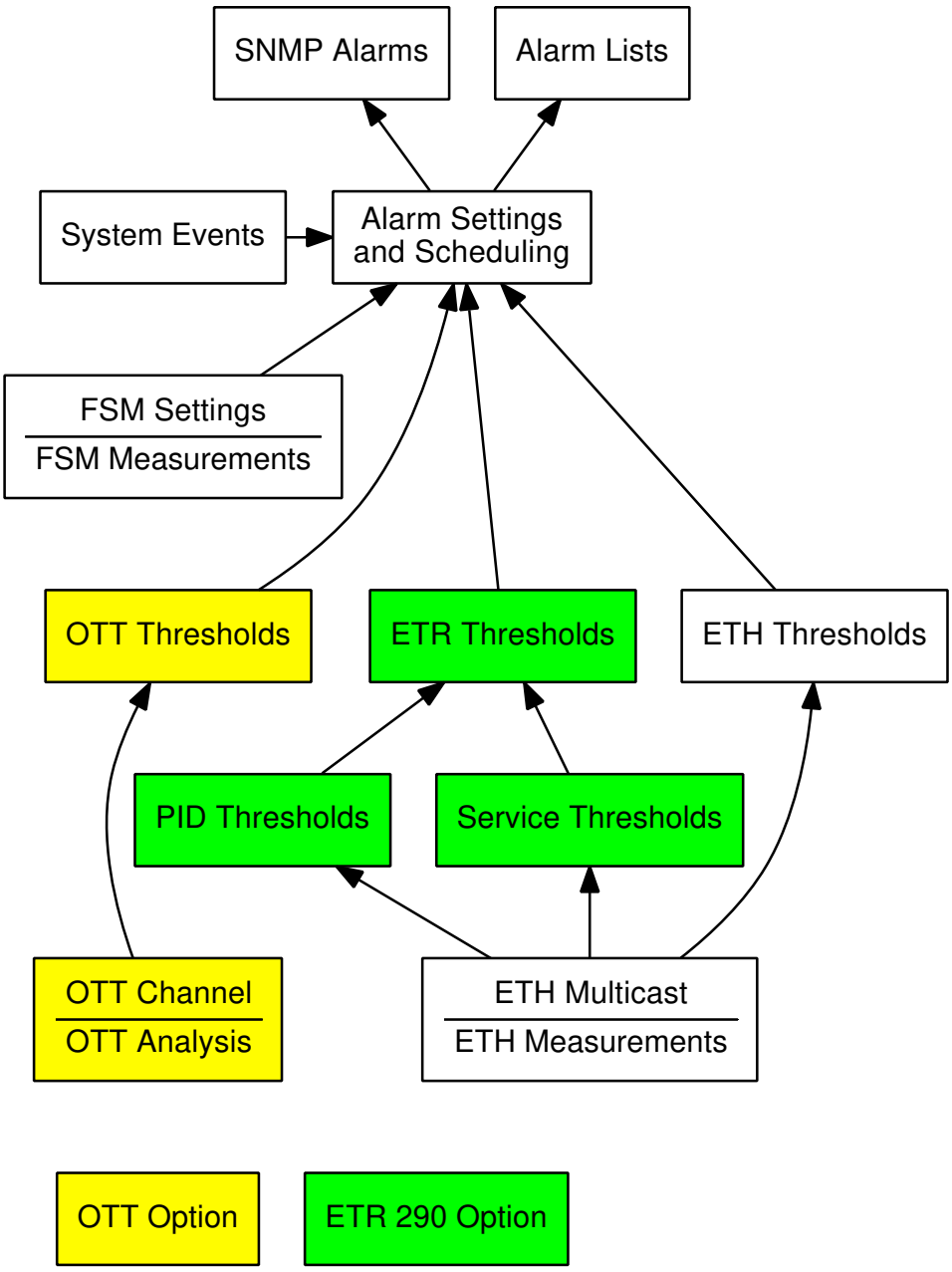


Figure 5.1: Alarm handling in the 10G Software Probe.

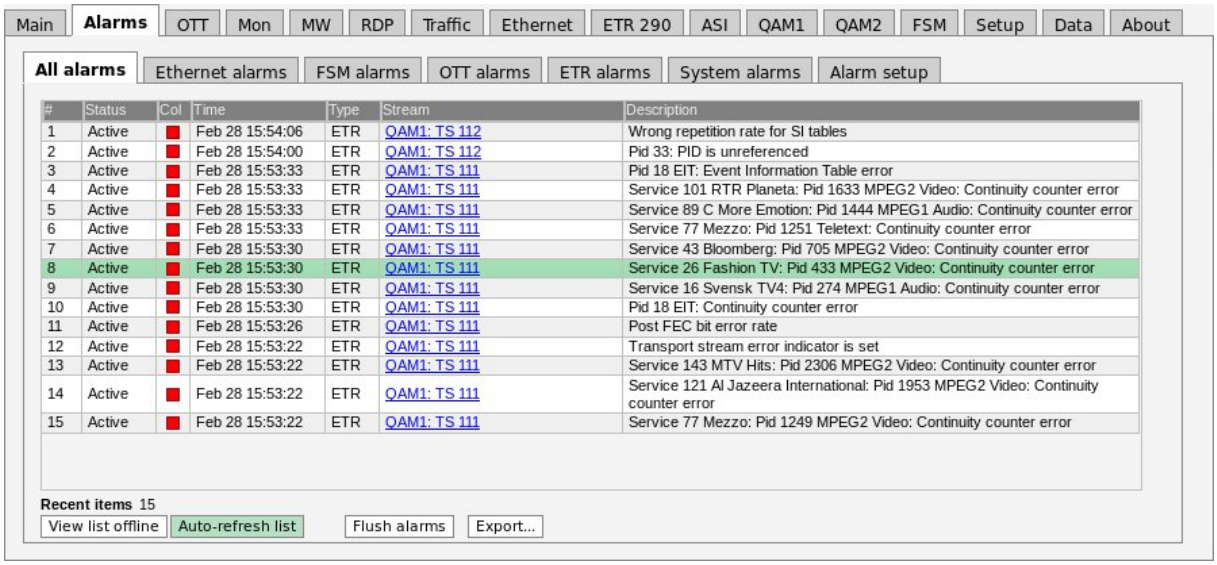
Figure 5.1 shows an overview of the alarm handling in the 10G Software Probe. It is useful to obtain an understanding of the alarm processing of the 10G Software Probe – in particular how threshold settings and alarm setup will affect alarm handling.

The 10G Software Probe continuously compares measurement data with user defined thresholds in order to generate alarms. These alarms are further checked against the settings defined in the **Alarms — Alarm setup** view, and the resulting alarms are presented in the alarm lists. These alarms will also be sent as

SNMP traps to support third party management systems. Refer to Appendix: VB330-SW Versus VBC Alarms for a description of alarm handling in the VBC Controller.

The 10G Software Probe distinguishes between events and alarms. The ETR software module will always generate alarms and the Systems software module will always generate events. The Ethernet software module will by default generate events for errors that are resolved within 1 second, otherwise it will generate alarms. This can be overridden by checking the 'Treat Ethernet events as alarms' box in the **Setup — Params** view. The OTT module generates alarms only.

5.2.1 Alarms — All Alarms



The **Alarms** view gives the user the possibility of viewing alarms according to type or as one combined list. The individual alarm lists can hold the number alarms indicated below independently of each other, meaning that one may become full without affecting the other lists.

Alarm list capacity	
Ethernet alarms (ETH)	4000 alarms
Full Service Monitoring (FSM)	100 alarms
Over The Top Television (OTT)	100 alarms
ETSI TR 101 290 Analysis (ETR)	400 alarms
System alarms (SYS)	100 alarms

If **Auto-refresh list** is selected, the alarm list will be continuously updated with new alarms. Active alarms are always located at the top of the list.

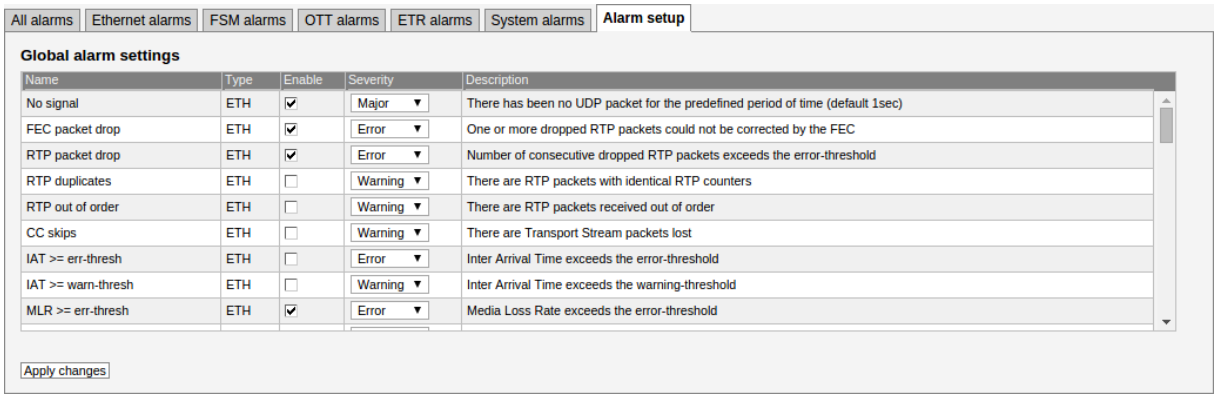
Clicking the **View list offline** button gives the user the opportunity to view the complete alarms and events list. By clicking one of the blue information icons leftmost in the offline list, a detailed alarm description can be viewed. The search field in the upper right corner of the view allows the user to type a text string and the alarm list is updated to display only streams and alarms matching the specified text. To update the offline alarm list click the **Auto-refresh list** button and then go back to the offline mode.

The alarm lists can be deleted by clicking the **Flush alarms** button. However it should be noted that this action will permanently clear the alarm lists — they cannot be restored.



The **Export** button enables export of the corresponding alarm list as an XML file. This file will open in a new window.

5.2.2 Alarms — Alarm setup



The **Alarm setup** represents the final filtering stage for VB330-SW alarms. The user selects whether an alarm should be enabled or ignored, and associates an error severity level with each alarm, and associates an error severity level with each alarm. When changes have been made to alarm settings click the **Apply changes** button for changes to take effect.

Figure 5.1 gives an overview of the total alarm handling of a 10G Software Probe. The settings in the **Alarm setup** view are represented by the **Alarm Settings** box in this figure.

Note that the probe alarm handling will also depend on the threshold template settings defined by the user in the **Multicasts — Ethernet thresh.**, **ETR 290 — ETR thresh.**, **ETR 290 — PID thresh.**, **ETR 290 — Service thresh.**, and **OTT — Thresholds** views.

Also note that only enabled alarms are shown in the alarm lists and forwarded as SNMP traps. Enabling or disabling 10G Software Probe alarms does however not affect the alarms presented by the VBC. Refer to Appendix: VB330-SW Versus VBC Alarms for a description of the VB330-SW versus VBC alarm handling.

The following alarm severity levels may be selected:

OK:	If enabled, the alarm will be present in the alarm list, color green
Warning:	If enabled, the alarm will be present in the alarm list, color yellow
Error:	If enabled, the alarm will be present in the alarm list, color orange
Major:	If enabled, the alarm will be present in the alarm list, color red
Fatal:	If enabled, the alarm will be present in the alarm list, color black

The following alarms and events are configured:

	ETH (Ethernet) alarms	
No signal:	There has been no UDP packet for the predefined period of time (default 1sec)	Default: Enabled, severity Major
FEC packet drop:	One or more RTP packets could not be corrected by the FEC	Default: Enabled, severity Error

RTP packet drop:	Number of consecutive dropped RTP packets exceeds the error-thresholds – only available if RTP headers are present	Default: Enabled, severity Error
RTP duplicates:	Number of RTP packets with identical RTP counters – only available if RTP headers are present	Default: Disabled, severity Warning
RTP out of order:	There are RTP packets received out of order – only available if RTP headers are present	Default: Disabled, severity Warning
CC skips:	Number of transport stream discontinuities due to packet loss. Note that the CC skips number does not necessarily equal the number of lost packets, as several consecutive packets lost will be counted as one CC skip.	Default: Disabled, severity Warning
IAT >= err-thresh:	The Inter-packet Arrival Time exceeds the error threshold	Default: Disabled, severity Error
IAT >= warn-thresh:	The Inter-packet Arrival Time exceeds the warning threshold	Default: Disabled, severity Warning
MLR >= err-thresh:	The Media Loss Rate exceeds the error-threshold	Default: Enabled, severity Error
MLR >= warn-thresh:	The Media Loss Rate exceeds the warning-threshold	Default: Disabled, severity Warning
TTL changed:	The Time-To-Live field is changing	Default: Enabled, severity Error
TOS changed:	The Type-Of-Service field is changing	Default: Enabled, severity Error
Multiple mcast sources:	There are multiple multicast sources	Default: Enabled, severity Error
Mcast source changed:	The multicast source changed to one of the valid multicast sources specified by the operator	Default: Enabled, severity Error
Bitrate overflow:	The net stream bitrate exceeds the maximum bitrate Ethernet threshold value specified by the operator	Default: Enabled, severity Error
Bitrate underflow:	The net stream bitrate goes below the minimum bitrate Ethernet threshold value specified by the operator	Default: Enabled, severity Error

FSM alarms

Full service monitoring:	No reply was obtained within time-out period for the configured FSM service	Default: Enabled, severity Major

ETR (ETR 290) alarms		
TS Sync:	No TS Sync (no signal)	Default: Enabled, severity Major
Sync byte:	Sync byte error, sync byte not 0x47	Default: Enabled, severity Major
PAT:	Program Association Table error	Default: Enabled, severity Major
Continuity:	Continuity counter error	Default: Enabled, severity Major
PMT:	Program Map Table error	Default: Enabled, severity Major
PID:	PID is missing	Default: Enabled, severity Major
Transport:	Transport stream error indicator is set	Default: Enabled, severity Major
CRC:	Table checksum error	Default: Enabled, severity Major
PCR:	Program Clock Reference error	Default: Enabled, severity Major
PCR Accuracy:	Program Clock Reference accuracy error (PCR jitter)	Default: Enabled, severity Major
PTS:	Presentation Time Stamp error	Default: Enabled, severity Major
CAT:	Conditional Access Table error	Default: Enabled, severity Major
NIT:	Network Information Table error	Default: Enabled, severity Major
SI Rep Rate:	Wrong repetition rate for SI tables	Default: Enabled, severity Major
Unref PID:	PID is unreferenced	Default: Enabled, severity Major
SDT:	Service Description Table error	Default: Enabled, severity Major
EIT:	Event Information Table error	Default: Enabled, severity Major
RST:	Running Status Table error	Default: Enabled, severity Major

TDT:	Time Date Table error	Default: Enabled, severity Major
MGT:	Master Guide Table error (ATSC mode)	Default: Enabled, severity Major
VCT:	Virtual Channel Table error (ATSC mode)	Default: Enabled, severity Major
PIM/PNM:	PIM/PNM error (ATSC mode)	Default: Enabled, severity Major
RRT:	Region Rating Table error (ATSC mode)	Default: Enabled, severity Major
ATSC EIT:	ATSC EIT Table error (ATSC mode)	Default: Enabled, severity Major
STT:	System Time Table error (ATSC mode)	Default: Enabled, severity Major
ETT:	Extended Text Table error (ATSC mode)	Default: Enabled, severity Major
CA System:	CA System error	Default: Enabled, severity Major
PID min. bitr.	PID minimum bitrate below threshold	Default: Enabled, severity Major
PID max. bitr.	PID maximum bitrate exceeds threshold	Default: Enabled, severity Major
PID checks:	PID check error	Default: Enabled, severity Major
Service min. bitr.	Service minimum bitrate below threshold	Default: Enabled, severity Major
Service max. bitr.	Service maximum bitrate exceeds threshold	Default: Enabled, severity Major
Service checks:	Service check error	Default: Enabled, severity Major
MIP:	Megaframe Insertion Packet error	Default: Enabled, severity Major
Content:	Content check error (checking of audio and video)	Default: Enabled, severity Major
Reference:	Reference check error (comparing the stream with a Gold TS)	Default: Enabled, severity Major
Gold TS:	Error found while comparing the stream with the stored Gold TS snapshot)	Default: Enabled, severity Major
Interface overflow:	Input interface overflow error. Means that the probe is overloaded and can not properly analyze the signals.	Default: Enabled, severity Major

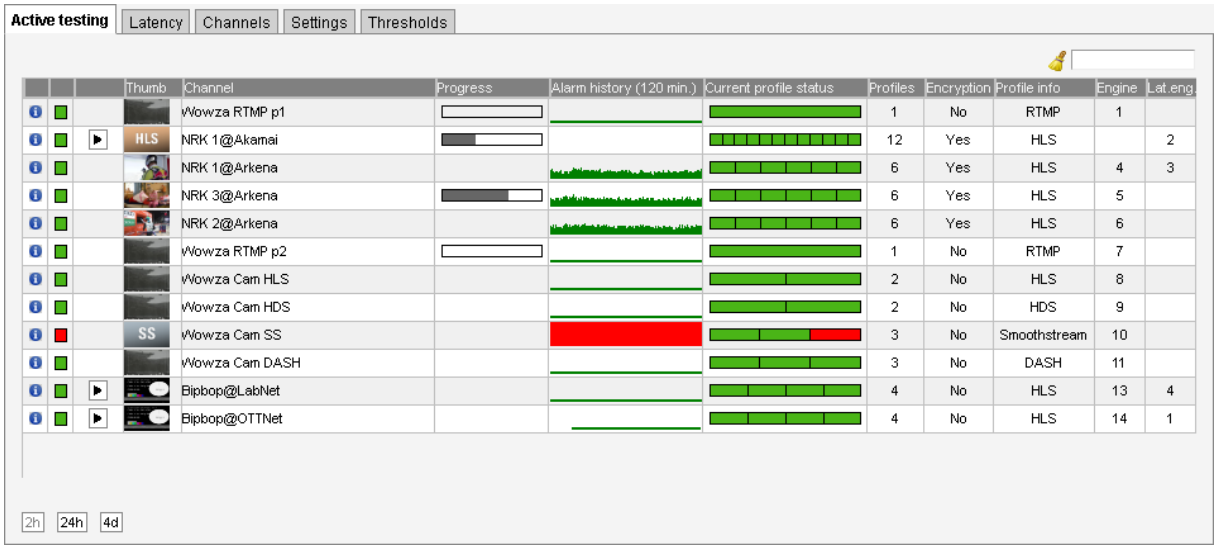
	SYS (System) events	
[Critical system errors]:	Critical system errors preventing the 10G Software Probe from operating correctly	Default: Enabled, severity 'Fatal'
[System errors]:	Enable this to view all system errors	Default: Enabled, severity 'Major'
[System info]:	Enable this to view system information messages	Default: Enabled, severity 'OK'

	OTT Alarms	
The number of profiles changed:	The number of profiles flagged in the manifest file changed	Default: Enabled, severity 'Warning'
Profile stream type changed:	The stream type of the profile changed in the manifest	Default: Enabled, severity 'Warning'
Minimum profiles	The channel has less profiles than specified in the threshold	Default: Enabled, severity Warning
Download bitrate low:	The download duration time exceeds the OTT bitrate threshold. The bitrate threshold is part of the OTT threshold template defined in the **OTT — Thresholds** view. A threshold template is assigned to a stream in the **OTT — Channels** view.	Default: Disabled, severity Warning
Download bitrate too low:	The download duration time exceeds the OTT chunk duration time	Default: Enabled, severity Error
Manifest size:	The manifest file size exceeds the OTT manifest size threshold	Default: Enabled, severity Warning
Actual bitrate:	The actual measured bitrate does not match the profile bitrate specified in the manifest file	Default: Enabled, severity Warning
Download timeout:	The download time exceeds twice the chunk duration time	Default: Enabled, severity Major
Address resolve error:	Unable to resolve address name	Default: Enabled, severity 'Error'
Connection failed:	Connection failed	Default: Enabled, severity 'Error'
Send error:	Could not send data to host	Default: Enabled, severity 'Error'
Receive error:	Could not receive data from host	Default: Enabled, severity 'Major'

Empty reply:	Response did not contain any data in body	Default: Enabled, severity 'Major'
HTTP error:	Invalid HTTP response	Default: Enabled, severity 'Major'
HTTP redirect error:	HTTP 3xx redirection error	Default: Enabled, severity 'Major'
HTTP client error:	HTTP 4xx client error	Default: Enabled, severity 'Major'
HTTP server error:	HTTP 5xx server error	Default: Enabled, severity 'Major'
Static manifest:	Manifest file unchanged for longer than configured threshold	Default: Enabled, severity Major
Manifest parse error:	Failed to parse manifest file. Invalid format	Default: Enabled, severity 'Major'
Unknown manifest:	Cannot recognize manifest XML format	Default: Enabled, severity 'Fatal'

5.3 OTT (Option)

5.3.1 OTT — Active testing



The OTT option enables monitoring of up to 500 OTT channels. Up to 50 OTT engines (depends on license) can operate in parallel, and each engine licensed allows any channels to be analyzed. Each engine analyses channels in series and can be configured with any number of channels up to the maximum allowed by the license.

The 10G Software Probe will parse a channel's manifest file, and for a live channel one of the latest chunks in each OTT profile's chunk sequence will be analyzed. The engine then moves on to the next OTT channel in the channel list defined by the user. For a VoD channel the OTT engine will analyze all chunks in the VoD file, one in each round-robin loop.

If manifest file parsing or chunk analysis reveals an error, an alarm will be raised. Note that some alarms depend on user defined threshold values. Alarms must also be enabled in the **Alarm — Alarm setup** view.

Thumbnail decoding is available for **non-encrypted** HLS, HDS, DASH and RTMP channels, as well as some types of encrypted HLS channels.

The following OTT information is displayed in the Active testing view:

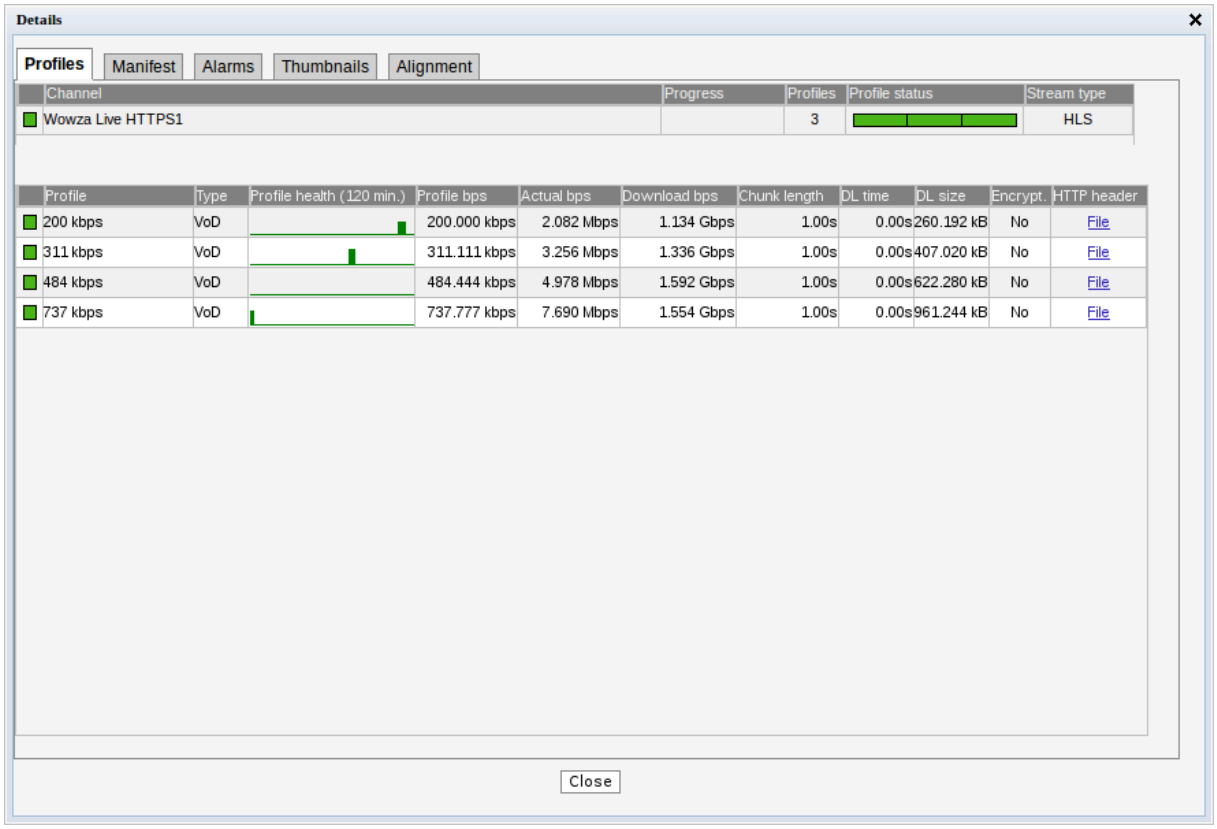
OTT channels	
Status bulb:	A bulb indicates the current status of the channel, i.e. the most severe profile status.
Thumb:	If the selected channel is of type HLS, HDS, DASH or RTMP a thumbnail of the content will be decoded and updated. Thumbnail decoding is a process asynchronous of the channel analysis and therefor should not be expected to be updated at the same time. The main purpose of the thumbnails is to provide brief information about the channel contents.
Channel:	The channel name defined by the user and linked to a URL in the **OTT — Channels** view.
Progress:	Channels will be analyzed sequentially, and the progress bar shows which channel is currently being monitored and how analysis is progressing.

Alarm history:	A bar graph showing alarm severity history. It can show the last 120 minutes, 24 hours or four days. To switch between the graphs, press the “24h”, “2h” or “4d” button on the left under the channel list. Each bar color represents the alarm severity level as configured under **Alarms — Alarm setup**.
Current profile status:	The channel health bar displays the current status for individual channel profiles. Profiles are separated by vertical black lines. Colors indicate profile alarm status: • Green: OK • Yellow: Warning • Orange: Error • Red: Major • Black: Fatal
Profiles:	The number of profiles associated with a channel.
Encryption:	Scrambling information is resolved from the profile manifest. If the profile is scrambled the encryption field will read *Yes*. If the profile is transmitted in clear the encryption field will read *No*.
Profile info:	Channel and profile information is resolved from the manifest files. At channel level the OTT format is displayed (Smoothstream, HLS, Adobe HDS, MPEG DASH or SHOUTcast). At profile level the profile bitrate is displayed.
Engine:	Indicates which OTT engine is assigned to what channel. The 10G Software Probe can be licensed with anywhere from 1 up to 50 OTT engines. Each engine is capable of handling any number of channels.
Lat.eng.:	Indicates which OTT latency engine has been automatically assigned to this channel. This column is only displayed if latency engines have been configured in the **OTT — Settings** view, and will only contain numbers for channels configured to perform latency measurements. See chapter 5.3.3 for more details.

5.3.2 OTT — Details

Click the blue information button on a channel to open the details window. This window provides detailed information about the status and alarms on all the profiles for the selected channel. The same pop-up can be opened from the **Main — Thumb Overview** view, see chapter 5.1.3 for more information.

5.3.2.1 OTT — Details — Profiles



The **Profiles** view in this pop-up consists of two tables detailed below:

The following information relevant for the overall OTT channel is shown in the first part of the **Details — Profiles** pop-up window:

Channel	
Channel:	The channel name defined by the user and linked to a URL in the **OTT — Channels** view. A bulb indicates the current status of the channel, i.e. the most severe profile status.
Progress:	Channels will be analyzed sequentially, and the progress bar shows which channel is currently being monitored and how analysis is progressing.
Profiles:	The number of profiles associated with a channel.
Profile status:	The channel health bar displays the current status for individual channel profiles. Profiles are separated by vertical black lines. Colors indicate profile alarm status: • Green: OK • Yellow: Warning • Orange: Error • Red: Major • Black: Fatal
Stream type:	Channel and profile information is resolved from the manifest files. At channel level the OTT format is displayed (Smoothstream, HLS, Adobe HDS, MPEG DASH or SHOUTcast).



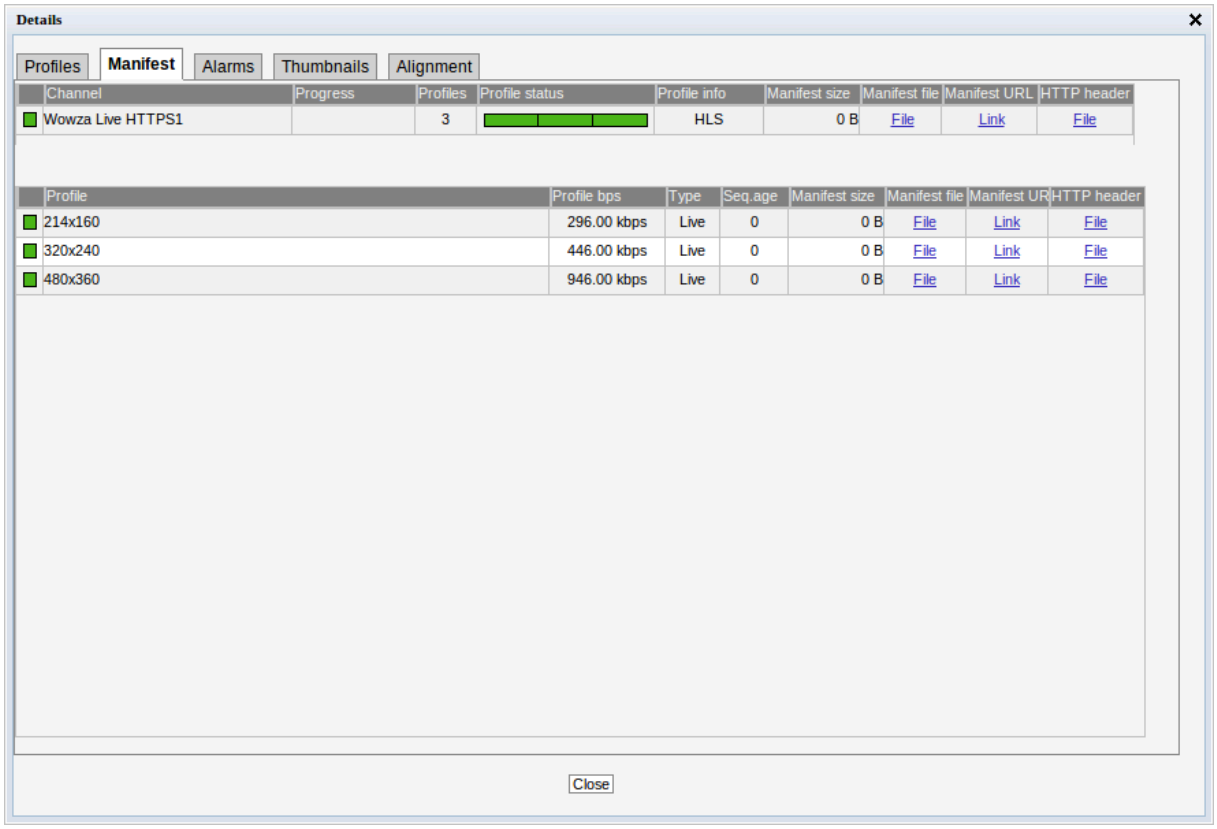
In the same view below the table for the overall channel a more detailed view per **channel profile** is shown with the following information in it:

Profiles		
Profile:		The name of the OTT profile as flagged in the manifest files.
Type:		**Live** for live content or **VoD** for stored content. The distinction between the two is done based on whether the profile sequence numbers update or not.
Profile health:	*	A timeline graph display of a combined bitrate and alarm representation for individual profiles. Refer to Appendix C for a description of these graphs. The timeline duration is either 2 or 24 hours, and the graph resolution is one minute for the 2 hour graph, and twelve minutes for the 24 hour graph.
Profile bps:	*	The profile nominal bandwidth as flagged in the manifest files.
Actual bps:	*	The actual profile bitrate, i.e. the chunk size (megabits) divided by the chunk length (seconds). The actual profile bitrate should match the manifest bitrate specification within limits defined by the user in the OTT thresholds template associated with a channel. Otherwise an alarm will be raised.
Download bps:	*	The download bitrate, i.e. the chunk size (megabits) divided by the download time (seconds).
Chunk length:	*	The profile chunk length (seconds) specified in the manifest file.
Download time:	*	The actual profile chunk download time (seconds).
First byte:	*	The time (in seconds) before the first payload data byte was received.
Download size:	*	The actual profile chunk size (bytes).
Encrypt.:		**Yes** or **No** depending on whether the content for that profile is encrypted or not.
HTTP header:	*	The current HTTP header of the last chunk downloaded for that profile.

Note: Items marked with * are not available if the channel has been configured to only perform latency measurements (see chapter 5.3.3 for more details).



5.3.2.2 OTT — Details — Manifest



The **Manifest** view shows health information on the overall manifest file for the channel as well as for the manifest files for the individual profiles.

Channel	
Channel:	The channel name defined by the user and linked to a URL in the **OTT — Channels** view. A bulb indicates the current status of the channel, i.e. the most severe profile status.
Progress:	Channels will be analyzed sequentially, and the progress bar shows which channel is currently being monitored and how analysis is progressing.
Profiles:	The number of profiles associated with a channel.
Profile status:	The channel health bar displays the current status for individual channel profiles. Profiles are separated by vertical black lines. Colors indicate profile alarm status: • Green: OK • Yellow: Warning • Orange: Error • Red: Major • Black: Fatal
Profile info:	The type of stream is shown here. Apple **HLS**, Microsoft **Smoothstream**, Adobe **HDS**, **MPEG DASH** or **SHOUTcast**.
Manifest size:	The size in bytes of the main/top manifest file for the overall channel.
Manifest file:	Clickable URL for displaying the manifest file as text for the overall channel.

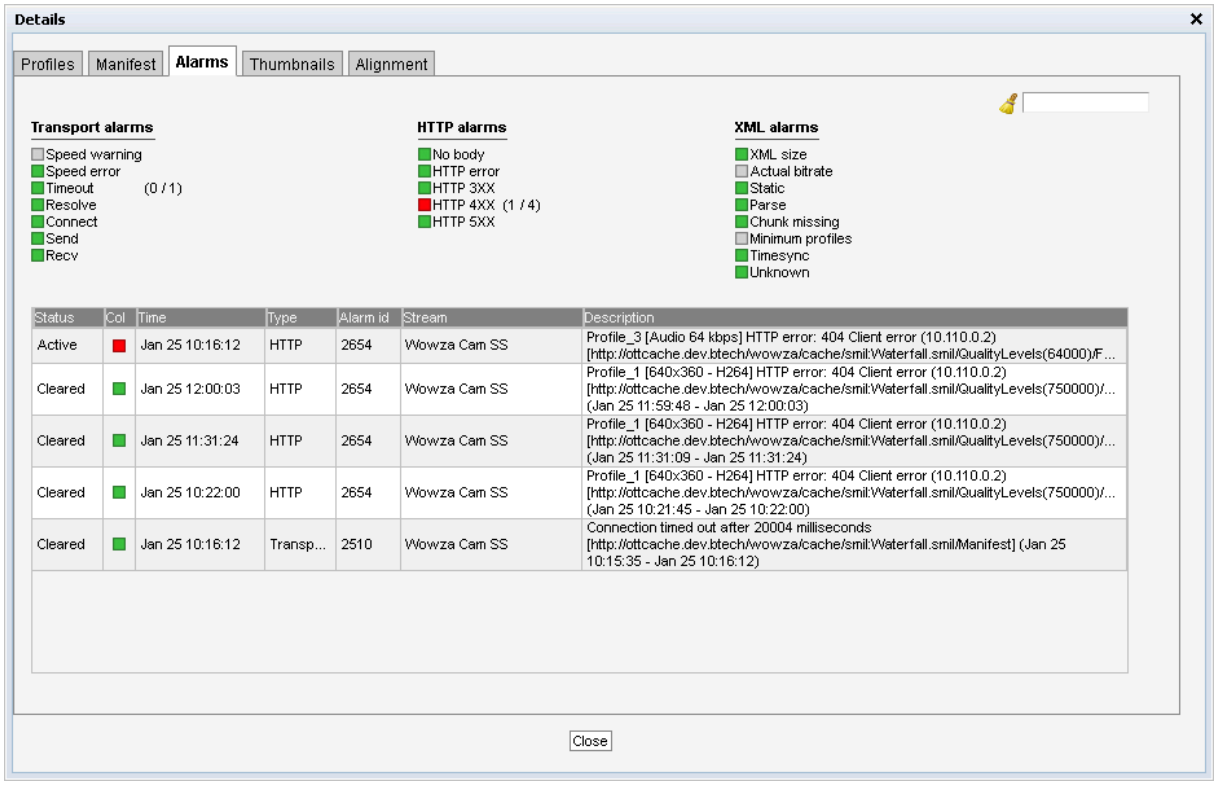


Manifest URL:	A clickable link to the current main/top manifest file for the overall channel.
HTTP header:	The current HTTP header of the main/top manifest file for the overall channel.

Just below the channel manifest information in the same window is the detailed manifest information per profile. This view contains the following information:

Profiles	
Profile:	The name of the OTT profile as flagged in the manifest files.
Profile bps:	The profile nominal bandwidth as flagged in the manifest files.
Type:	**Live** for live content or **VoD** for stored content. The distinction between the two is done based on the contents of the manifest file.
Seq.age:	The profile sequence shows how long it has been since the manifest was updated in whole seconds.
Manifest size:	The size in bytes of the manifest file for a particular profile.
Manifest file:	Clickable URL for displaying the manifest file as text for this particular profile.
Manifest URL:	Clickable URL to the profile manifest file.
HTTP header:	URL to HTTP header in text form for a particular profile manifest file.

5.3.2.3 OTT — Details — Alarms

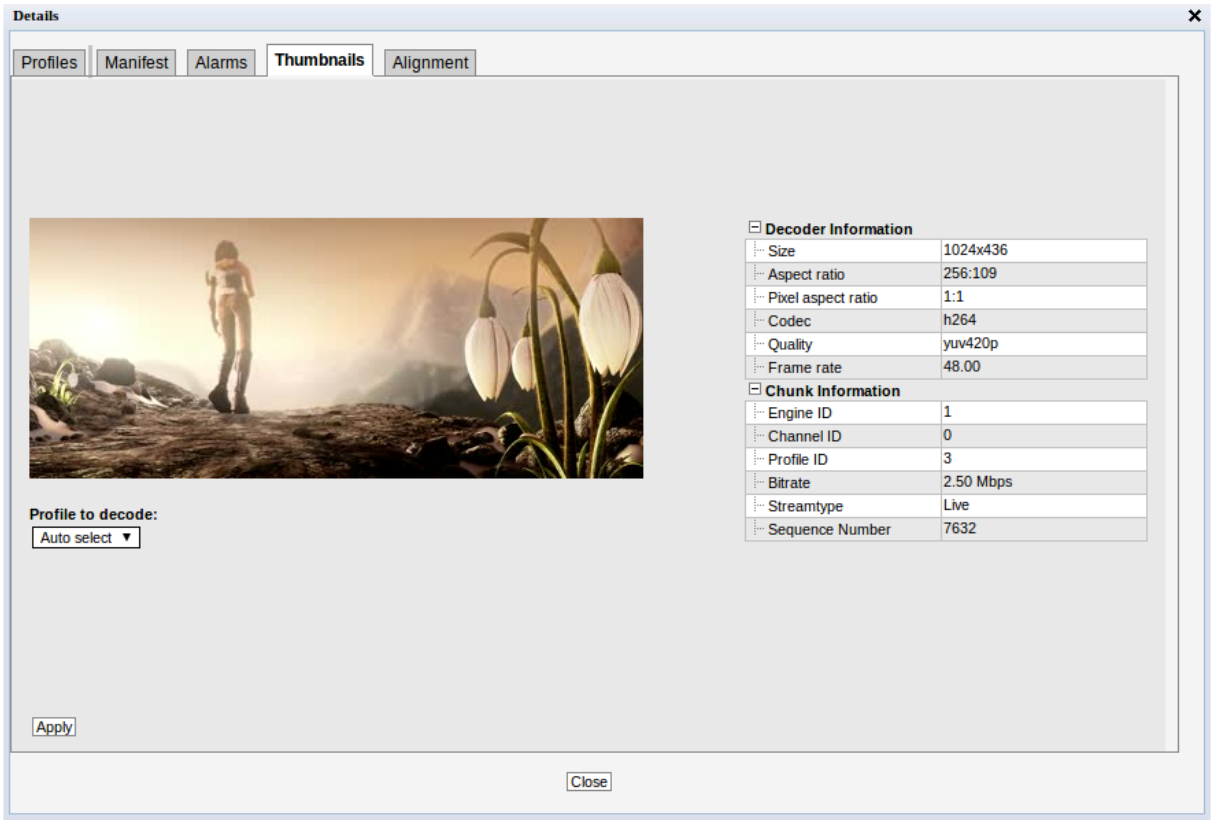


The **Details — Alarms** view gives an at-a-glance overview of any active OTT alarms for the selected channel. An alarm log for the selected channel is also provided here.

In the right corner of the pop-up window is a free text search field used to narrow down the entries in the alarm log.

The alarms are the same ones as explained for the **Alarms — Alarm setup** view, see chapter 5.2.2 for more information.

5.3.2.4 OTT — Details — Thumbnails



The Thumbnails tab will provide information about the current thumbnails in the channel.

The quality of the content in the selected profile can be viewed in the thumbnail section, and the user may alter the selected profile in the drop down list.

The section on the right hand side provides specific decoder and chunk information.

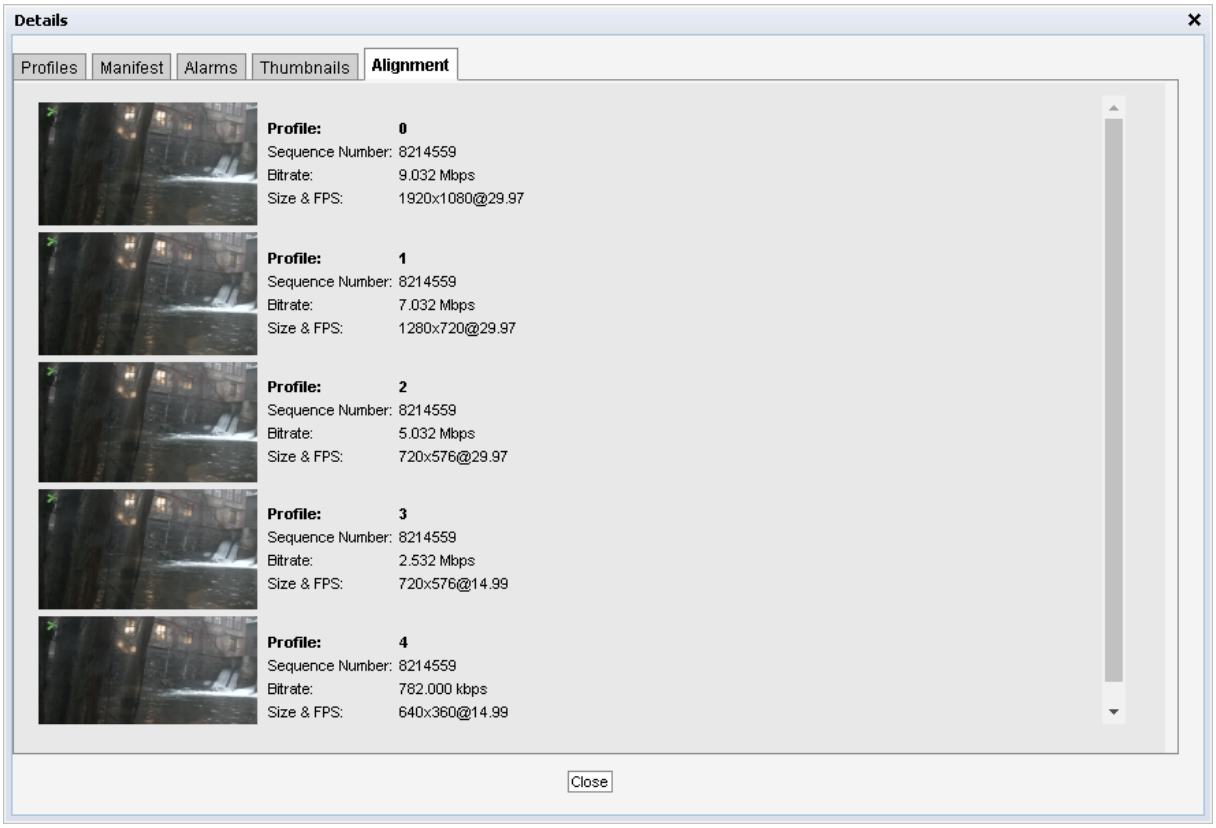
By pressing the **Apply** button without selecting a profile from the drop-down list the thumbnail will be switched to the default selection; **Auto select**. Auto select will select the profile with the highest bitrate and video data.

Decoder information	
Size:	The video picture size of the selected profile
Aspect ratio:	The video aspect ratio of the selected profile
Pixel aspect ratio:	The video pixel aspect ratio of the selected profile
Codec:	The video encoding format of the selected profile
Quality:	The video sampling format of the selected profile
Frame rate:	The video frame rate of the selected profile (Hz)

Chunk Information	
Engine ID:	The OTT engine monitoring the selected channel.
Channel ID:	The ID of selected channel corresponding to the list of channels defined by the user.

Profile ID:	The ID of the selected profile.
Bitrate:	Bitrate rate of the a chunk.
Streamtype:	The type of the stream detected; live or video on demand.
Sequence Number:	The sequence number of a chunk.

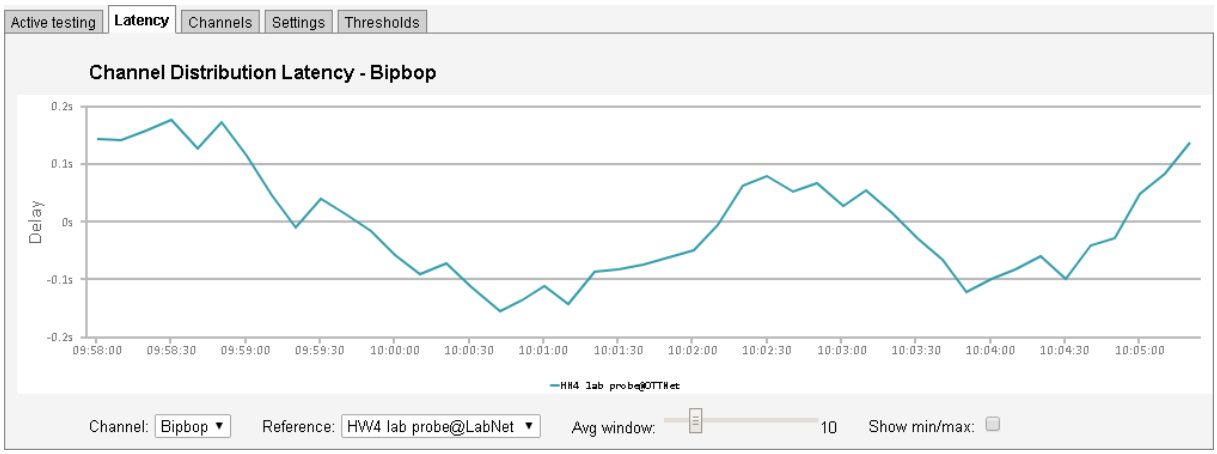
5.3.2.5 OTT — Details — Alignment



The Alignment tab gives the user a view of all the profiles for a selected channel with thumbnails and corresponding data.

Profile Alignment Information	
Profile:	This is a generated ID that identifies the OTT profile. The first profile listed is always the one with the highest signaled bitrate.
Chunk/Sequence Number:	The chunk or sequence number for the current thumbnail. This is either signaled in the stream, or generated by the VB330-SW. If the sequence numbers are highlighted in yellow, the thumbnails are not generated from the same chunk for all profiles, and may therefor appear to be out of synchronization.
Bitrate:	The signaled bitrate for this profile (bits/s).
Size & FPS:	Indicates the original video size (pixels) and the frame-rate (Hz).
Audio:	Indicates the audio channel layout.

5.3.3 OTT — Latency



The OTT Channel Latency Distribution feature makes it possible to measure the delay from when a chunk is available through different caches, compared to its origin.

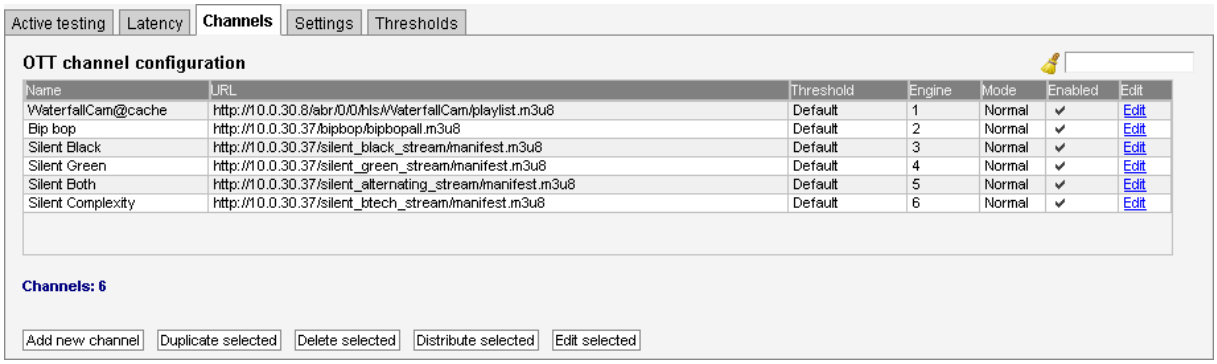
Before using this feature, you must set aside a number of OTT engines to exclusively measure the timings of one channel on one server. This is done in the **OTT — Settings** view. In general, you would need to use two Latency Engines per channel: one for the origin and one for the cache.

After selecting the number of Latency Engines, open the **OTT — Channels** view and add the channel from multiple sources (URLs), using the same base name, but different **classes**, e.g. TV1@**Origin** and TV1@**CDN**. Then set the **Measurement mode** to **Latency** if you are only interested in the timings from this server, or **Both** if you also want the traditional Active Testing measurements. Each added channel will use one dedicated Latency Engine, if you try setting **Latency** or **Both** and there is no free Latency Engine available, it will default back to **Normal**.

Once the configuration is finished, you are ready to use this feature. Select the channel to produce a latency graph for using the **Channel** drop-down. Then select which of the classes of the channel that is to be used as the reference in the **Reference** drop-down. This is used to calculate the time delta difference.

The graph will start off showing the difference in availability time of each chunk for the last minute and will build up history until displaying the last hour. Due to the nature of timing in different engines, these measurements are accurate down to ±0.5 seconds. To minimize these inaccuracies, a moving average is provided, smoothing the spikes. The sliding window can be manually controlled by moving the **Avg window** slider. It is also possible to display the minimum and maximum values by checking the **Show min/max** checkbox.

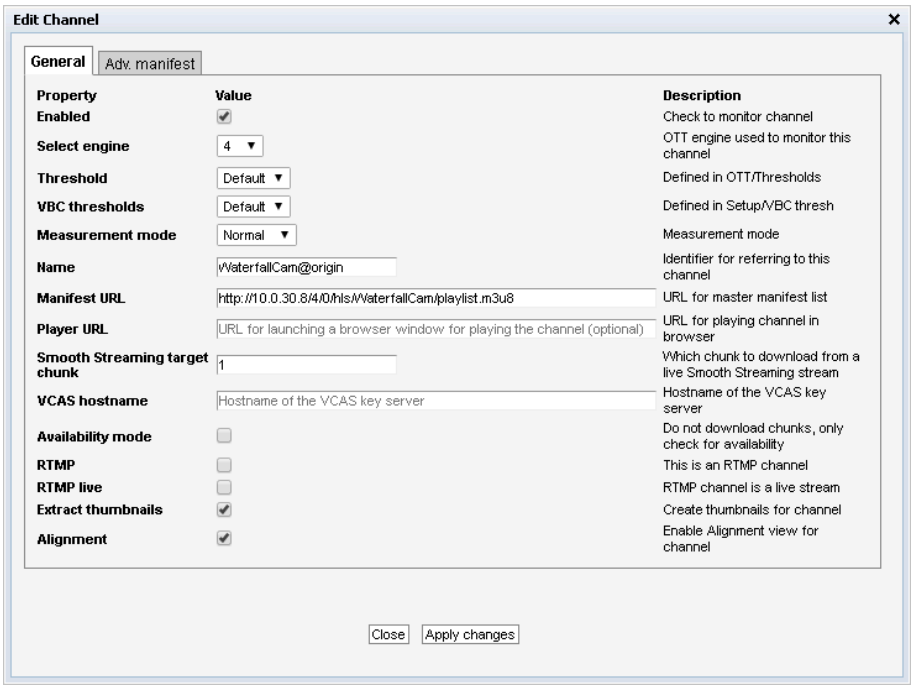
5.3.4 OTT — Channels



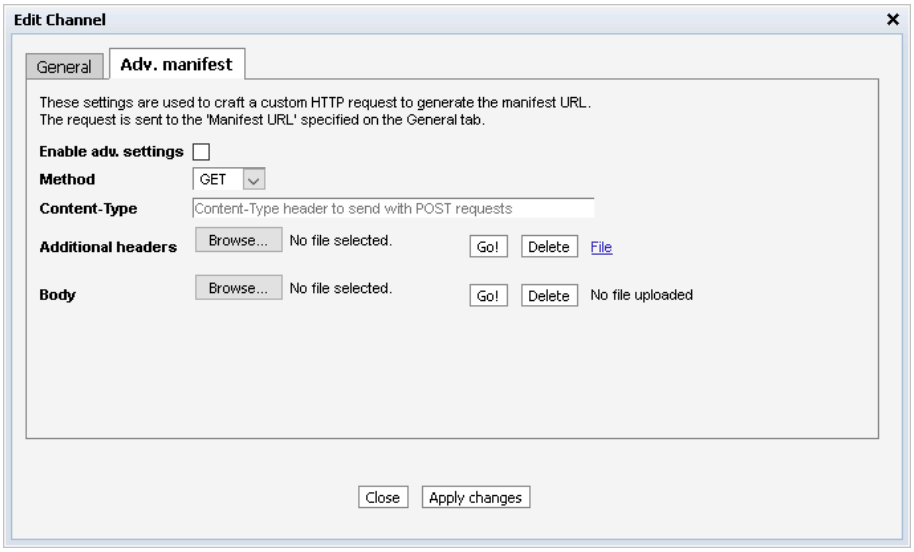
The OTT Channel Configuration list shows OTT channels configured by the user.

To add a channel to the list click the **Add new channel** button. This will open the **Edit channel** pop-up view, allowing the user to define channel parameters. A channel entry can be selected by clicking the channel; the list entry will be highlighted. Several list entries can be selected by using regular *Ctrl* + *click* functionality. Clicking the **Duplicate selected** button will open the **Edit channel** pop-up view with all channel parameters duplicated, except the channel name. Clicking **Delete selected** will delete the highlighted list entry. Clicking **Distribute selected** will distribute the selected channels across the licensed OTT engines (the VB330-SW can be licensed with up to 50 OTT engines). Clicking **Edit selected** will open the **Edit channel** pop-up view associated with the highlighted channel. Batch editing is supported; this is convenient if a new threshold template should be assigned to a number of channels or if monitoring of several channels should be enabled or disabled. Select the channels and click the **Edit selected** button. Parameters differing between channels will be indicated in the **Edit selected** pop-up view by an asterisk wildcard symbol.

The search field in the upper right corner of the view allows the user to type a text string, and the OTT channel list is updated to display only channels matching the specified text.



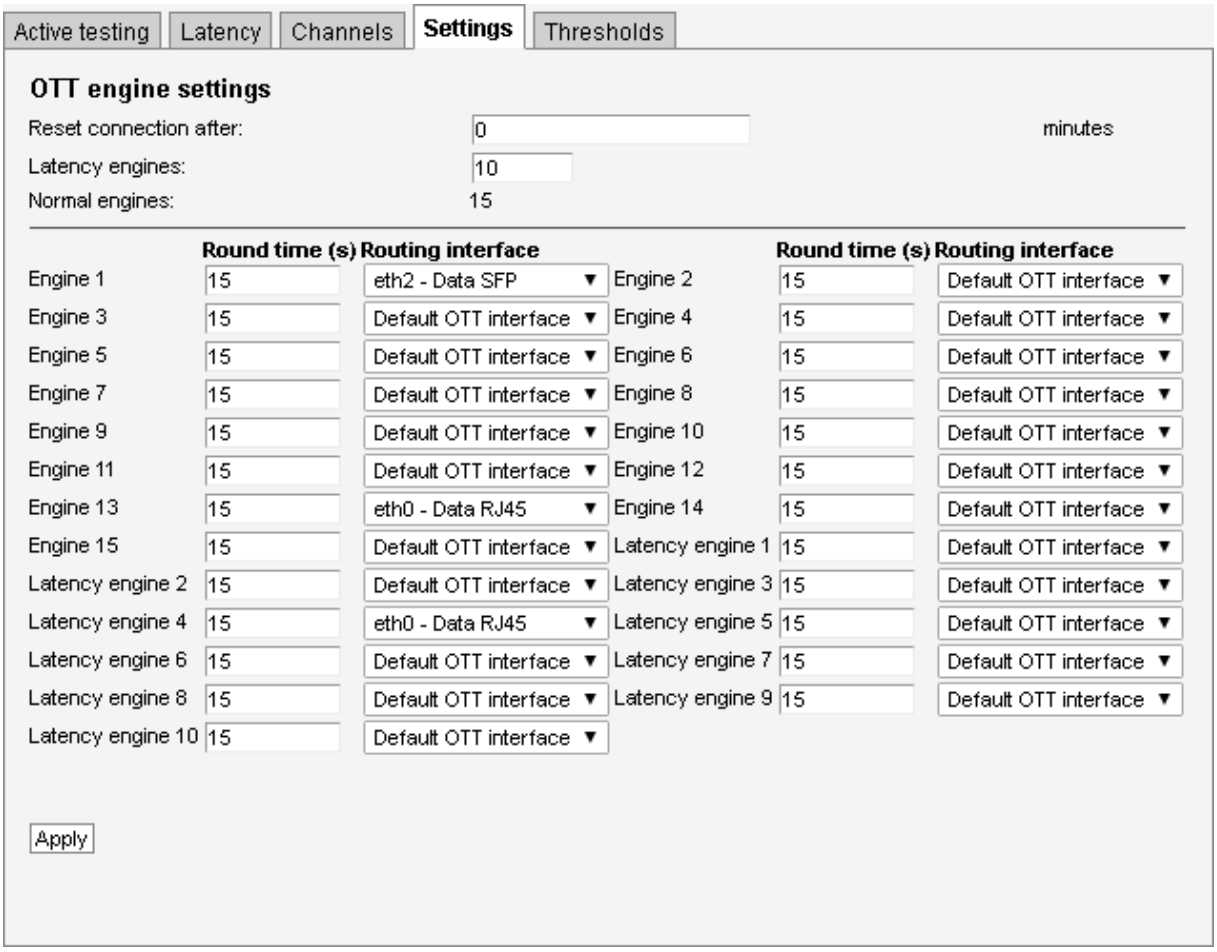
	General
Enabled:	Check the 'Enabled' check box to start monitoring the OTT service.
Select engine:	A number between 1 and 50, depending on license activated, indicating which OTT engine the channel uses.
Threshold:	The OTT threshold that should be assigned to the OTT channel. OTT thresholds that have been defined in the **OTT — Thresholds** view are available for selection from the drop-down menu.
VBC thresholds:	The alarm threshold template used to configure when alarms are generated towards the VBC server.
Measurement mode	Specify if you want **Normal** active testing measurements, OTT Channel Distribution **Latency** measurements, or **Both** kinds of measurements for this channel. Each channel you set to either **Latency** or **Both** uses up one Latency Engine. If you do not have any spare, it will be set back to **Normal**. See **OTT — Latency** for more info.
Name:	A name should be assigned to each OTT channel. The name will be used throughout the VB330-SW's user interface when referring to this channel.
Manifest URL:	The URL of the OTT channel.
Player URL:	In this field you can enter the URL to a web page which will open the OTT channel in your browser. If entered, a 'play' button will be displayed in the OTT overview tab, which will open the selected URL in a new browser tab.
Smooth Streaming target chunk:	For Smooth Streaming, this specifies which chunk, counted from the bottom of the list, the VB330-SW should download when doing active testing on a live channel. For other formats, this option is ignored.
VCAS hostname:	If this channel is encrypted using a Verimatrix VCAS 3.7 server, entering the IP address or hostname of the VCAS server's encoder interface will allow descrambling of the encrypted chunks. See **OTT descrambling with Verimatrix** for more info.
Availability mode:	If this option is enabled, the engine will only check for chunk presence but not download the entire file. This also disables thumbnail generation.
RTMP:	Check this check box if the channel is an RTMP channel.
RTMP live:	Check this check box if the RTMP channel is a live service.
Thumbnail:	If the thumbnail option is enabled thumbnails will be available for the selected channels in the Active testing and Thumbnails sections.
Alignment:	If the alignment option is enabled the alignment section will be available.



Adv. manifest	
Enable adv. settings:	Check this box to enable the advanced manifest settings. If unchecked, all settings on this page are ignored.
Method:	Determines which HTTP method to use when requesting the top-level manifest file. Supported methods are **GET** and **POST**.
Content-Type:	When requesting the manifest using the HTTP **POST**, use this Content-Type for the submitted request body.
Additional headers:	To provide additional custom request headers or overwrite the default headers when requesting the top-level manifest file, create a text file containing the headers and upload them here.
Body:	When requesting the manifest using the HTTP **POST**, upload the file to submit here.

The advanced manifest options can be used in instances where the master manifest file is not directly available to download. If your channel needs several steps of authentication or other web service calls before supplying clients with an URL to the master manifest, you can make an “in-between” web service which the VB330-SW sends all required info to do the authentication and/or channel lookups through this interface, and which returns an JSON file with an “url” parameter containing the URL to the master manifest file.

5.3.5 OTT — Settings

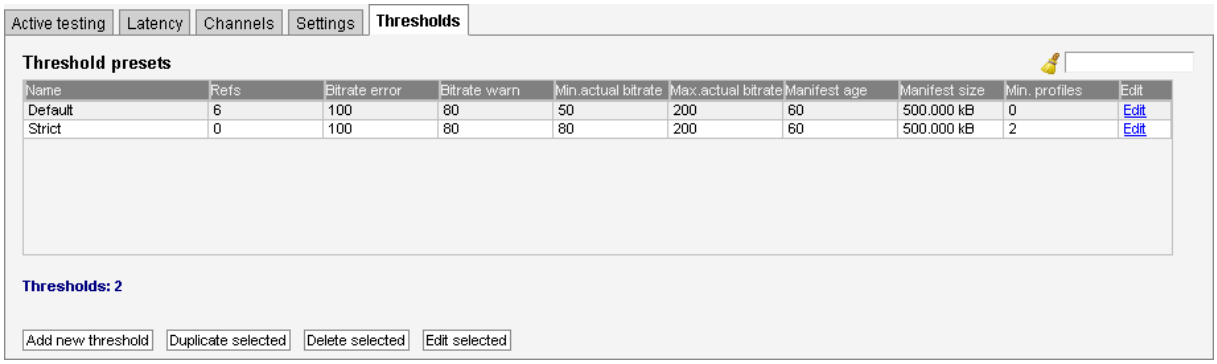


The Settings tab makes it possible to change global and per-engine OTT monitoring parameters. Press **Apply** to confirm changes made.

Settings	
Reset connection after:	Configures the VB330-SW OTT engines to reset the connections after the specified number of minutes. This is useful for cases where the server has a limit for how long a session can live. By resetting before that limit a new session is created and the problem is avoided.
Latency engines:	Select the number of engines to dedicate to OTT latency monitoring. These engines will not be available for regular OTT monitoring, and the value must be less than the total number of licensed OTT engines on the probe. See **OTT — Latency** for more info. Latency engines are assigned to channels automatically, and are listed in the **OTT — Active Testing** view.
Normal engines:	The number of normal OTT engines (i.e., not dedicated to OTT latency monitoring) is automatically calculated and displayed here.

Round time (s):	Sets the minimum round time for each OTT engine, in seconds (default: 15 seconds). If an engine finishes processing all its channels in less time than this, it waits until this amount of seconds has passed since it started the round before starting to process through its channels again. Note: The round time may not be set to a value less than 2 seconds.
Routing interface:	Selects the interface on which to connect to the OTT server. This defaults to the interface selected in the **Setup — Routing** view, but can be overridden for each engine. The routing applies to all channels monitored by this engine. Latency engines are assigned to channels automatically, and are listed in the **OTT — Active Testing** view.

5.3.6 OTT — Thresholds



The OTT **Threshold presets** list shows OTT threshold templates configured by the user.

To add a threshold template to the list click the **Add new threshold** button. This will open the **Edit threshold** pop-up view, allowing the user to define threshold parameters. A threshold template entry can be selected by clicking the threshold template; the list entry will be highlighted. Several list entries can be selected by using regular *Ctrl* + *click* functionality. Clicking the **Duplicate selected** button will open the **Edit threshold** pop-up view with all threshold template parameters duplicated, except the threshold template name. Clicking **Delete selected** will delete the highlighted list entry. Clicking **Edit selected** will open the **Edit threshold** pop-up view associated with the highlighted threshold template. Batch editing is supported. Select the threshold templates and click the **Edit selected** button. Parameters differing between templates will be indicated in the **Edit selected** pop-up view by an asterisk wildcard symbol.

The search field in the upper right corner of the view allows the user to type a text string, and the threshold list is updated to display only thresholds matching the specified text.

To disable a threshold alarm, set the threshold value to –1. This does **not** apply for *Manifest XML size*.

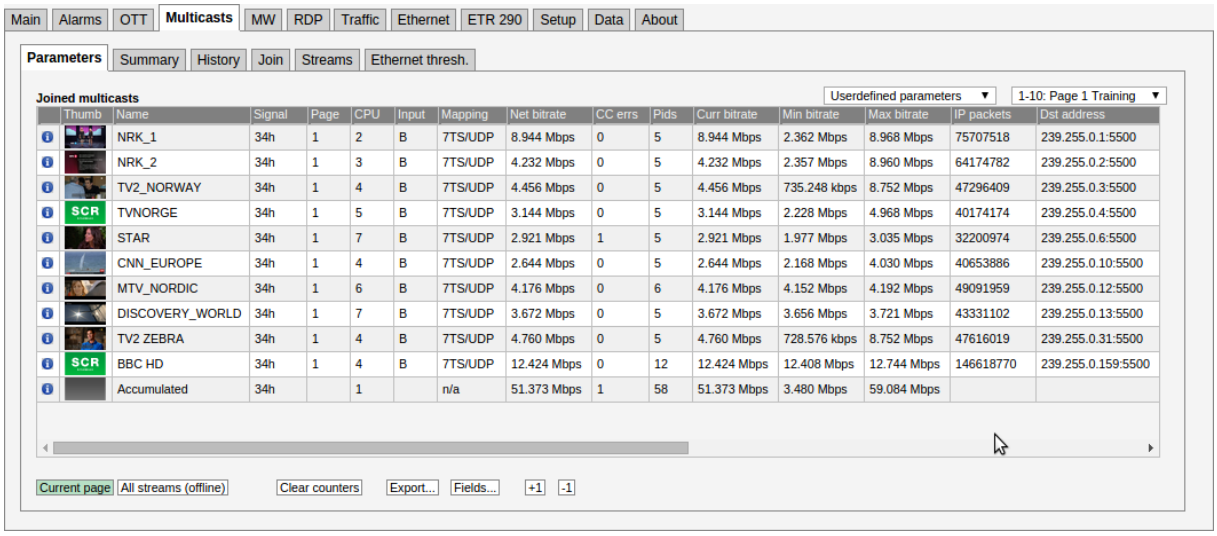
Threshold preset	
Name:	The threshold template name defined by the user.
Refs:	The number of channels associated with the threshold template
Download speed error:	The maximum allowed difference between profile bitrate and download bitrate (%). If the difference exceeds the threshold value a bitrate error alarm will be raised.

Download speed warn:	The maximum allowed difference between profile bitrate and download bitrate (%). If the difference exceeds the threshold value a bitrate error warning will be raised.
Actual bitrate min:	The minimum allowed bitrate when measured actual bitrate is compared to profile bitrate (%). If the actual bitrate goes below the threshold an actual bitrate alarm will be raised.
Actual bitrate max:	The maximum allowed bitrate when measured actual bitrate is compared to profile bitrate (%). If the actual bitrate exceeds the threshold an actual bitrate alarm will be raised.
Sequence age:	The maximum time a manifest can remain unchanged before a manifest age alarm is raised.
Manifest XML size:	The maximum detected size of the manifest before a manifest size alarm is raised.
Min. profiles:	Minimum number of profiles in the selected channel before an alarm is raised.



5.4 Multicasts

5.4.1 Multicasts — Parameters



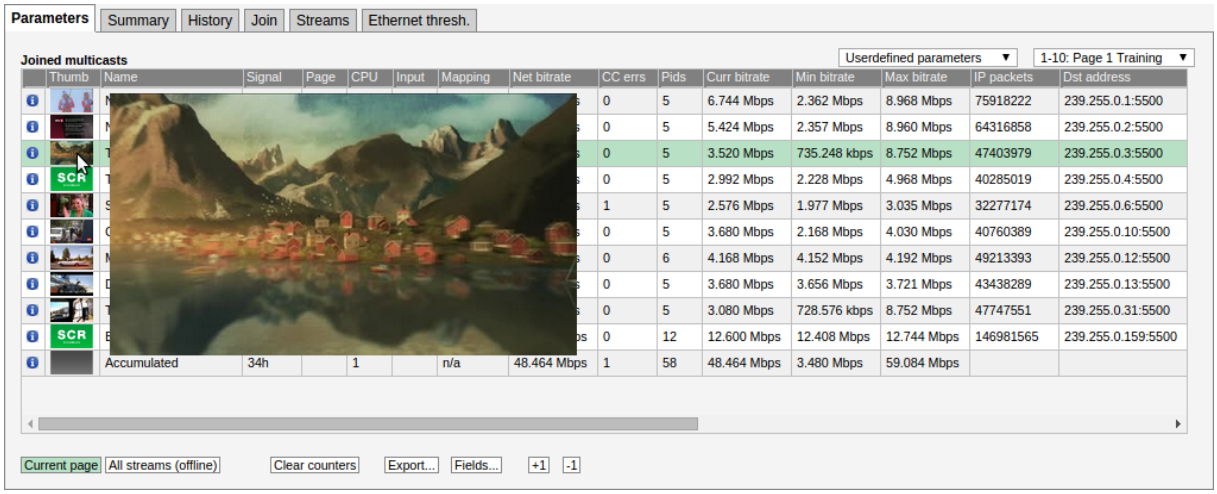
The **Multicasts — Parameters** view displays detailed information about each stream.

The user selects which group of measurements should be displayed. Selections are *IP parameters*, *TS parameters*, *Ethernet parameters*, *RTP and FEC parameters*, *User-defined parameters* and *Statistical parameters*. If *User-defined parameters* is selected, the **Multicasts** view displays parameters selected by the user in the **Multicasts — Parameters — Fields** view.

For each page the *Accumulated* row at the bottom of the multicast list displays accumulated values for all streams associated with the page. The accumulated *Min bitrate* and *Max bitrate* is the minimum and maximum value of the *Accumulated* current bitrate.

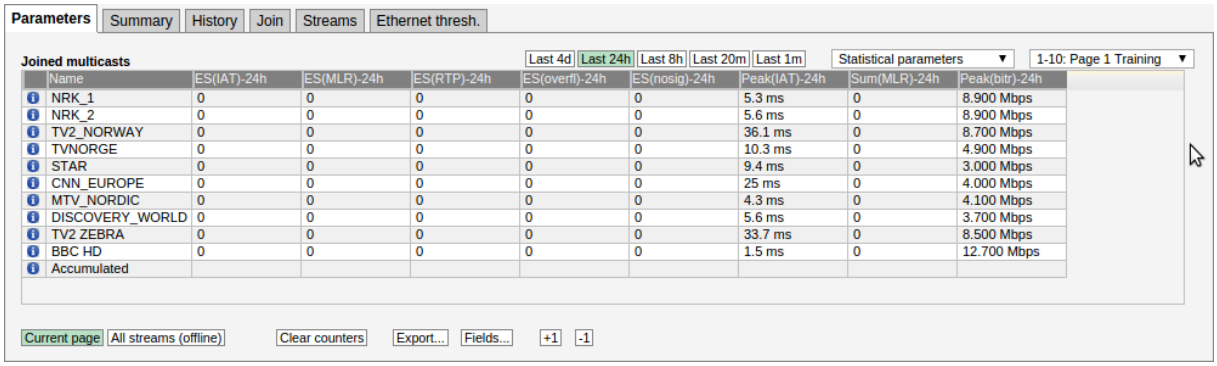
When the **Current page** button is clicked it is possible to select the page from a drop-down menu. The associated thumbnails are shown in the leftmost column of the list of measurements. Click one of the small thumbnails to view a larger thumbnail that is updated more frequently. Note that it is possible to disable probe thumbnail extraction in the **Setup — Params** view.

When **All streams (offline)** is clicked a complete list of measurements for all joined streams is displayed. A search field allows the user to type a text string and the multicast list is updated to display only multicasts matching the specified text. Note that monitoring parameters and thumbs will not be updated in **All streams (offline)** mode.



Peak and aggregate measurements are cleared when the **Clear counters** or **Clear counters all pages** button is clicked. Clicking this button also restarts the ETR monitoring for the streams have this enabled.

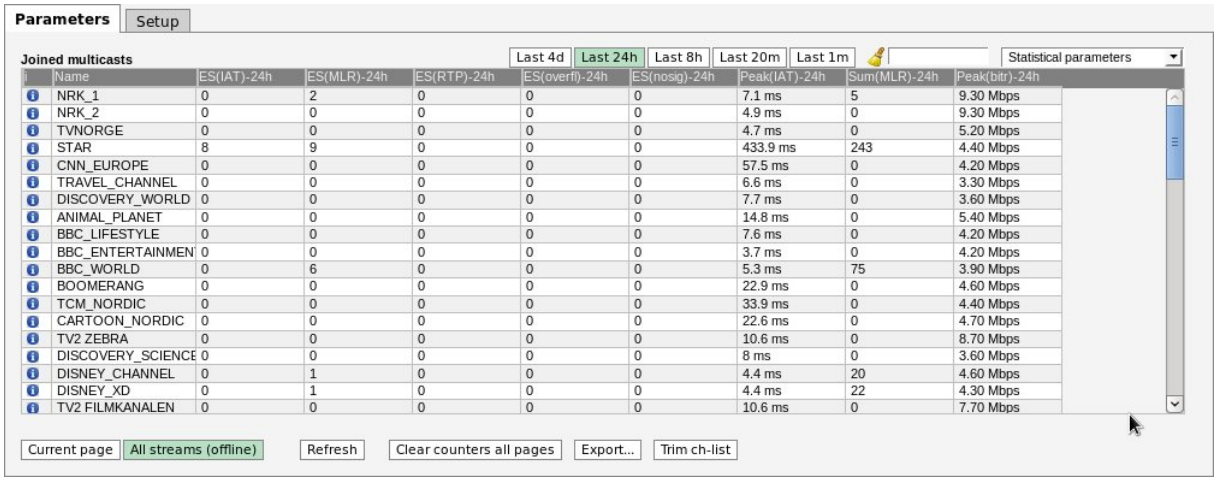
Clicking the **Export** button will allow export of the measurement data as an XML file that is opened in a new window.



Click the **Trim ch-list** button to unjoin streams with current status ‘No signal’, thereby removing them from the list. The **Statistical parameters** view lists sum or peak values for parameters over the interval indicated by the selected time button (Last 4d, Last 24h, Last 8h, Last 20m, Last 1m).

Clicking a stream brings up the **Detailed monitoring** pop-up described later in this section.

In **All streams (offline)** mode a search field allows the user to type a text string and the multicast list is updated to display only multicasts matching the specified text.





Joined multicasts	
ⓘ:	Click the information icon to access the **Detailed Monitoring** pop-up view.
Thumb:	A thumbnail is displayed for each stream. Click the small thumbnail to view a larger image that is updated more frequently.
Name:	The stream name specified by the user in the **Edit Multicast** view
Signal:	Time since last signal loss
Page:	The page associated with the multicast
Mapping:	For MPEG-2 Transport streams, the number of MPEG-2 packets mapped into each RTP or UDP packet is displayed here. For SMPTE 2022-6 SDI over IP streams, “SDI/RTP” is displayed, and for other unsupported RTP streams, “RTP data” is displayed.
Net bitrate:	Instantaneous MPEG-2 Transport Stream bitrate excluding null packets (PID 8191). The instantaneous bitrate is measured over a time period of 1000 ms.
CC errs:	The number of times a discontinuity has been detected for all the MPEG-2 Transport Stream continuity counters. This value is the total number of discontinuities detected for all PIDs present. Note that this value does NOT represent the number of MPEG-2 TS packets lost because any continuity counter mismatch detected for an IP-frame will increase CC errs by one. CC errors are serious as they will in practice usually result in visual video artifacts (‘blocking’) if occurring on the video PIDs. CC errors can be due to an erroneous input signal to the streaming head-end (e.g. from satellite rain fading or changes in the uplink). Alternatively, CC errors can arise from IP packets being dropped in the network.
PIDs:	Number of PIDs in the MPEG2-TS
Syncb errs:	Number of transport stream packets with wrong syncbyte (0x47)
Curr bitrate:	Instantaneous MPEG-2 Transport Stream bitrate including null packets (PID 8191). The instantaneous bitrate is measured over a time period of 1000 ms. For non-TS traffic the bitrate is calculated from the size of the UDP payloads.
Min bitrate:	The minimum current bitrate measurement
Max bitrate:	The maximum current bitrate measurement
IP packets:	The number of IP packets received
Dst address:	Multicast/unicast destination address : port
TOS:	Type-Of-Service (also called Differentiated Services Field)
TTL:	Time-To-Live
VLAN ID:	Native VLAN ID of this stream
Src address:	Multicast/unicast source address : port
Joined src:	The source address of the originally joined multicast.
IAT avg:	Average Inter-Arrival Time. The average time between consecutive IP frames (in milliseconds). Recalculated each second.
IAT min:	The Minimum Inter-Arrival Time is the minimum registered time between two consecutive IP frames carrying video. Units are in milliseconds.

IAT max:	The Maximum Inter-Arrival Time is the maximum registered time between two consecutive IP frames carrying video. Units are in milliseconds. The Max-IAT is a measure of the maximum amount of network-induced packet jitter present. IP packet jitter affects video quality and should be minimized.
Src MAC:	Source MAC address
Dst MAC:	Destination MAC address
RTP drops:	Accumulated number of dropped IP-frames due to network errors. Only available for multicasts that carry RTP information. When running video inside an RTP wrapper it is possible to exactly deduce the number of dropped IP frames due to network issues. This is possible as a result of the 16-bit sequence counter inside the RTP header. The following sequence will generate an RTP drops of +3: . . . , 10, 11, 12, 16, 17, 18, . . .
RTP dups:	Accumulated number of duplicate IP-frames. Only available for multicasts that carry RTP information. Duplicate IP-frames in the network can occur under normal circumstances and does not necessarily indicate network problems. The following sequence will generate an RTP dups of +2: . . . , 10, 11, 12, 12, 12, 13, 14, . . .
RTP ooo:	Accumulated number of times a packet has been found to be out of order. Only available for multicasts that carry RTP information. An out-of-order situation is defined to have occurred when the current sequence number is lower than the previous one. The following sequence will generate an RTP ooo of +2 (since there are two occurrences): . . . , 10, 11, 15, 12, 16, 17, 13, 14, 18, 19, . . .
RTP lag:	The maximum number of packet positions an out-of-order packet has been moved relative to its correct position. So for example 1,2,3,5,6,7,8,4,9,10 will result in an RTP lag of 4. The RTP lag is a good measure of how big a packet re-ordering buffer is needed in the receiving equipment to re-order packets.
Min hole size:	Minimum number of consecutive dropped RTP packets. The sequence 1,2,3,10,11,12,15 gives a min hole size of 2.
Max hole size:	Maximum number of consecutive dropped RTP packets. The sequence 1,2,3,10,11,12,15 gives a max hole size of 6.
Min hole sep:	Minimum number of RTP packets separating any holes. The sequence 1,2,3,10,11,12,15 gives a min hole sep of 3.
Num holes:	Number of packet loss sequences. The sequence 1,2,3,10,11,12,15 gives a num holes of 2.
FEC mode:	The CoP3 FEC mode
FEC drops:	Number of RTP packet drops in the main stream that the FEC could not correct
C-FEC drops:	Number of IP packets in the column-FEC streams dropped
R-FEC drops:	Number of IP packets in the row-FEC streams dropped

Statistical parameters

MPEG-2 transport stream parameters	
ⓘ:	Click the information icon to access the **Detailed Monitoring** pop-up view.
Name:	The stream name specified by the user in the **Edit Multicast** view
ES(IAT):	Number of seconds during selected period with Inter-packet Arrival Time higher than associated Ethernet IAT warning threshold

ES(MLR):	Number of seconds during selected period with Media Loss (corresponding to number of seconds with CC-errors)
ES(RTP):	Number of seconds during selected period with RTP packet drops
ES(overfl):	Number of seconds during selected period with bitrate overflow
ES(nosig):	Number of seconds during selected period without signal
Peak(IAT):	Peak Inter-packet Arrival Time during selected period.
Sum(MLR):	Sum of Media Loss during selected period (equals number of TS packets lost)
Peak(bitr):	Peak stream bitrate during selected period

Thumbnails

The probe will try to generate thumbnail pictures for all streams. For multi-program transport streams (MPTS) the first video component is selected. MPEG-2, H.264/MPEG-4, H.265/HEVC and JPEG 2000 video formats in standard definition, high definition or ultra-high definition are supported in MPEG-2 transport streams, as well as SMPTE 2022-6 uncompressed video in RTP streams.

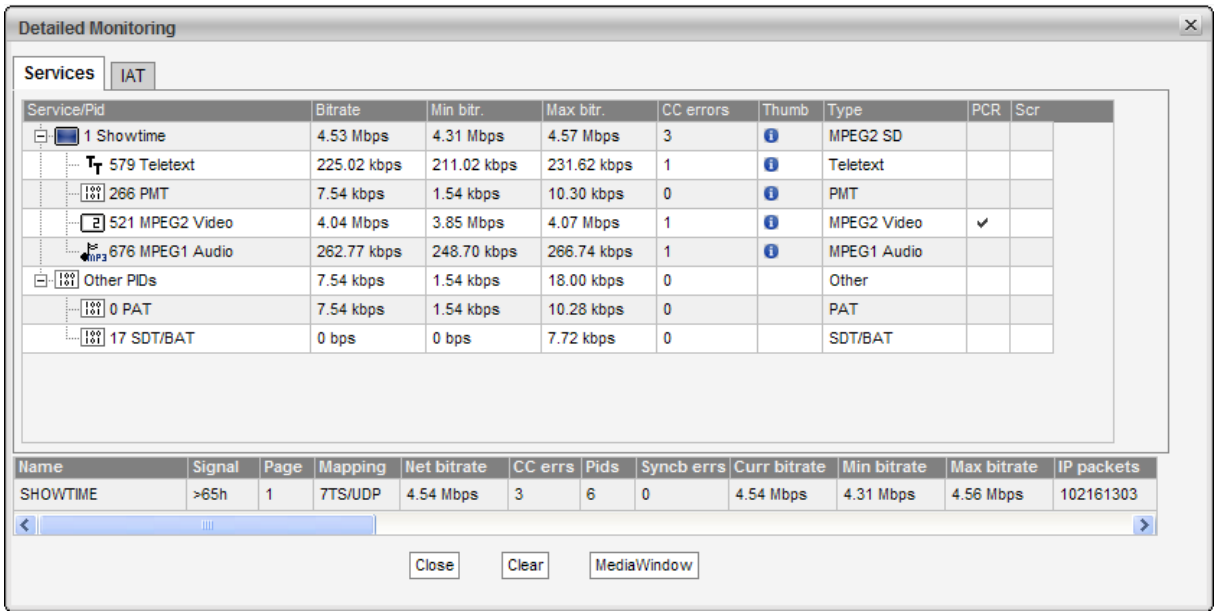
The thumbnail update rate will depend on how the streams are coded and if they are standard definition, high definition or ultra-high definition. It is possible to increase the update rate by opening the **Thumb View** pop-up, described below.

If the probe is unable to generate a thumbnail from the signal, it will present one of the following icons:

	Shown if no data is received for the stream. There should be a match between presenting this icon and a No-signal alarm; however since the alarm and thumbnail mechanisms work independently of each other they have been given different names (loss of signal and no signal).
	Shown while the thumbnail engine is trying to decode a thumbnail picture and more precise status information has not yet been obtained. This icon is typically displayed after probe reboot or if new streams have recently been joined.
	Shown if the service does not carry a video PID — which is the case for radio services.
	The stream contains no service, as signaled in PSI/SI.
	The signal cannot be decoded due to excessive CC errors or RTP packet drops.
	The probe does not support thumbnail generation for this protocol mapping.
	The signal is recognized as being MPEG-2 encoded but the thumbnail extractor is unable to correctly decode a thumbnail picture.
	The signal is recognized as being MPEG-4/H.264 encoded but the thumbnail extractor is unable to correctly decode a thumbnail picture.
	The signal is recognized as being MPEG-H/H.265 encoded but the thumbnail extractor is unable to correctly decode a thumbnail picture.
	The signal is recognized as being JPEG 2000 encoded but the thumbnail extractor is unable to correctly decode a thumbnail picture.

RAW	The signal is recognized as being an uncompressed (raw) video stream but the thumbnail extractor is unable to correctly decode a thumbnail picture.
PSE PSI ERROR	This icon is shown if the probe is unable to receive or analyze the PMT PID. Only streams with PSI information can have thumbnails decoded since the probe does not support a manual specification of the video PID.
SCR SCRAMBLED	The probe can only generate a thumbnail picture if the video data is not scrambled.

Detailed Monitoring



The **Detailed Monitoring** pop-up is activated by clicking a stream line in the monitoring list.

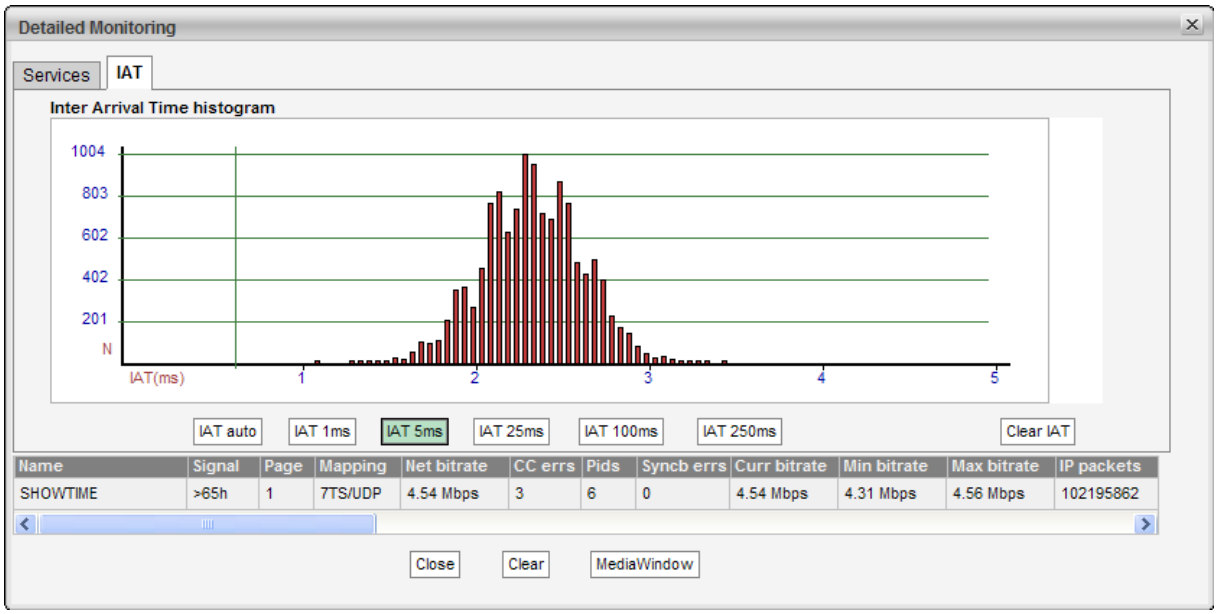
The 10G Software Probe is continuously gathering detailed information for the selected multicast. The VB330-SW will continue updating the detailed information for the selected multicast until another is selected. Clicking the **Clear** button will clear all information about the selected stream, including PSI/SI analysis data.

The **Detailed Monitoring — Services** view lists detected MPEG-2 TS services (by analyzing the PSI/SI tables) or SMPTE 2022-6 SDI over IP components, providing the following aggregate information for each service:

Service/Pid:	For each service, the service-name or service-id is obtained from the PSI/SI tables. PIDs that do not belong to a service are denoted ‘Other PIDs’. The service ID is presented in square brackets.
Service/Component:	This replaces the “Service/Pid” column for SMPTE 2022-6 SDI over IP streams, displaying the identified components.
Bitrate:	Service or component bitrate in bits per second
Min bitr.:	Minimum service or component bitrate in bits per second
Max bitr.:	Maximum service or component bitrate in bits per second

CC errors:	Number of Continuity Counter occurrences
Thumb:	Click the ① icon to access the **Thumb** pop-up view, explained below
Type:	The list entry service type or PID type
PCR:	This field will be checked if the corresponding PID carries PCR
Scr:	This field will be checked if the corresponding PID is scrambled

Directly beneath this list, the current parameters for the selected stream are displayed, as in the **Joined multicasts** list.



In the **Detailed Monitoring — IAT** view the **Inter Arrival Time** histogram shows the accumulated number of IAT measurements within each presented interval. Vertical green lines indicate the maximum and minimum IAT values. By clicking the IAT range buttons it is possible to change the zooming of the graph. If the **IAT auto** button is pressed the diagram will auto-scale to always include the minimum and maximum IAT readings.

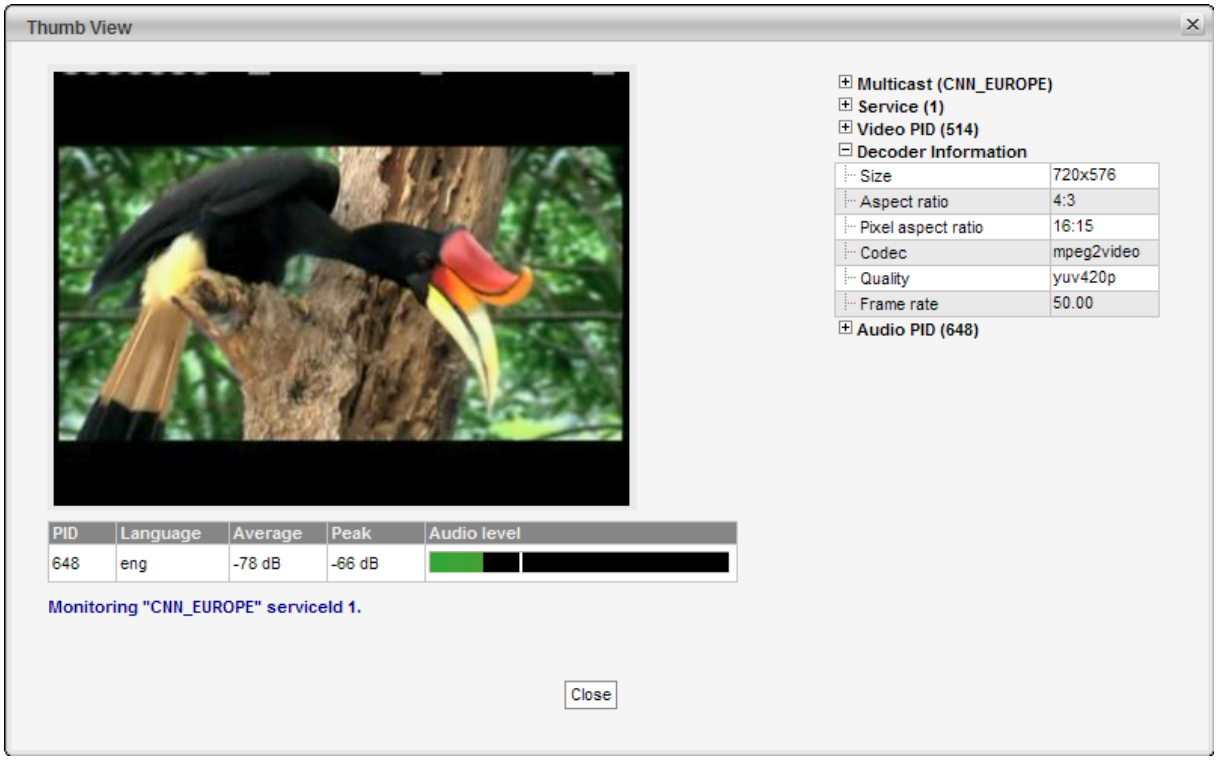
The IAT histogram is a very useful and intuitive measure of how well the network is performing in terms of forwarding real-time traffic. A predictable and tightly bunched graph indicates small levels of network jitter. An unbound graph indicates network jitter issues typically brought forward by traffic congestion or misconfigured routers. Clicking the **Clear IAT** button will clear the IAT graph.

Under the IAT histogram the **Multicasts — Parameters (Current parameters)** measurements for the selected stream are displayed. Clicking the **Clear** button will clear all information about the selected stream, including PSI/SI analysis data.

Clicking the **MediaWindow** button will open the Media Window **Selected channel** view. This is described in section 5.5.

Note that for variable bitrate streams the IAT histogram will show a very different IAT distribution compared to the histogram for a constant bitrate stream. The histogram in the screenshot above displays the IAT distribution for a CBR stream.

Thumb View



The **Thumb View** pop-up is accessed by clicking an information icon in the **Detailed Monitoring — Services** view. This view presents a large thumbnail, as well as video and audio metadata for the selected stream, with an increased update rate compared to non-selected streams. Service audio level is indicated by one audio level bar per audio component. The same pop-up can be opened from the **Main — Thumb Overview** view, see chapter 5.1.3 for more information.

Clicking the **Close** button will close the **Thumb View** view.

The following metadata is displayed for multicasts:

Audio fields	
PID:	The audio PID for which the associated parameters apply
Language:	The audio language, as derived from PSI/SI
Average:	The average audio level in dB, measured over 0.4 seconds
Peak:	The peak audio level in dB, detected during 0.4 seconds
Audio level:	An audio level bar displaying the average audio level as a green bar referenced to the peak audio level, the peak level being indicated by a white line

Please note that audio information is only decoded when requested by opening this window. Initial extraction of audio information can take up to one minute.

The right-hand column will display the following detailed metadata:

Multicast	
Name:	The name of the multicast containing the selected service, as defined by the user

Type:	The type of the stream containing the selected service; multicast or unicast
Multicast address:	The multicast address of the stream containing the selected service
Multicast port:	The port number of the multicast containing the selected service
Transport stream ID:	The ID of the selected stream as shown in the list of multicasts in the Ethernet section; non-TS services display *1* here
Stream status:	The status of the stream containing the selected service, as reported by the decoding engine
Bitrate:	The total stream bitrate of the multicast containing the selected service (bits/s)

Service	
Service ID:	The service ID of the selected service; non-TS services display *1* here
PSI/SI Name:	The name of the selected service, as derived from PSI/SI; non-TS services display the multicast name here instead
Controlbit scramble state:	The scramble state as indicated by the MPEG TS control bit
PES sync scramble state:	The scramble state as detected from the PES sync state
Number of PIDs/Components:	The number of PIDs or components associated with the selected service
Bitrate:	The total bitrate of the selected service (bits/s)

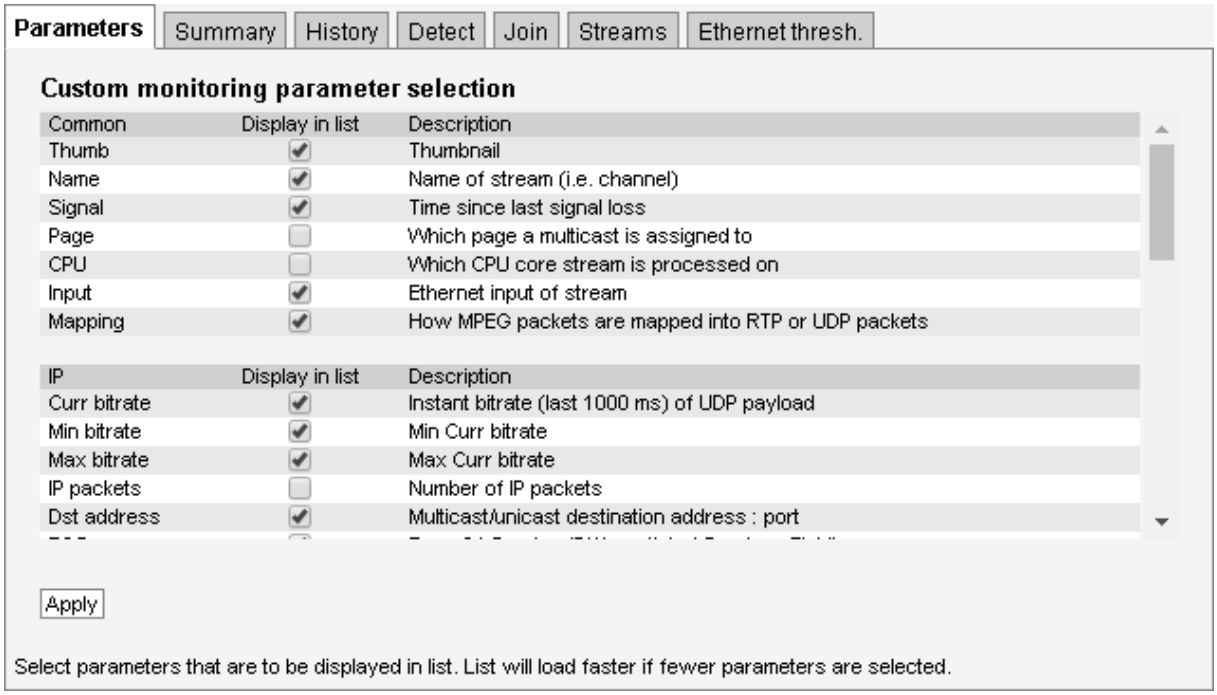
Video PID/Component	
PID/Component:	The video PID of the selected service for MPEG-TS services, or the video component number for non-TS services
Has PCR:	Yes if the selected stream contains PCR, No if not
Bitrate:	The video PID bitrate of the selected service
PES sync:	The latest PES sync state
PES length indicator:	If signaled in the PES packet header, the PES packet length is displayed; for non-TS services “N/A” is displayed
Status:	The status of the video PID as reported by the decoding engine

Video Information	
Size:	The video picture size of the selected service
Aspect ratio:	The video aspect ratio of the selected service, or “N/A” if no information is available
Pixel aspect ratio:	The video pixel aspect ratio of the selected service, or “N/A” if no information is available
Codec:	The video encoding format of the selected service
Quality:	The video sampling format of the selected service
Frame rate:	The video frame rate of the selected service (Hz)

Audio PID/Component	
PID/Component:	The audio PID of the selected service for MPEG-TS services, or the audio component number for non-TS services Note that there may be several audio PIDs or components associated with a service
Type:	The audio encoding standard
Has PCR:	Yes if the selected Audio PID contains PCR
Language:	The language of the audio, as defined in the MPEG-TS Program Map Table (PMT)
Bitrate:	The audio bitrate for this PID or component (bit/s)
Is scrambled:	'Yes' if the audio PID is scrambled.
Peak level:	The peak audio level in dB, detected during a period of approximately 0.4 seconds
Average level:	The average audio level in dB, measured over a period of approximately 0.4 seconds

Audio Information PID/Component	
Codec:	The audio encoding format
Samplerate:	The audio sample rate (Hz)
Channels:	The number of audio channels represented by the audio PID or component
Layout:	The audio channel layout
Format:	The binary format of the audio stream
Bitrate:	The effective audio bitrate (bit/s)

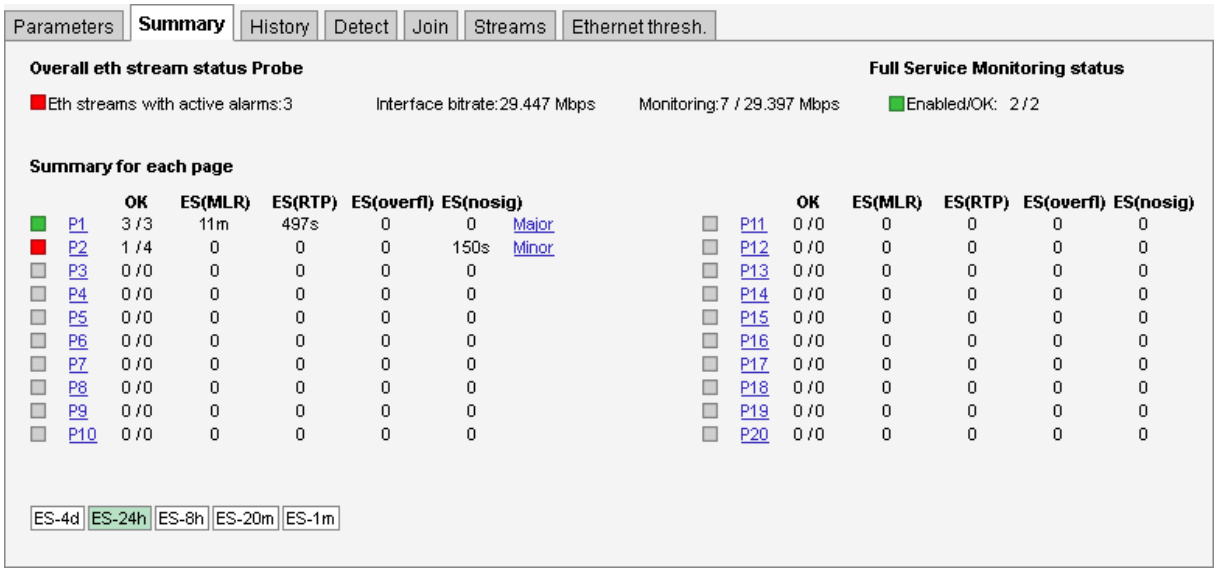
5.4.2 Multicasts — Parameters — Fields





The **Multicasts — Parameters — Fields** view enables selection of the parameters to be displayed in the **Multicasts — Parameters** view. Note that thumbnails must also be enabled in the **Setup — Params** view for thumbnail availability.

5.4.3 Multicasts — Summary



The intention of this page, together with the **alarm list**, is to provide enough information for the operator to immediately see if there is anything seriously wrong with one or more Ethernet input streams. The overall status for the Full Service Monitoring (FSM) is also shown.

Throughout this view the bulb colors indicate the most severe active alarm. They may be green (no alarm), yellow (warning), orange (error) or red (major). The bulb color is based on user defined alarm severity settings for each alarm. A grey bulb indicates that monitoring is disabled.

The following Ethernet parameters are shown:

Eth streams withactive alarms:	Shows the number of streams that are presently in an alarm state. Note that the number of alarms counted refers to default settings, and alarms disabled by the user will still be counted.
Interface bitrate:	This is the total bitrate sensed on the data/video interface(s). It should be greater than or equal to the Monitoring bitrate.
Monitoring:	This is the total number of Ethernet streams monitored and the total bitrate for these streams.
Full Service Monitoring status:	The number of enabled FSM services / number of OK FSM services

The probe is capable of monitoring several thousand streams simultaneously. The probe splits streams into pages for easy handling. Each of the 30 predefined pages can be given a name and have a user defined number of streams associated.

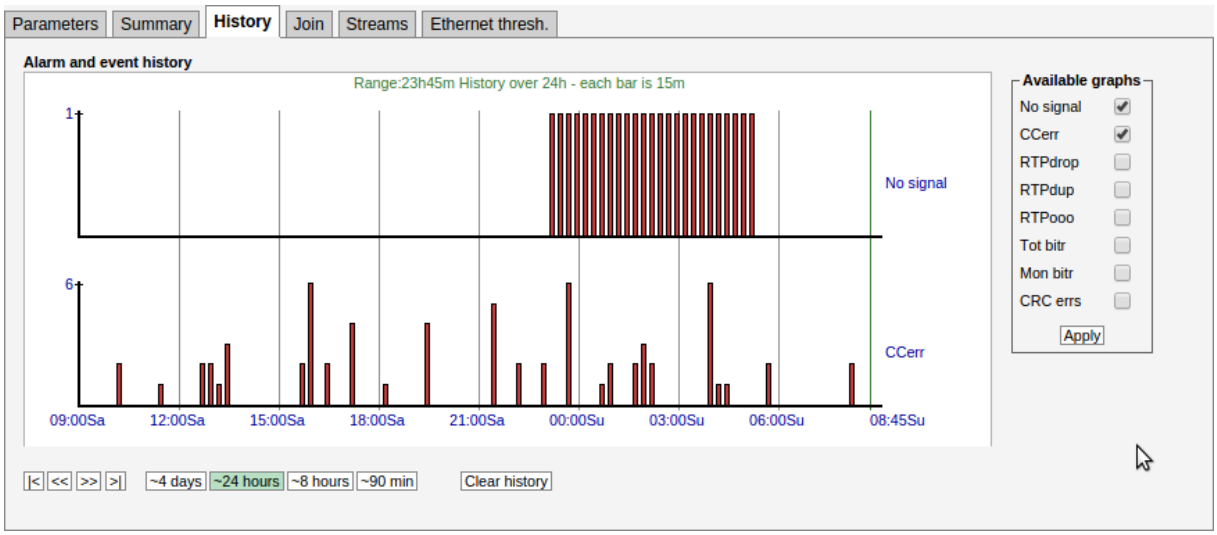
Part of the page-status is error-second statistics for the fundamental parameters **MLR**, **RTP**, **overfl** and **nosig** summed across all streams belonging to that page.

The error-second statistics interval is selected by clicking the buttons. For example, clicking the **ES–8h** button will present error-seconds for the last 8 hours. If 10 streams for a page have been without signal for the last 8 hours, the **nosig** will show as 80hours.

The following parameters are presented (note that the error second values are accumulated from probe boot time, and they will only be cleared by reboot or by clicking the **Clear all** counters button in the **Main** view):

'Bulb':	The bulb indicates the most severe active alarm for any of the streams on the page. Active alarms are located on top of the alarm list. The alarm severity is reflected by the color of the associated icon. Next to the bulb is a link that will lead to the **Monitoring page** if pressed. The Monitoring page will present error-second statistics for each stream individually.
OK:	Shows how many of the streams monitored on this page are without active alarms
ES(MLR):	Number of seconds in selected period with continuity counter errors in the MPEG2 transport stream (which corresponds to the number of seconds with non-zero Media Loss Rate).
ES(RTP):	Number of seconds in selected period with RTP packet-drop
ES(overfl):	Number of seconds in selected period with bitrate overflow
ES(nosig):	Number of seconds in selected period where no signal (i.e. no data) was received

5.4.4 Multicasts — History



The probe keeps statistical Ethernet information for the last 4 days for visual inspection in the **history timeline view**.

Each bar in the histogram corresponds to a number of events that occurred within a certain time interval. The interval that each bar represents depends on the scale, from 1 minute (when 90 min is selected) to 1 hour (when 4 days is selected).

Clicking the **Clear history** button will reset all history graphs.

Tool-tip information is available for each bar and shows the time-interval for the bar and its exact value. For example, the tool-tip information '1315-1330:2' means that within the time interval 13:15–13:30 there were 2 occurrences.



The histogram is updated every minute.

Any subset of the following parameters can be selected, click the **Apply** button for changes to take effect:

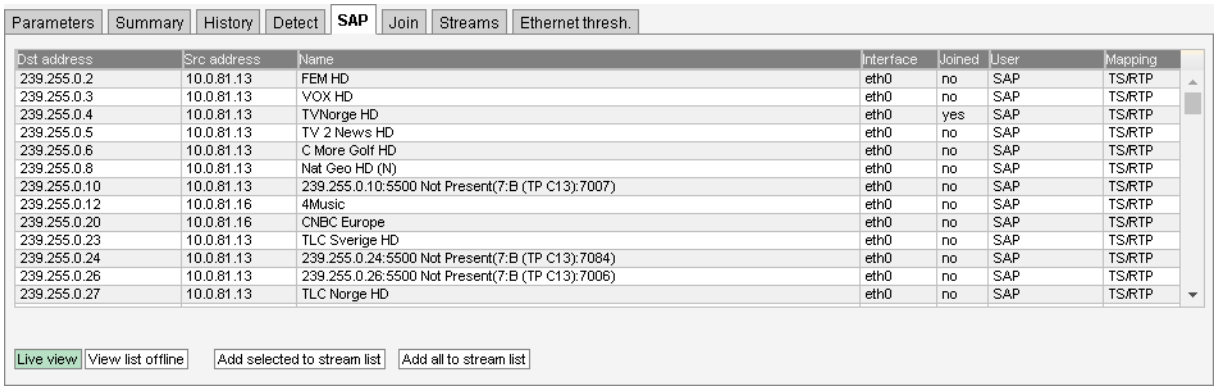
No signal:	The number of streams that reported the 'No signal' alarm during the interval represented by the bar.
CCerr:	The number of times a discontinuity has been detected for all the MPEG-2 Transport Stream continuity counters in the interval represented by the bar. This parameter corresponds to the sum of **CC errs** reported by all streams.
RTPdrop:	Accumulated number of dropped IP-frames due to network errors in the interval represented by the bar. This parameter corresponds to the sum of **RTP drops** reported by all streams.
RTPdup:	Accumulated number of duplicate IP-frames in the interval represented by the bar. This parameter corresponds to the sum of **RTP dups** reported by all streams.
RTPooo:	Accumulated number of times a packet has been found to be out of order in the interval represented by the bar. This parameter corresponds to the sum of **RTP ooo** reported by all streams.
Tot bitr:	Bitrate sensed on the data/video interface(s).
Mon bitr:	Bitrate on the data/video interface(s) corresponding to joined multicasts.
CRC errs:	Detected CRC errors. Ethernet CRC errors are most likely caused by a bad cable or a misconfigured router. A CRC error may impact packet loss measurements such as CC errors and RTP errors.

Note that the history graphs show the sum for all streams being analyzed across all pages. So for example, if two streams experience **No signal** at the same time the **No signal** graph will increase by 2.

5.4.5 Multicasts — Detect

Please see chapter 5.7.2 on page 84.

5.4.6 Multicasts — SAP



The **SAP** view displays streams announced using the Session Announcement Protocol, detected by the VB330-SW.

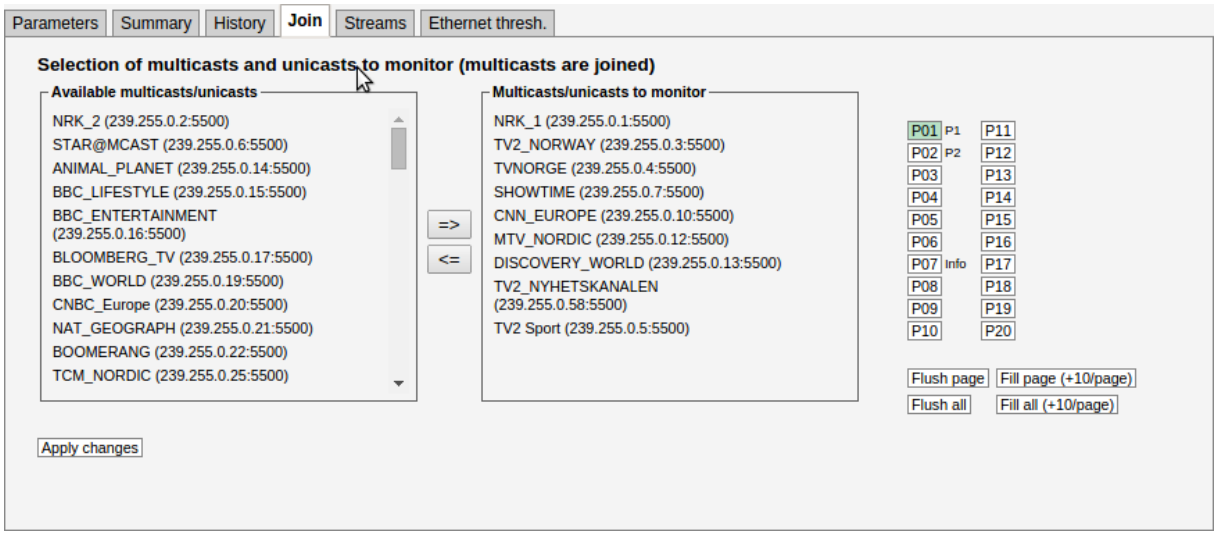
As long as **Enable SAP discovery** is enabled in the **Setup — Params** view, the VB330-SW will continuously try to detect streams. Click the **View list offline** button to view the stream list in offline mode. Click the **Refresh** button to update the stream list in offline mode.

The source address makes it possible for the 10G Software Probe to distinguish between multicasts with the same destination IP address and port, provided that **Source specific multicasts** has been enabled in the **Setup — Params** view.

If the stream is currently joined by the 10G Software Probe (i.e. the VB330-SW is currently monitoring the stream), the **Joined** field is set to yes.

Detected streams can be added to the VB330-SW's stream list by selecting streams and clicking the **Add selected to stream list**. To add all detected streams the **Add all to stream list** button can be pressed.

5.4.7 Multicasts — Join



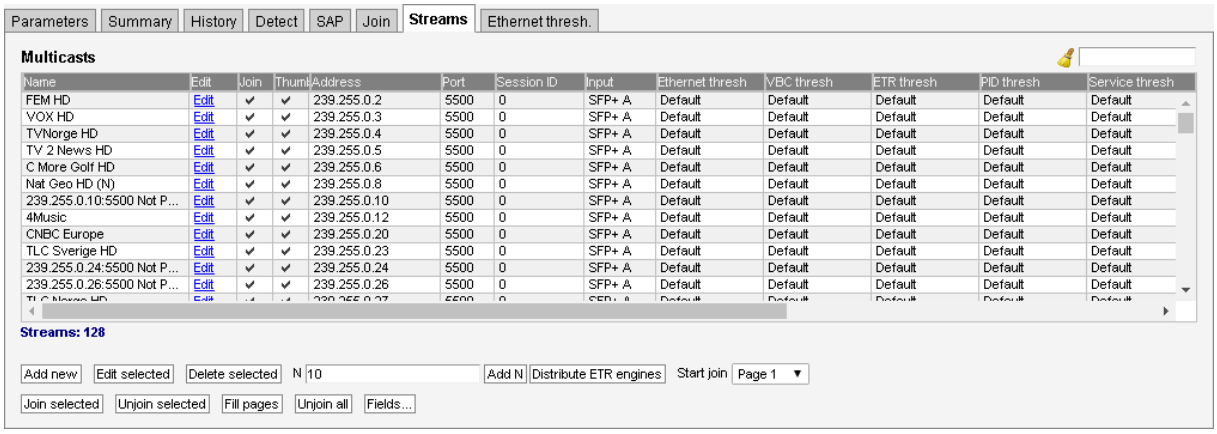
In order for the defined Ethernet multicasts to be monitored by the probe, they must be joined. The **Multicasts — Join** view and the **Multicasts — Streams** view allow the user to select which multicasts that are joined by the probe.

Streams defined in the **Multicasts — Streams** view will appear as available streams on the left hand side of the arrows in this view. Select streams to be monitored by clicking them and moving them to the right hand side of this view using the arrow. Changes should be confirmed by clicking the **Apply changes** button.

Joined streams may be freely associated with the 30 probe pages. The streams will be presented in the Joined multicasts list in the **Multicasts — Parameters** view.

It is possible to flush or fill the multicasts/unicasts to monitor list by clicking the corresponding button. Note that these operations will take effect immediately; it is not necessary to click **Apply changes** for multicasts to be joined or unjoined.

5.4.8 Multicasts — Streams



In this view the operator can define multicasts available to the probe and associate a name with each multicast address. This name will be used by the probe when referring to the multicast. If no name has been defined the probe will use the multicast address:port notation.

It is possible to add, delete or edit several entries simultaneously. Several entries are selected by using the regular *Ctrl + click* or *Shift + click* functionality. When adding new entries the current dialogue values will be used as the template with the values for Name and Address incremented for each.

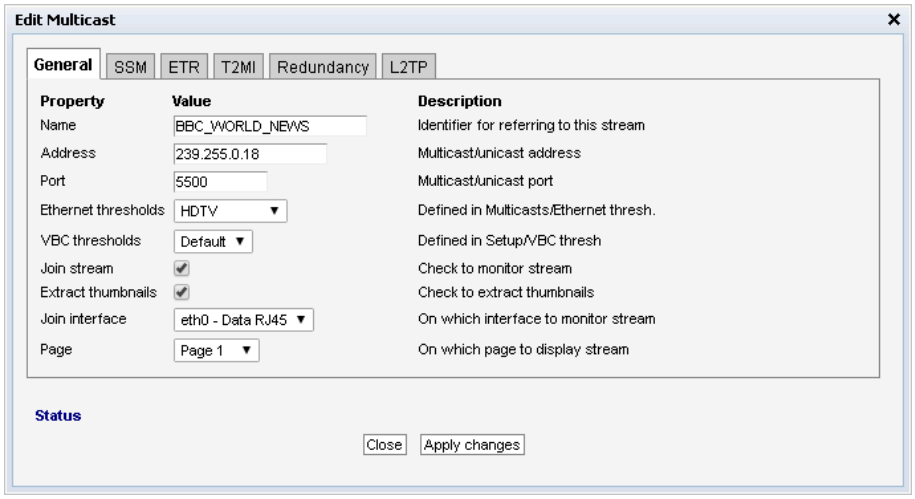
Note that both multicast and unicast addresses can be entered here.

The **Distribute ETR engines** button will distribute the selected streams, with ETR disabled, on the unused ETR engines. An ETR engine is considered unused if no stream with ETR enabled is assigned to it.

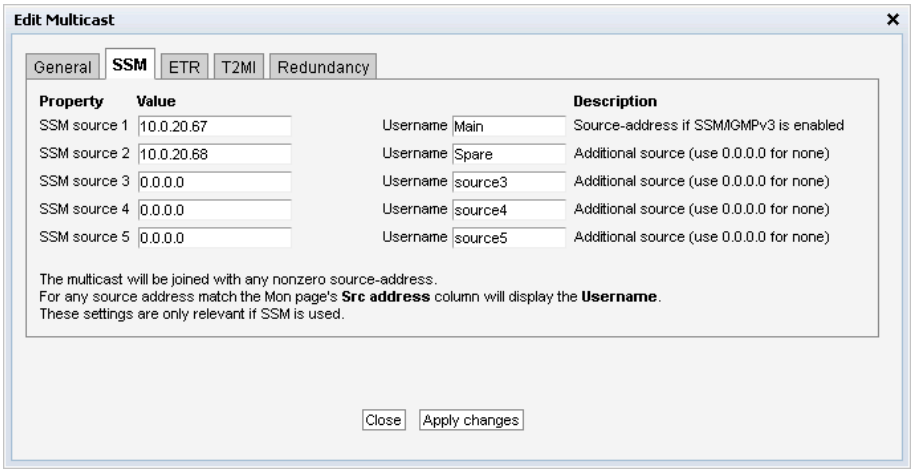
The search field in the upper right corner of the view allows the user to type a text string, and the multicast list is updated to display only streams matching the specified text.

Clicking **Add new** or selecting one or more multicasts and clicking **Edit selected** will open the **Multicast — Streams — Edit** pop-up view. When multicasts have been defined, clicking **Join selected** will join the selected multicasts and enable monitoring. The probe will only analyze joined multicasts. Clicking **Join all** will join all multicasts in the list (up to the licensed maximum number of channels). Unjoining one or more multicasts is done by selecting multicasts and clicking **Unjoin selected** or by clicking **Unjoin all**.

When the Edit button is clicked it is possible to define the following multicast parameters (note that some parameters are only relevant and selectable when the probe is equipped with the correct options):

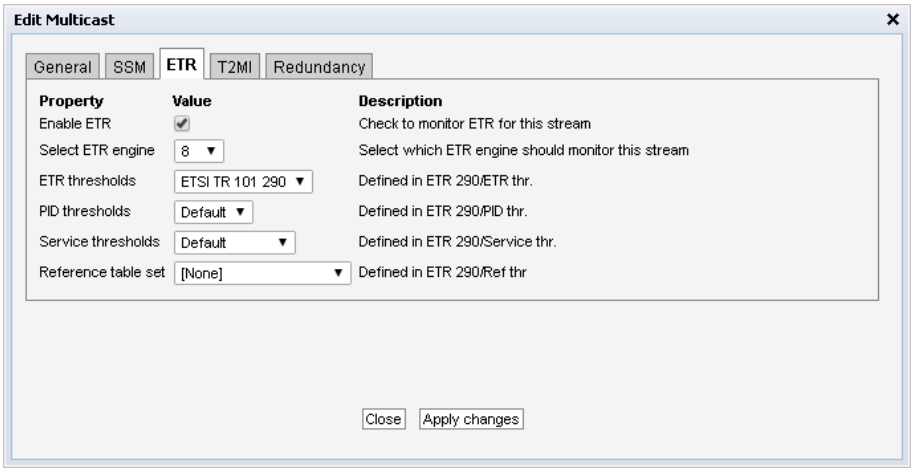


General	
Name:	A name should be assigned to each unicast/multicast. The name will be used throughout the VB330-SW user interface when referring to this stream. It may also be used by an external management system like the VBC Controller.
Address:	The IP address of the unicast or multicast. For a T2MI inner stream enter a dummy address.
Port:	The port number of the unicast or multicast. For a T2MI inner stream enter a dummy port number.
Ethernet thresholds:	The Ethernet thresholds specify various error limits. Selectable Ethernet thresholds templates are defined in the **Multicasts — Ethernet thresh.** view. For a T2MI stream select a dummy threshold template.
VBC thresholds:	The VBC thresholds specify various error limits to be used by VBC Controller to generate alarms. These thresholds are only relevant if the VBC Controller is used. VBC threshold templates are defined in the **Setup — VBC thresh.** view.
Join stream:	Check the 'Join stream' check box to join a multicast or unicast. Only joined streams are analyzed. A stream may also be joined from the **Multicasts — Join** or **Multicasts — Streams** views, and the status of this check box will be updated accordingly.
Extract thumbnails:	When enabled, the probe will generate thumbnails for this multicast. In order to enable this option, *Extract thumbnails* also needs to be enabled in the **Setup — Params** view
Join interface:	Select which interface to join the selected multicast. The data interface(s) are listed.
Page:	For easy navigation, each stream can be assigned a specific page. The names of the pages are defined in **Setup — Pages**.

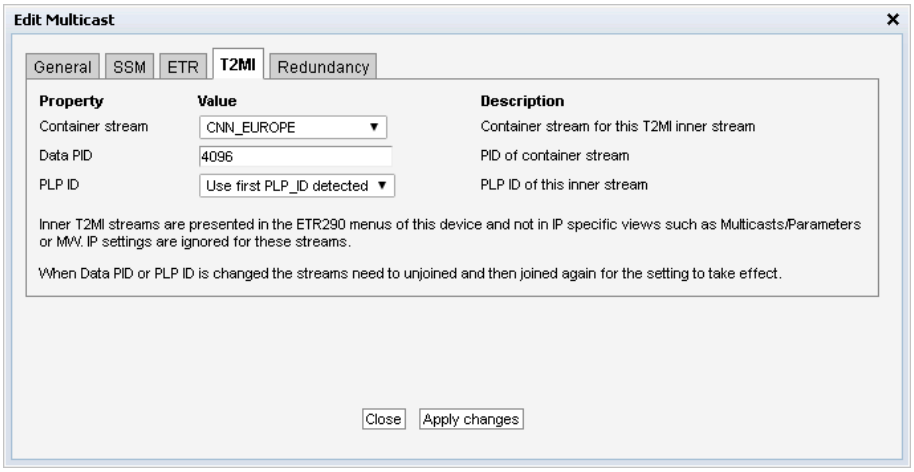


SSM	
SSM source 1:	If source specific multicasts (SSM) is enabled in the VB330-SW and a zero source address is specified for a multicast it will be joined using IGMP version 2 (i.e. without a source). This allows both source specific multicasts and non-source specific multicasts to co-exist in the same network and be joined by the VB330-SW.

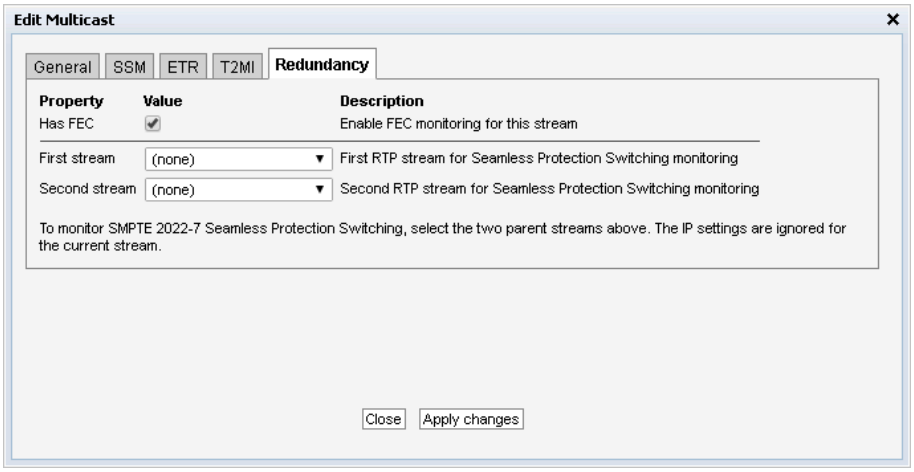
SSM source 2:	Additional SSM source addresses may be specified to enable back-up solutions. Note that it is the operator's responsibility to ensure that a multicast is only transmitted by one SSM source at any time.
SSM source 3:	Additional SSM source address
SSM source 4:	Additional SSM source address
SSM source 5:	Additional SSM source address



ETR (ETR290 Option)	
Enable ETR:	ETR monitoring of a stream will not take place unless it is enabled by this setting. This parameter is only relevant if the probe is ETR enabled.
Select ETR engine:	If the probe is licensed for several Ethernet ETR engines the user may select which engine should be used to analyze the stream. The default ETR engine selection is Ethernet1. It is also possible to use the **Distribute ETR engines** button described above to assign streams to engines.
ETR thresholds:	The ETR thresholds specify various error limits and alarm conditions. Selectable ETR thresholds templates are defined in the **ETR 290 — ETR thresh.** view. The round-robin cycling time is also defined by this threshold template. This parameter is only relevant if the probe is ETR enabled.
PID thresholds:	The PID thresholds specify various error limits and alarm conditions. Selectable PID thresholds templates are defined in the **ETR 290 — PID thresh.** view. This parameter is only relevant if the probe is ETR enabled.
Service thresholds:	The Service thresholds selection defines various error limits and alarm conditions. Selectable service thresholds templates are defined in the **ETR 290 — Service thresh.** view. This parameter is only relevant if the probe is ETR enabled.
Reference table set:	The Reference table set selection is used to compare the tables in the transport stream with a set of stored tables. These tables are defined in the **ETR 290 — Gold TS thresholds** view.



T2MI (T2MI Option)	
Container stream:	For an T2MI inner stream the container stream (outer stream) must be specified. Select the container stream from the drop-down menu. For streams other than T2MI inner streams (none) should be selected.
Data PID:	The container stream PID carrying the inner stream
PLP ID:	The PLP ID for the inner stream. Select a fixed PLP ID value from the drop-down menu or specify that the first detected PLP ID should be used.

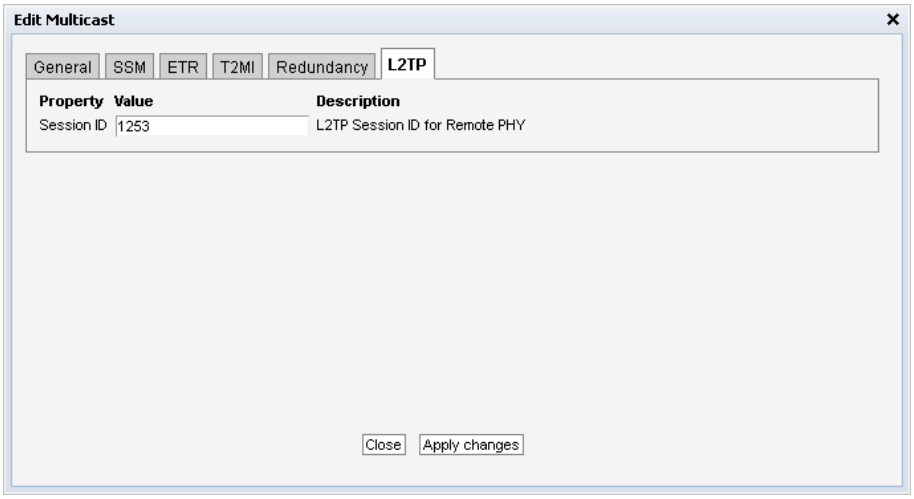


Redundancy	
Has FEC:	The stream carries COP3 (SMPTE 2022-5) Forward Error Correction. If enabled, statistics about FEC drops and correctible errors will be reported for the stream.
First stream:	For a Seamless Protection Switching (SMPTE 2022-7) protected stream, select the first of the two redundant RTP streams here. For other streams, (none) should be selected.
Second stream:	Select the second of the two redundant RTP streams here.

Seamless Protection Switching (SMPTE 2022-7) monitors the same stream transmitted twice. The probe verifies that the two streams combined do not have packet loss and the jitter between the two streams. When two multicast/unicast streams are selected, the probe will report errors report errors if the same

RTP packets are missing from both streams. Errors are also reported if the timing between the two stream exceeds the threshold settings.

Seamless Protection Switching has been optimized for monitoring SDI over IP (SMPTE 2022-6) streams.

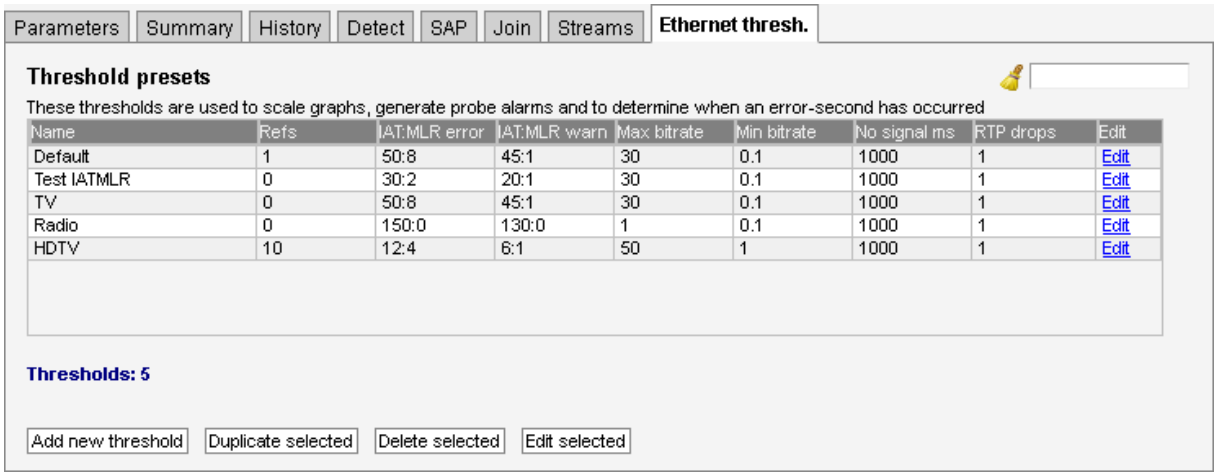


L2TP	
Session ID:	The session ID of the L2TP stream is specified here (or 0 if not used). It is used together with the multicast address to identify the L2TP stream.

L2TP (remote PHY) streams are mapped into multicasts. In order to identify the correct stream the multicast address is entered in the **General** tab and the session ID of the L2TP stream is specified here. The port number is not used, and will be shown as 0.

To identify available session IDs, join the stream first and then use the **Multicasts — Detect** view to see the session IDs that are available. Both IPv4 and IPv6 is supported.

5.4.9 Multicasts — Ethernet thresh.



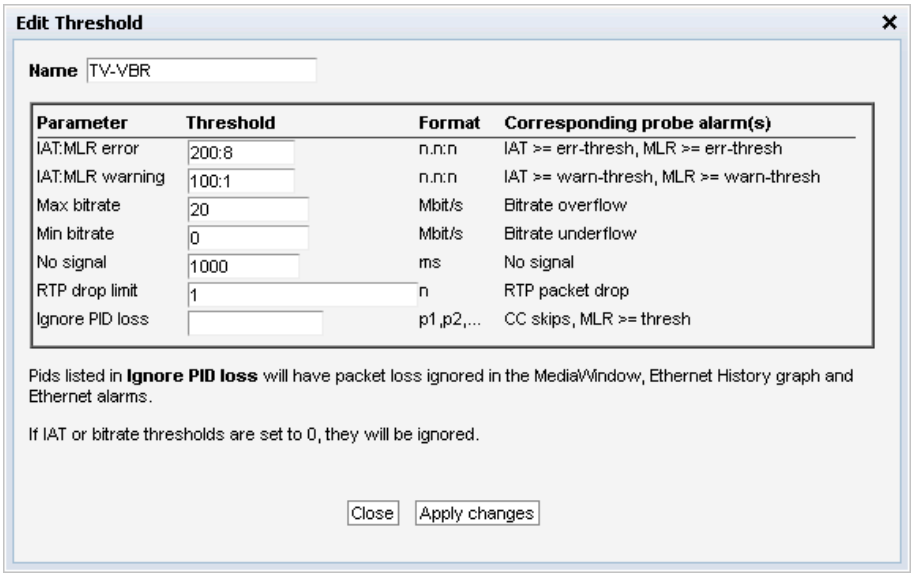
Thresholds are used to determine when to actually raise an alarm upon detection of an error. The Ethernet thresholds are used for generating Ethernet probe alarms as well as for calculating error-seconds. Error seconds and ETH probe alarms are issued whenever measurements exceed the defined threshold levels

for a parameter. Ethernet thresholds are also used to scale some graphs like the MediaWindow graphs. The alarm level of each of these alarms is set in the **Alarms — Alarm setup** view. Note that it is also possible to disable alarms in the **Alarms — Alarm setup** view.

The **Multicasts — Ethernet thresh.** view makes it possible to define threshold values that operate at stream level. Thresholds are associated with each stream in the **Multicasts — Streams — Edit** view. There are two different ways of creating user-defined thresholds. To create a new threshold template from scratch the operator should click the **Add new threshold** button. A pop-up window will appear allowing the user to define alarm conditions. Another way of creating a user-defined threshold template is by highlighting one of the threshold templates already defined and then click the **Duplicate highlighted** button.

Deleting a threshold template is done by highlighting the threshold template that should be removed and clicking **Delete selected**. It is possible to delete or edit several entries simultaneously. Several entries are selected by using the regular *Ctrl + click* or *Shift + click* functionality. Click the **Edit** button to edit one or more selected threshold templates. Note that the predefined 'Default' threshold template cannot be deleted or changed.

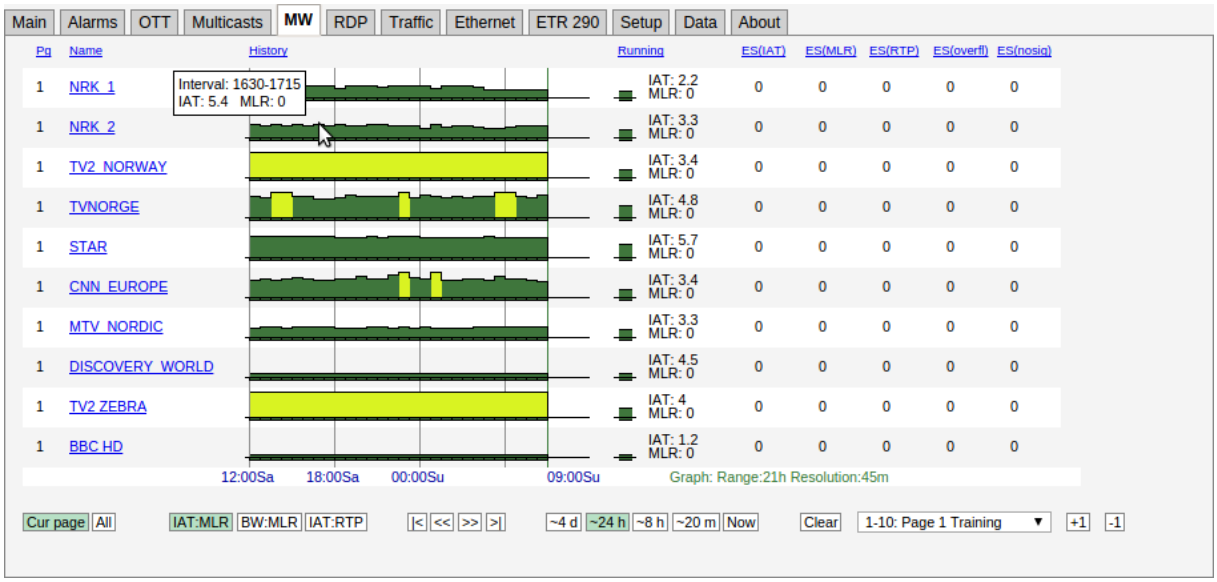
In the threshold presets list the 'Refs' column displays how many streams are associated with each stream threshold template.



Ethernet thresholds	
Name:	A text string that identifies the Ethernet threshold
IAT:MLR error:	This threshold contains error limits for IAT (Inter-packet Arrival Time) and MLR (Media Loss Rate). The IAT limit is the first parameter (before the colon), the MLR limit is the last parameter. If the IAT limit is exceeded the alarm 'IAT >= err-thresh' will be raised. If the MLR limit is exceeded the alarm 'MLR >= err-thresh' will be raised. The severity (and hence the color used in the MediaWindow view) for IAT:MLR errors depend on the severity assigned to these alarms in the **Alarms — Alarm setup** view. Note that error seconds based on MLR are counted regardless of this threshold if one or more packets are missing.

IAT:MLR warning:	This threshold contains warning limits for IAT (Inter-packet Arrival Time) and MLR (Media Loss Rate). The IAT limit is the first parameter (before the colon), the MLR limit is the last parameter. If the IAT limit is exceeded the alarm 'IAT >= warn-thresh' will be raised. If the MLR limit is exceeded the alarm 'MLR >= warn-thresh' will be raised. The severity (and hence the color used in the MediaWindow view) for IAT:MLR errors depend on the severity assigned to these alarms in the **Alarms — Alarm setup** view.
Max bitrate:	The maximum bitrate in Mbit/s. An alarm will be raised if the stream bitrate exceeds the maximum bitrate.
Min bitrate:	The minimum bitrate in Mbit/s. A value of 0 will never generate an alarm. A value of 0.1 Mbit/s will generate an alarm if the minimum bitrate threshold is less than 0.1 Mbit/s.
No signal:	Number of milliseconds without receiving any signal before the 'No signal' alarm is raised
RTP drop limit:	If the number of lost RTP packets exceeds the RTP drop limit an alarm will be raised. Note that error seconds based on packet drops are counted regardless of this threshold.
Ignore PID loss:	A comma separated list of PIDs for which the probe should ignore packet loss. Packet loss that affects these PIDs will not result in an error-second count, and the ETR monitoring engine will not count these errors.

5.5 MW (Media Window)



The **MW** Media Window view provides an at-a-glance status for each of the multicasts/unicasts being monitored. From the graphs it is easy to see the jitter characteristics of the signal and if there is packet loss or CC errors present in the signal. Periods of no signal are also displayed.

The measurements are always aggregated over a time interval – typically one second. The IAT(max) is the maximum time measured between two neighboring IP frames within the measurement time interval (the peak packet Inter-arrival time). IAT is expressed in milliseconds.

The MLR is the peak estimated number of lost MPEG-2 Transport Stream packets inside any second within the actual time period. The number of lost TS packets is derived from the continuity counters inside the TS packet headers.

A common scenario is to have 7 TS packets per UDP frame. Losing an IP packet will therefore usually (but not always) result in an MLR of 7 (not always the case because some TS packets such as null packets or PCR packets do not carry a valid CC field).

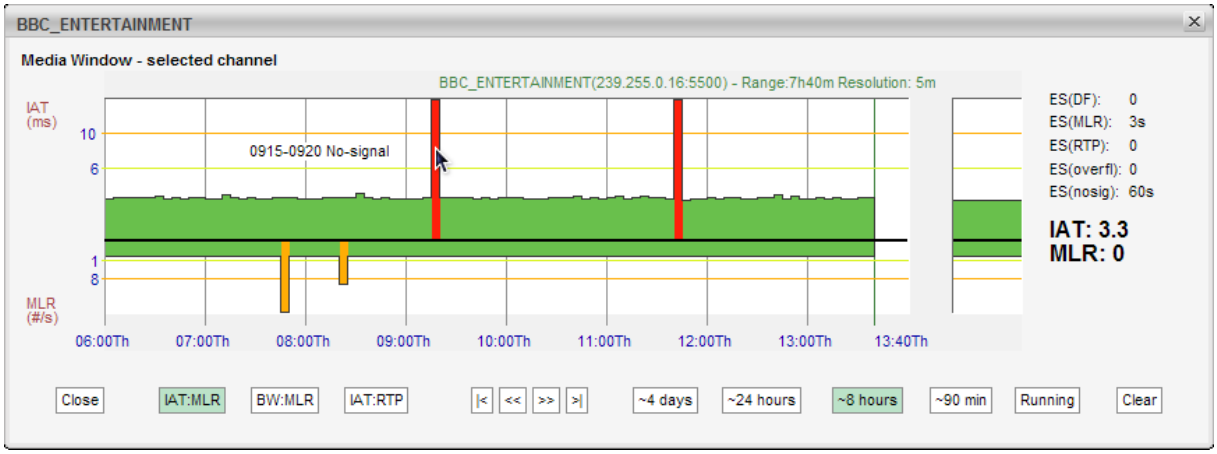
Bridge Technologies' patented **Media Window** presents both jitter and packet loss measurements in one graph, with jitter (IAT) values growing upwards (+ve Y) and packet loss (MLR) growing downwards (-ve Y). Each sample along the x-axis corresponds to a measurement time-interval that depends on the range of the graph selected. Periods of no sync are also displayed in the graph.

Error-second statistics for the graph-interval is displayed to the right. As the graphs are zoomed or scrolled the error-second statistics is updated as well as the graphs.

Tool-tip provides the exact jitter (IAT) and packet loss (MLR) values for a selected bar in a selected graph, the denotation is IAT::MLR. The current graph value displayed under 'Running' provides the maximum MLR and IAT values measured during the last 3 seconds.

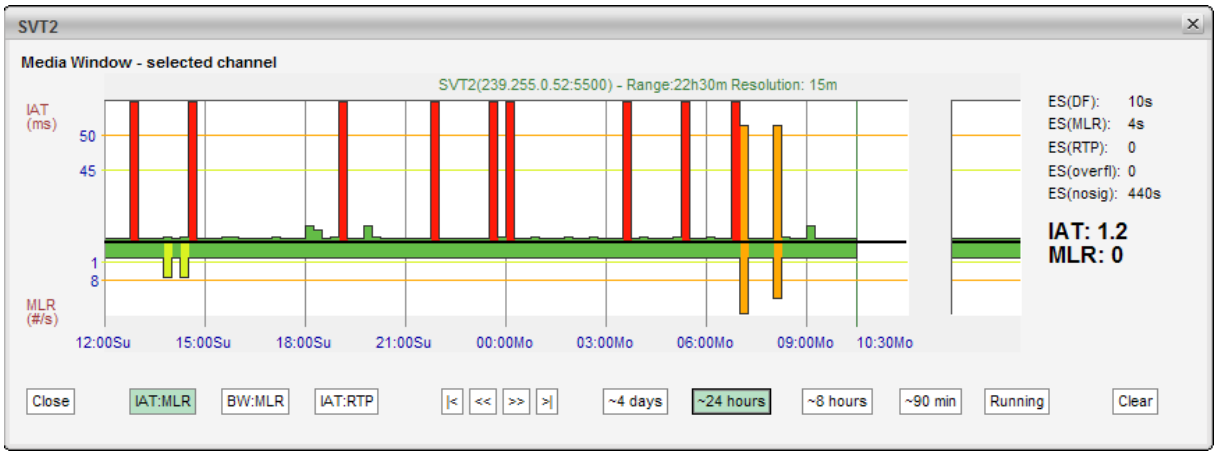
Red color is used to indicate that within the period represented by the bar there has been one or more occurrences of no-signal. Orange is used to indicate error while yellow indicates warning. The error and warning thresholds are allocated to each multicast in the **Multicasts — Streams** view.

The user determines whether only multicasts associated with the currently selected page should be displayed (by clicking the **Cur page** button), or if all joined multicasts should be presented in one list (by clicking the **All** button). The time window buttons allow selection of x-axis resolution in the graphs, and by using the arrow buttons it is possible to move the timeline to view an error incident more accurately. Clicking **Clear** will clear all graphs. Note that clearing graphs cannot be undone. Clicking the **+1** button will display the next page. Clicking the **–1** button will display the previous page.



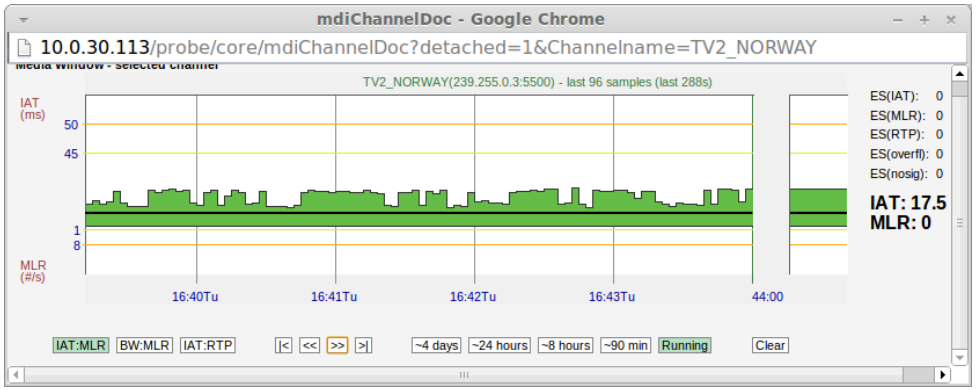
By zooming and panning the user can pinpoint more accurately when errors occurred. In the above diagram tooltip reveals that 'No signal' occurred between 9:15 and 9:20.

5.5.1 Media Window — Selected channel



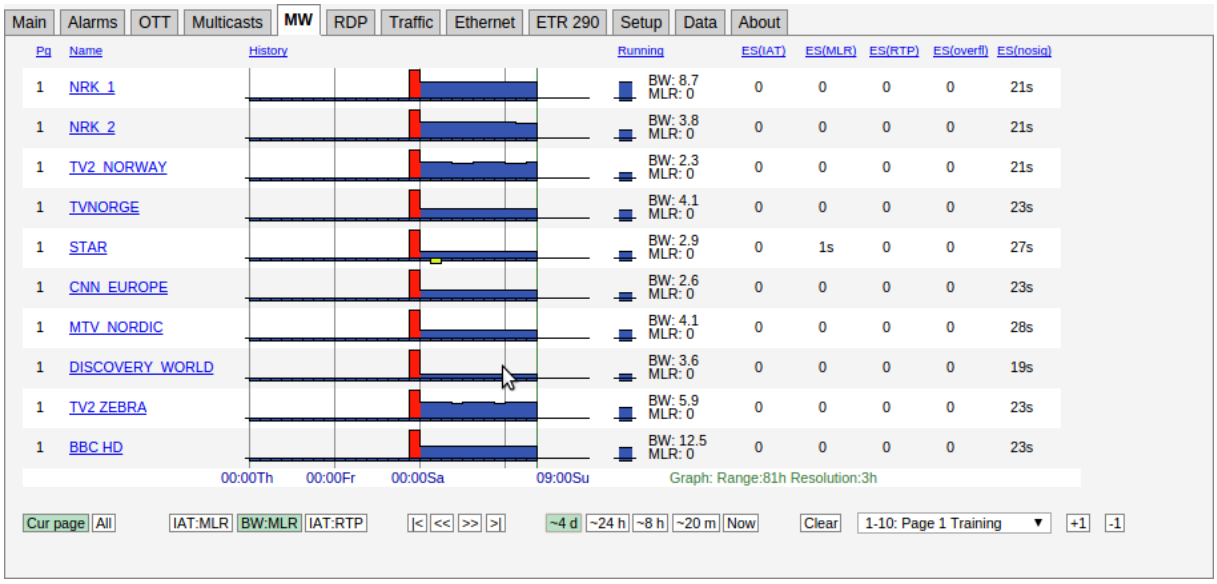
The **Media Window — selected channel** view is activated by clicking a multicast label in the **MW** page. Clicking anywhere in the running graph will zoom in, unless you already are at the maximum zoom level.

This high-resolution version of the **Media Window** reveals more details than the compressed version. There are 3 times more samples along the X-axis, and the graph indicates visually the error and warning thresholds. Note that the time windows of the regular **Media Window** and **Media Window — selected channel** are not exactly the same, even if the same time window has been selected for both views.



By clicking the **Popup** button, a pop-up window will appear. This separate window can be used to display the selected channel even when navigating away from the probe. This also provides the ability to monitor media windows for several streams without starting several browser sessions.

5.5.2 Media Window — Bandwidth graph

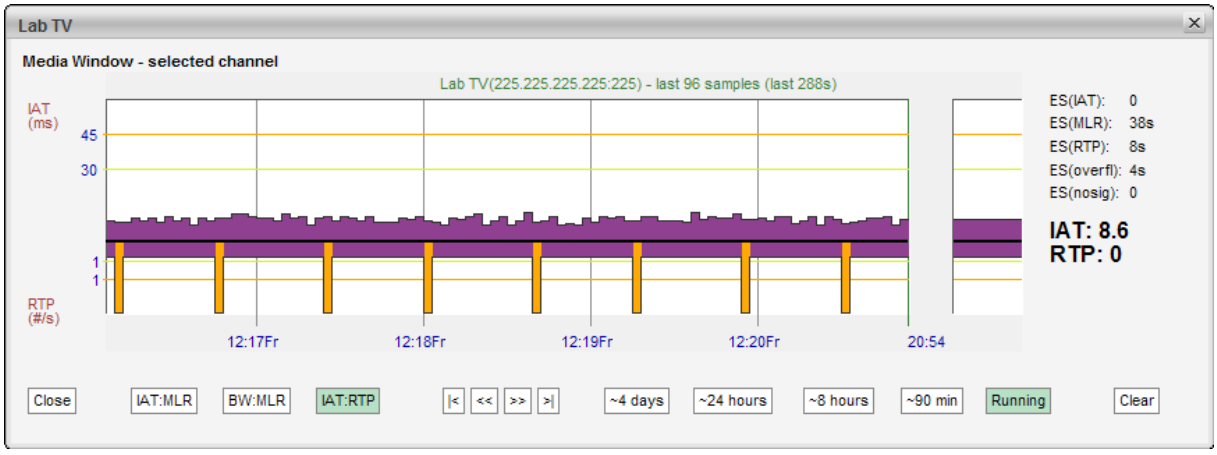


By clicking the **BW:MLR** button the graph displays the peak bandwidth as a function of time. The negative part of the composite graphs is still the packet loss (i.e. the MLR).

If the stream contains a transport stream (mapping TS/x) the bitrate corresponds to the **Multicasts** parameter **Net bitrate** (i.e. bitrate excluding null packets). Otherwise the bitrate is the UDP payload bitrate corresponding to the **Multicasts** parameter **Curr bitrate**.

The bandwidth error threshold is configured in the **Multicasts — Ethernet thresh.** view.

5.5.3 Media Window — Inter Arrival Time graph

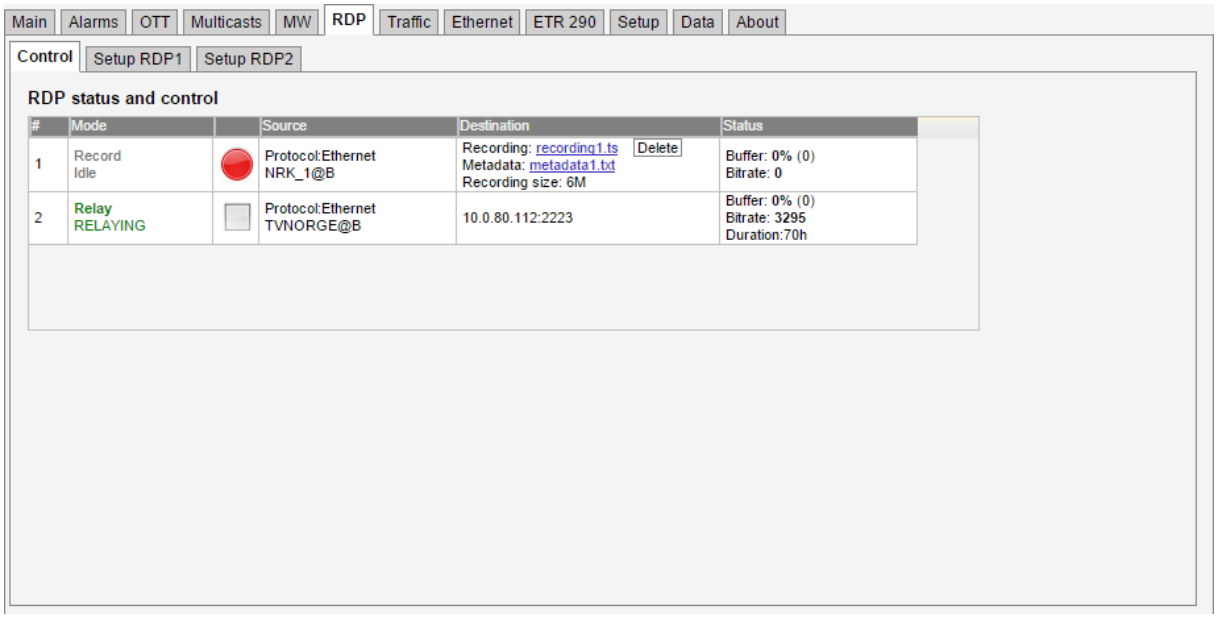


By clicking the **IAT:RTP** button the graph displays the packet jitter as a function of time. The composite graphs displays the RTP packet loss below the X-axis. If the monitored stream is not RTP encapsulated, IAT will be represented by grey color and there will never be any indication of packet loss in the graph.

5.6 RDP (Return Data Path)

The Return Data Path feature enables forwarding of streams from any probe interface to another destination IP address. Stream may also be recorded to file, either directly or triggered by alarms. The probe supports forwarding or recording of two streams in parallel.

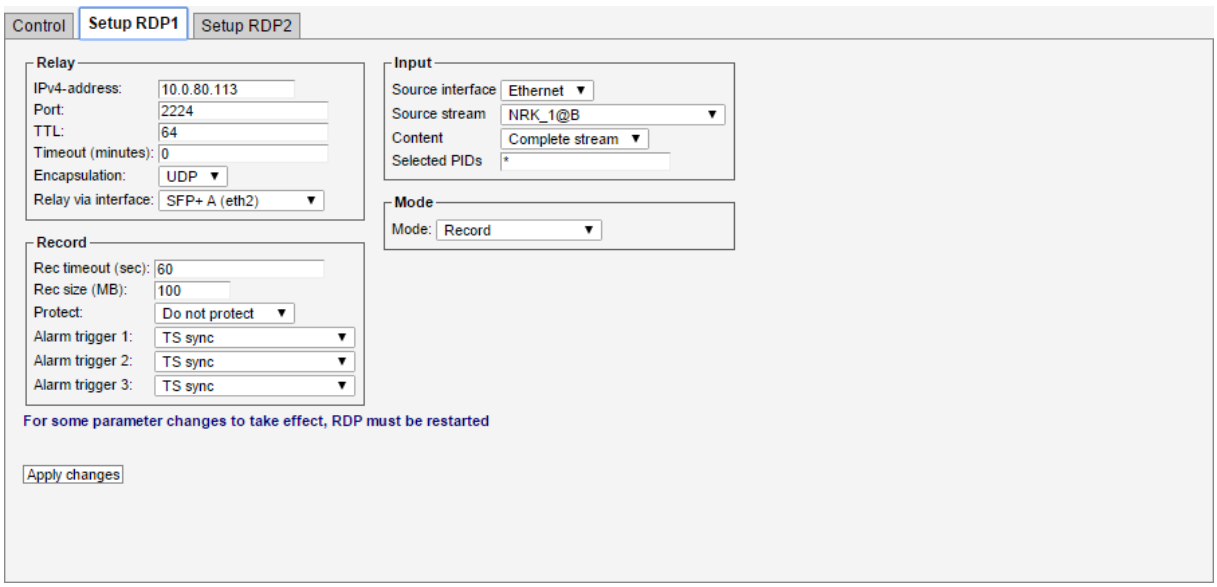
5.6.1 RDP — Control



Click the icons in the Control tab to activate or de-activate an RDP engine. There are different icons for controlling RDP engines depending on whether they are configured to relay or record. The state of each RDP engine is restored after a reboot.

For recordings and triggered recordings the last recording is made available in the Destination column along with the metadata file. The metadata file contains basic information about the recording such as the recording size, list of PIDs and CC-errors for each PID. In the case of triggered recording, the alarm causing the recording is also included. Pressing the Delete button deletes the recording. For triggered recordings the number of recordings is stated in the Status column. Pressing the Delete button resets this counter. The buffer utilization is stated as a percentage and should never approach 100% for correct relaying or recordings.

5.6.2 RDP — Setup



Each of the RDP engines is configured separately. First the Mode is selected. Depending on the mode either the Relay or Record settings needs to be configured. The Input selects the stream or interface to relay or record.

These are the settings:

Mode and Input	
Mode:	Select whether this RDP engine should relay, record or trigger-record.
Source interface:	The source interface drop-down menu allows selection of available input signals.
Source Stream:	When Ethernet input is selected the user selects the stream to forward or record. Ethernet streams being joined/monitored by the probe are available for selection.
Content:	The user selects the service to be relayed or recorded, or alternatively selects that the complete stream should be used. The PIDs associated with the service are automatically displayed in the 'Selected PIDs' field, and these may be edited if required.
Selected PIDs:	The user can specify the PIDs to be selected, default is all PIDs. Typically PAT and PMT PIDs should be forwarded in addition to video and audio PIDs, however this depends on the equipment receiving the forwarded stream.

When mode **Relay over IP** has been selected, the RDP parameters are:

RDP Ethernet	
IPv4-address:	The unicast address or multicast address to forward to. Multicast addresses are in the range 224.0.0.0 – 239.255.255.255.
Port:	The port to forward to. The combination of IP address and port fully describes the destination address.
TTL:	The Time-To-Live flagging of the relayed signal. The default value is 64.
Timeout:	The relaying period in minutes. If the value 0 is selected, no timeout applies, and relaying will continue until it is stopped manually.
Encapsulation:	The encapsulation format of the relayed stream. **UDP** or **RTP** may be selected.
Relay via interface:	The available interfaces for forwarding the stream are listed.

When mode **Record** or **Trigger recording** has been selected the options are:

Record and trigger options	
Rec timeout:	The maximum recording time in seconds. This setting enables the user to limit recordings of low-bitrate streams.
Rec size:	The total file size of the recording. When in alarm trigger mode the resulting recording will consist of a fixed sized portion of data before the alarm is raised and the remaining recording from data after the trigger occurred.
Protect:	When in alarm trigger mode the user may select to protect a recording from being overwritten due to a new alarm occurrence. The user may select between 'Never overwrite', 'Do not protect', '30 seconds', '60 seconds' and '5 minutes'.

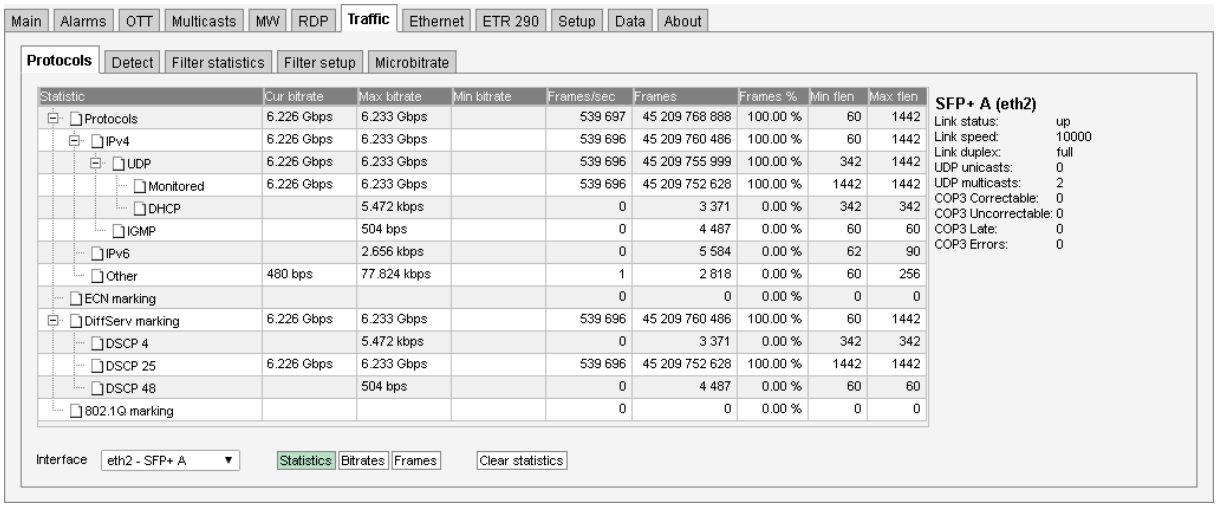


Alarm trigger 1–3:	Select a maximum of three different alarms that should trigger recording. Note that a recording will start upon a transition from status *OK* to status *alarm*. Alarms that have been disabled in the **Alarm — Alarm setup** view will be shown in brackets – these will never trigger a recording.

The maximum recording size depends on the amount of free disk on the probe, up to a maximum of 1500 Mbyte.

5.7 Traffic

5.7.1 Traffic — Protocols



The **Protocols** view allows monitoring of IP traffic on the selected port in terms of the protocols used.

The interface can be selected using the drop-down at the bottom of the page. Clicking the **Clear statistics** button will reset displayed values.

The following measurements are presented, depending on which statistic is selected:

Statistics	
Statistic:	The protocol for which the following measurements apply
Cur bitrate:	The current total bitrate for this protocol (measured over the last 1s period)
Max bitrate:	The maximum bitrate during any 1s period
Min bitrate:	The minimum non-zero bitrate during any 1s period
Frames/sec:	Traffic speed in number of IP packets per second
Frames:	Number of Ethernet frames
Frames %:	Percentage of total number of frames
Min flen:	Minimum Ethernet frame length
Max flen:	Maximum Ethernet frame length

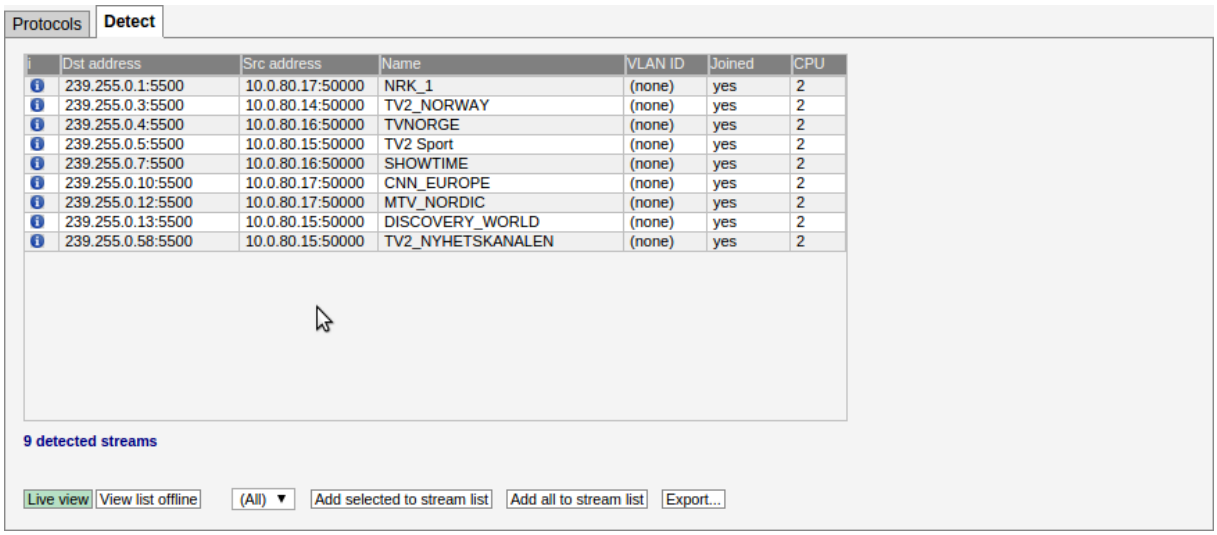
Bitrates

Statistic:	As above
Cur bitrate:	As above
Bitrates:	A graph displaying the bitrate over time, displaying the last five minutes
Bitrate graph:	Click the bitrate graph button to display a detailed bitrate graph for the specified protocol

Frames	
Statistic:	As above
Frames/sec:	Traffic speed for this protocol expressed in number of IP packets per second
Frames:	A graph displaying frames per second over time, displaying the last five minutes
Frames graph:	Click the frames graph button to display a detailed frames per second graph for the specified protocol

Interface statistics	
Link status:	Displays whether the interface is up or down
Link speed:	Displays the interface speeds, as bits per second
Link duplex:	Indicates whether the interface is operating at full or half duplex
UDP unicasts:	The number of detected UDP unicasts
UDP multicasts:	The number of detected UDP multicasts
COP3 Correctable:	Total count of dropped payload IP packets that are correctable by the FEC
COP3 Uncorrectable:	Total count of dropped payload IP packets that cannot be corrected by the FEC
COP3 Late:	Payload or FEC packets are received slightly too late according to the buffer model and may result in errors in another implementation of the specifications. The number of packets with this error.
COP3 Errors:	Either the L/D parameters are not consistent across the streams or payload-/FEC packets are received too late or too early according to the buffer model. The number of packets with these errors.

5.7.2 Traffic — Detect



The **Traffic Detect** view displays all UDP traffic sensed by the probe. Note that promiscuous network mode should be enabled in the **Setup — Params** view for the probe to detect all traffic, and not only multicasts already joined by the probe. Note that generally the upstream switch or router will not output streams that are not joined by downstream equipment, i.e. usually only joined streams will be available for monitoring.

If the unicast/multicast destination address is known to the probe (i.e. listed in the **Multicasts — Streams** view) the stream's **Name** is looked up, otherwise a generic name is used.

When the **Traffic — Detect** view is entered after probe booting, the probe will continuously try to detect streams. Click the **View list offline** button to view the stream list in offline mode. Click the **Refresh** button to update the stream list in offline mode.

The source address makes it possible for the probe to distinguish between multicasts with the same destination IP address and port, provided that **Source specific multicasts** has been enabled in the **Setup — Params** view.

If the stream is currently joined by the probe (i.e. the probe is currently monitoring the stream), the **Joined** field is set to yes.

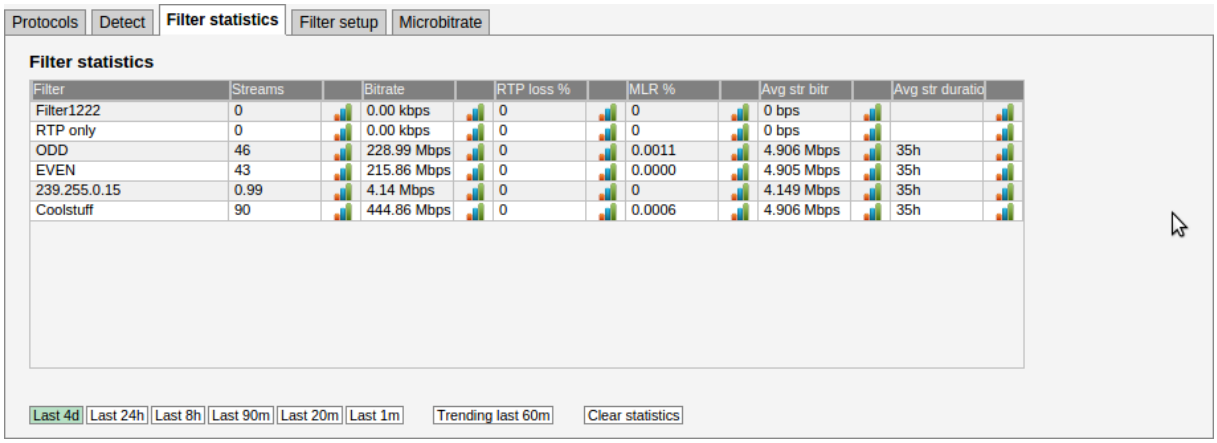
Detected streams can be added to the probe's stream list by selecting streams and clicking the **Add selected to stream list**. To add all detected streams the **Add all to stream list** button can be pressed. Only streams not already in the probe's stream list are considered. Clicking the **Export** button will generate an XML-file that opens in a new window.

A drop down menu allows filtering of detected streams, making is possible to view streams of a specific type only. Stream types are defined in the **Traffic — Filter setup** view. If the AEO option is enabled for the probe the Detect list will contain the following additional columns: Mapping, signal, RTP drops, CC errors and Bitrate. These parameters are the same as on the **Multicasts** page.

ⓘ:	Click the blue information icon to pop up the detailed stream info.
Dst address:	The multi- or unicast address
Src address:	The stream source address
Name:	The stream name, as defined in the **Multicasts — Streams** view. A generic name will be used for multi- or unicasts not defined by the user.

Interface:	The stream source network interface (physical or VLAN)
Joined:	If the stream is joined by the probe this field will read ‘Yes’.
CPU:	The probe CPU used to analyze the stream (1-7)
Mapping:	The transport stream to IP mapping. Typically seven transport stream packets are mapped into one IP packet.
Signal:	The duration of stream availability
RTP drops:	The number of detected RTP drops for the stream. This is only valid if the stream is RTP encapsulated.
CC errors:	The number of detected continuity counter errors for the stream.
Bitrate:	The stream bitrate

5.7.3 Traffic — Filter statistics



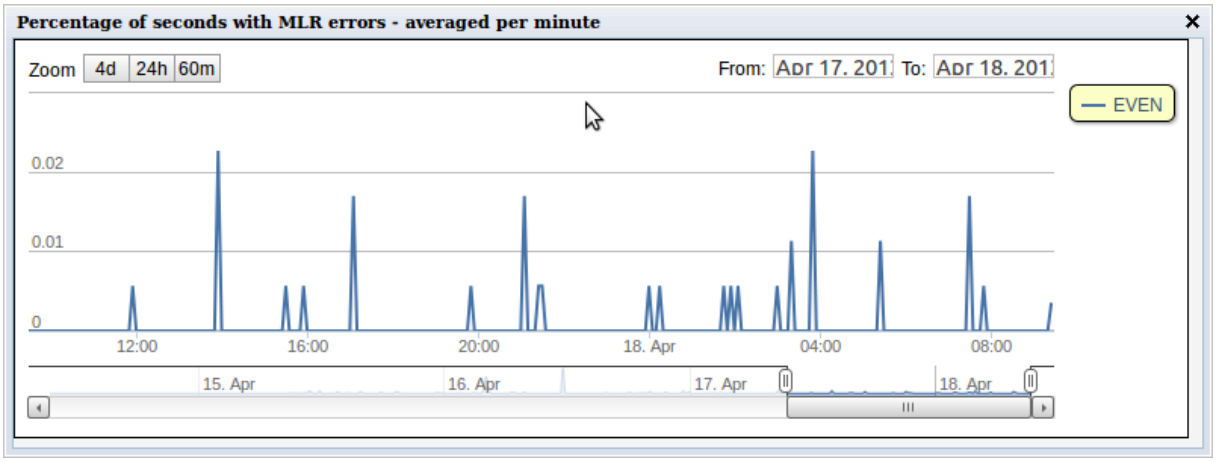
The **Traffic — Filter statistics** view makes it possible to view statistics for different stream types. Stream types are defined by the user in the **Traffic — Filter setup** view.

Statistics is displayed for a time period selected by clicking one of the time duration buttons.

Filter statistics:	
Filter:	The filter name, as defined by the user in the **Traffic — Filter setup** view.
Streams:	The number of streams matching the associated filter.
Bitrate:	The total summed bitrate for streams matching the associated filter.
RTP loss %:	Percentage of time an average stream that matches the filter experiences RTP packet loss inside selected time period. Example: If the **Last 1m** period is selected and there are totally three streams caught by filter: • stream A: present for 60 seconds, 4 RTP error seconds • stream B: present for 30 seconds, 0 RTP error seconds • stream C: present for 30 seconds, 5 RTP error seconds RTP loss % = 9ES / 120s RTP loss % = 9ES / 3streams / 120s *100% = 7.5%

MLR %:	Percentage of time an average stream that matches the filter experiences MLR inside selected time period. The calculation is similar to that for RTP loss %.
Avg str bitr:	The average bitrate for streams matching the associated filter.
Avg str duration:	The stream duration is calculated for each stream by identifying the stream's average stream alive counter inside the selected time period, then multiply by 2. The stream alive counter is the number of seconds the stream has existed. This gives accurate results for streams that begin within the selected time period, but may give up to twice the real bitrate for streams that begin (long) before the selected period. Examples: a stream exists for 100 seconds, and begins within the selected period. The calculation becomes: Stream duration = (1+2+. . . +100)/100*2 = 101 If the same stream started 50 seconds before the selected period, the calculation becomes: Stream duration = (51+52+. . . +100)/50*2 = 151

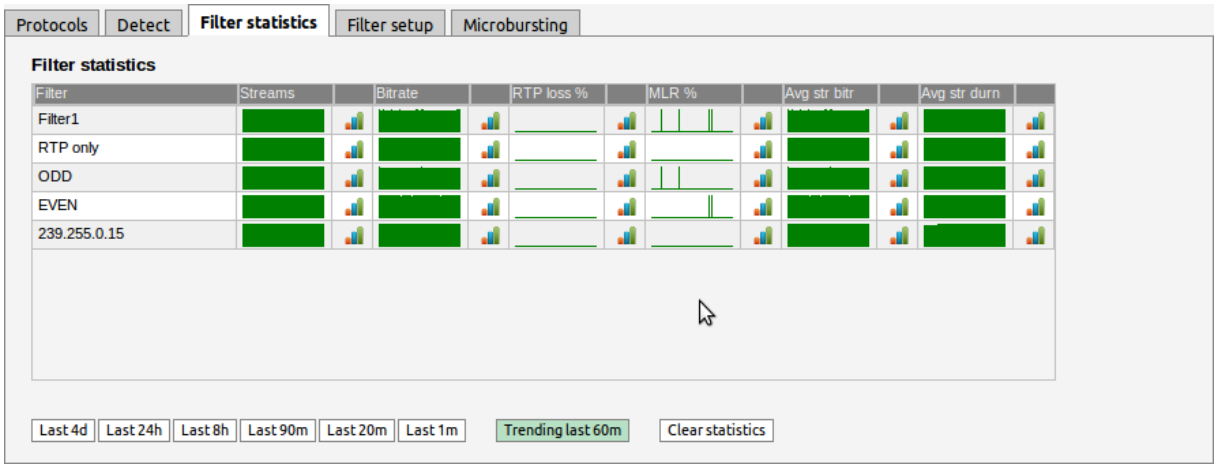
Clicking the icon next to each value brings up the detailed graph window.



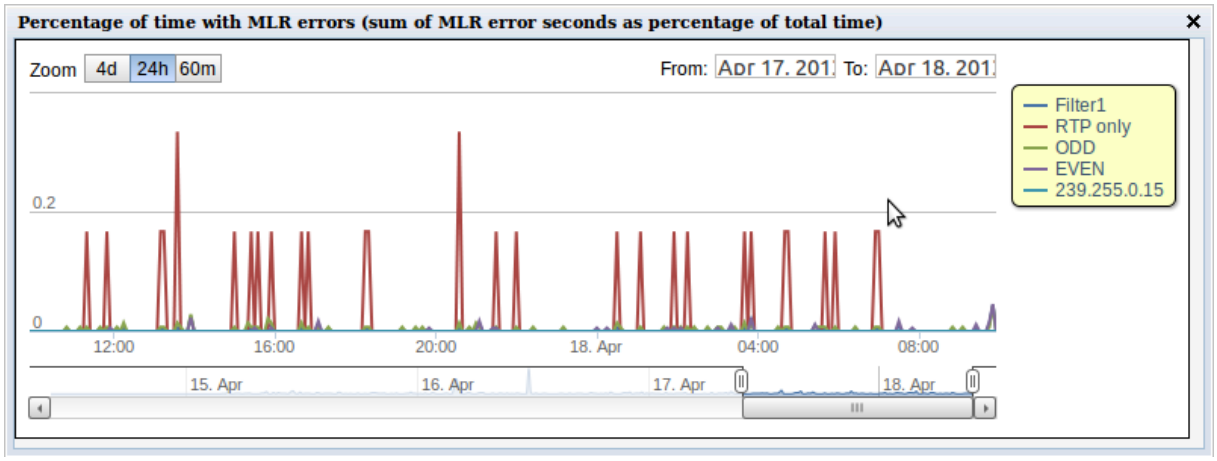
The detailed graph window displays up to 4 days of history.

Trending

Clicking the **Trending last 60m** button will present at-a glance trending graphs for each parameter for the last 60 minutes.

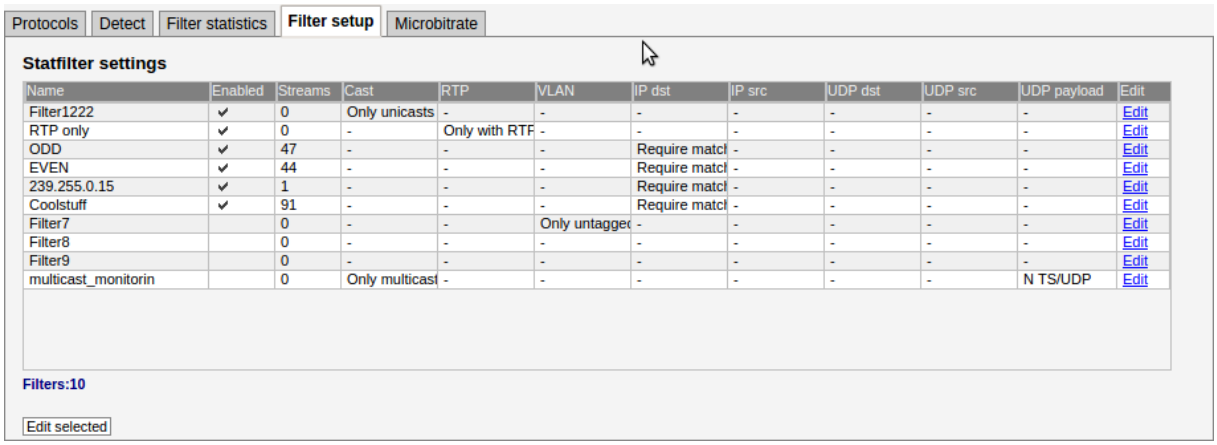


Clicking a graph icon displays the corresponding detailed graph for the selected filter. Clicking the trend graphs itself will bring up the same detailed graph but will plot all the filters so that they can easily be compared.



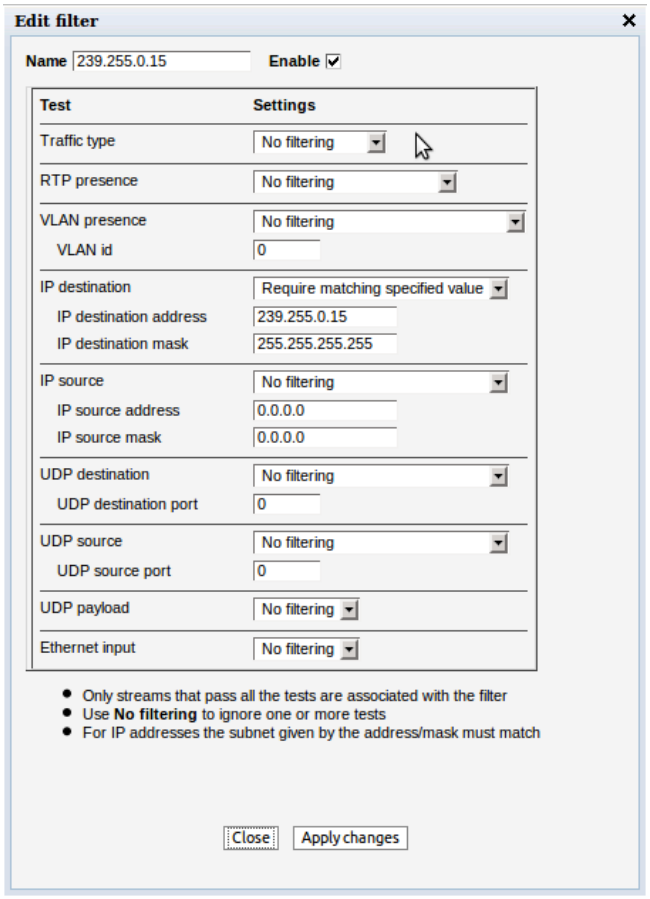
The detailed trending graph above displays MLR errors for all filters.

5.7.4 Traffic — Filter setup

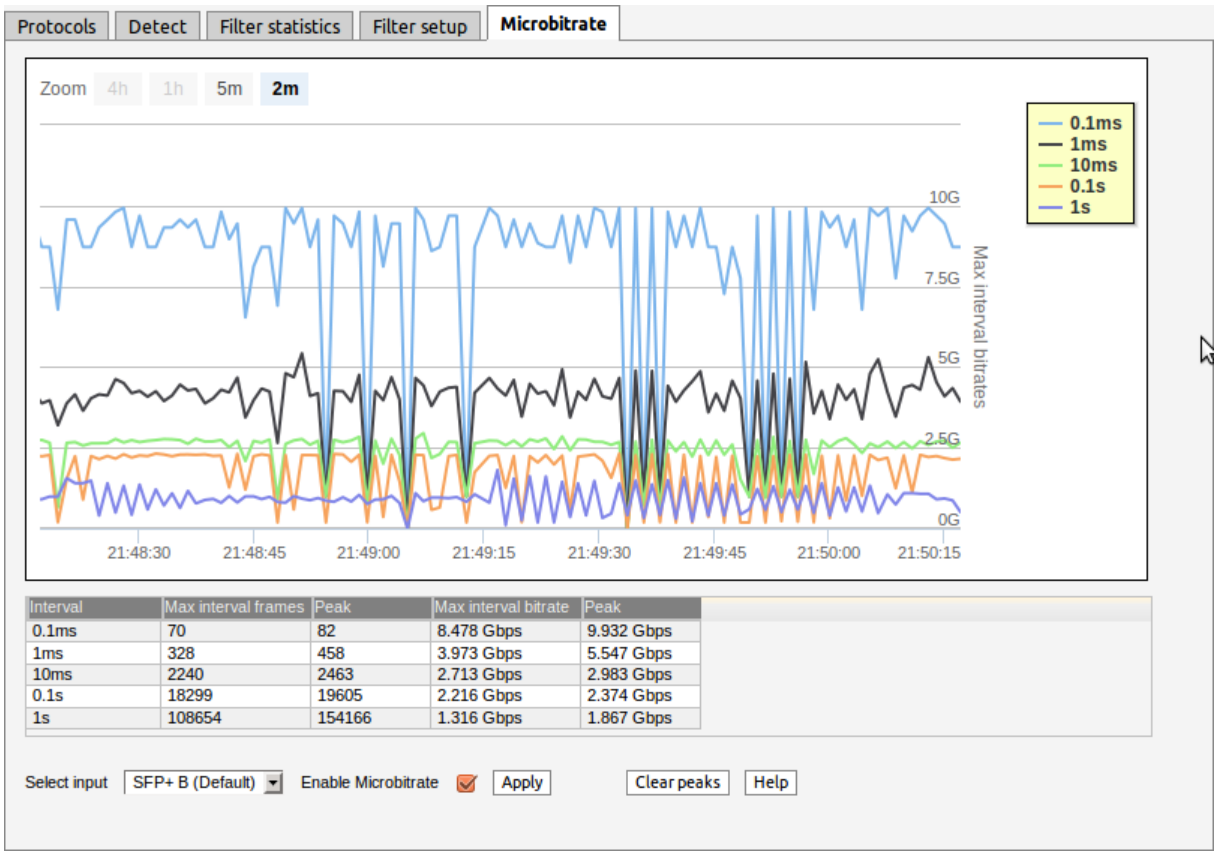


The **Traffic — Filter setup** view makes it possible to define stream filter requirements affecting the **Traffic — Detect** and **Traffic — Filter statistics** views. Ten filters can be defined and enabled by the user.

Statfilter settings:	
Name:	A text string defining the filter
Enabled:	Only enabled filters are in use
Streams:	The number of streams matching filter requirements
Cast:	The type of stream: *No filtering*, *Only unicasts* or *Only multicasts*
RTP:	The RTP mode: *No filtering*, *Only with RTP header* or *Only without RTP header*
VLAN:	VLAN selection mode: *No filtering*, *Only tagged traffic*, *Only untagged traffic* or *Require matching specified value* (a specific VLAN ID).
IP dst:	The IP destination address mode: *No filtering* or *Require matching specified value* (a specific IP address/netmask)
IP src:	The IP source address mode: *No filtering* or *Require matching specified value* (a specific IP address/netmask)
UDP dst:	The UDP destination mode: *No filtering* or *Require matching specified value* (a specific UDP port number)
UDP src:	The UDP source mode: *No filtering* or *Require matching specified value* (a specific UDP port number)
UDP payload:	The UDP payload mapping type: *No filtering*, *7 TS/UDP* or *N TS/UDP* (any integer number of TS to UDP mapping)
Edit:	Click the Edit link to edit filter settings.



5.7.5 Traffic — Microbitrate



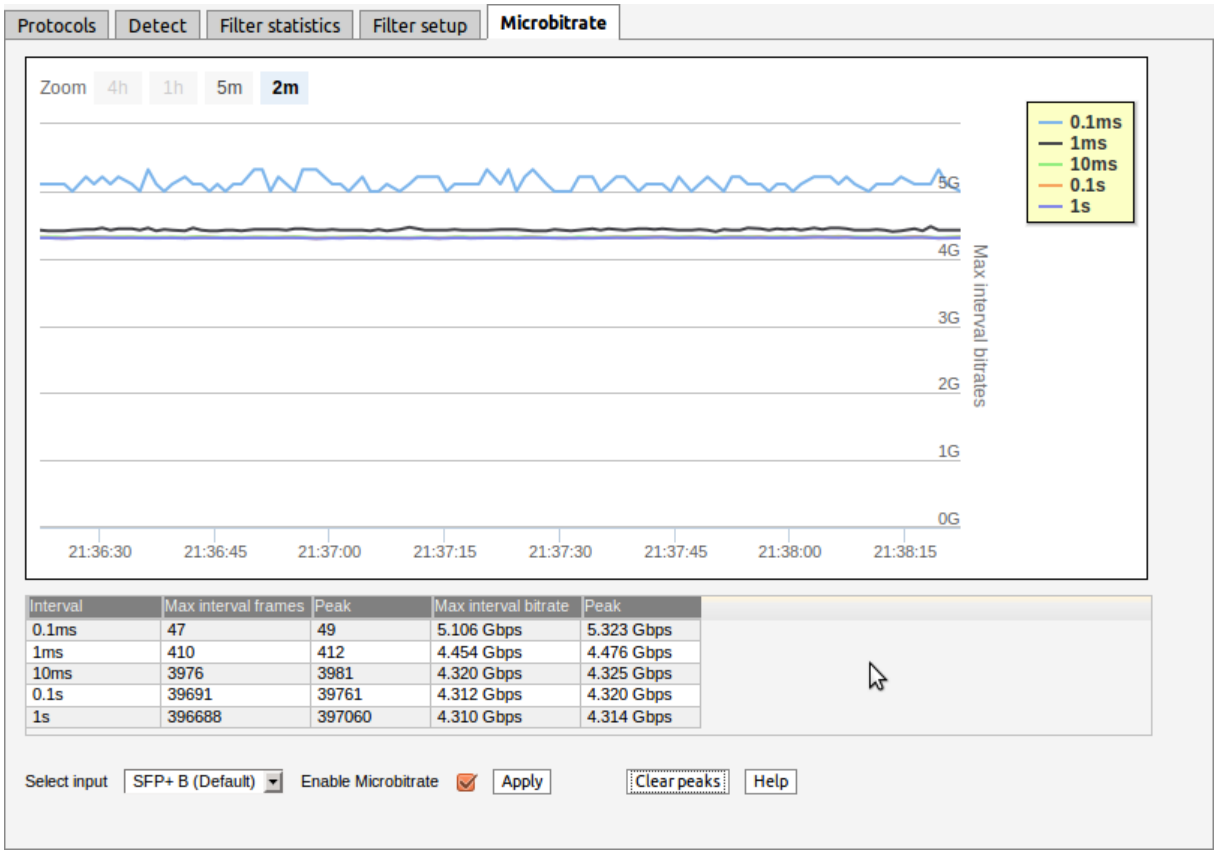
The Microbitrate feature allows sampling of bitrate at various sampling intervals. When enabling this feature, each Ethernet frame is timestamped in hardware on probe ingress. This timestamp is used to calculate exact bitrates at various sampling intervals.

The **Interval** is the sampling interval of each bitrate calculation. There are 5 intervals tracked simultaneously.

The **Max interval frames** is the max number of frames within one interval last second. The **Max interval bitrate** is the max sum of Ethernet frame sizes inside one interval last second converted to bits per second. This number should always be bigger or equal for shorter intervals.

Click the legends in the graph to show or hide graphs.

The above graph is a typical OTT-traffic graph where the client periodically requests limited amounts of data at maximum speed resulting in traffic that is bursting near line-speed at 10 Gbit/s for short intervals while the average bitrate for larger intervals is only a fraction. This traffic shape is challenging for network equipment since it demands all remaining capacity up to line speed.



For multicast type traffic the traffic pattern will look more like the graph above. Here the bitrate is much more steady even for short intervals. The network never experiences near line-speed bursting since each stream is bitrate controlled by the sender.

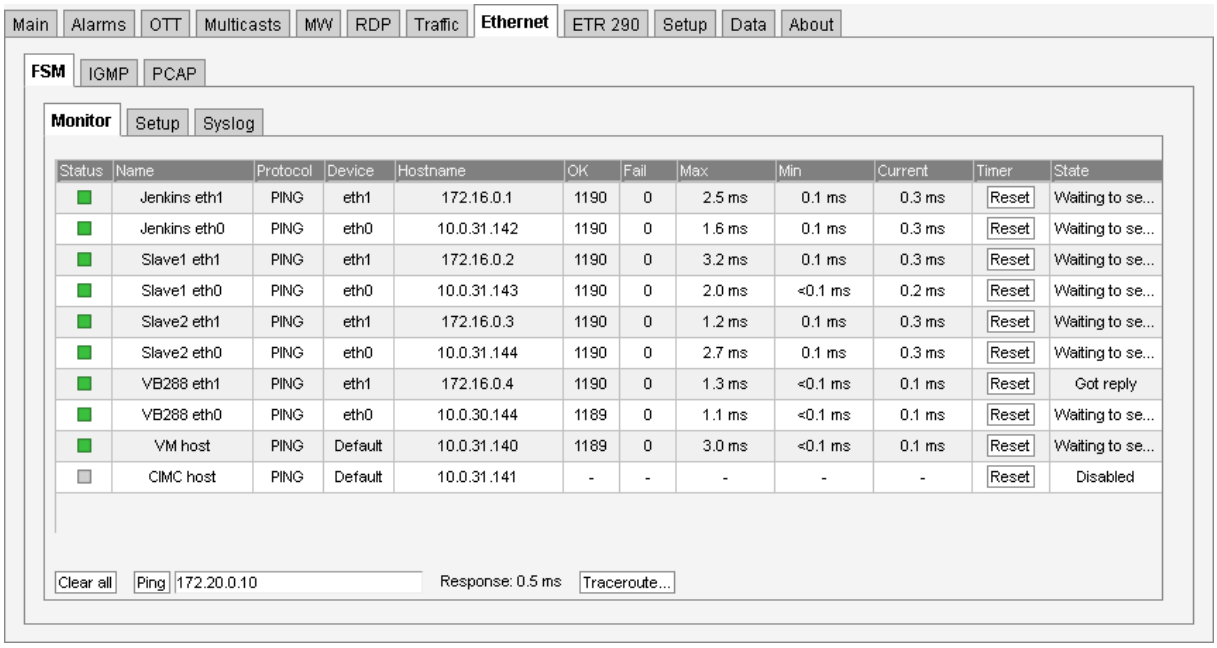
5.8 Ethernet

5.8.1 Ethernet — FSM

Full Service Monitoring (FSM) allows easy validation of any server reachable by the probe via Ethernet. The servers may be probed by either sending an ICMP Echo Request packet (also known as Ping) or performing an HTTP Get request.

Up to 10 services may be defined and each service will be checked at regular intervals. Any errors will be logged. An error is defined as no reply within 5 seconds for the Ping option or no, or incorrect, reply within 5 seconds for the HTTP option. If there are more consecutive errors than a fails threshold value an alarm will be raised.

5.8.1.1 Ethernet — FSM — Monitor



The following parameters are continuously monitored for each service:

Status:	Red = active alarm, Green = no alarm
Name:	User defined service name
Protocol:	Type of protocol. HTTP or Ping
IP address:	IP address. Must be numeric, host name is not accepted
OK:	Total number of valid checks
Fail:	Total number of invalid checks
Max:	Maximum response time recorded
Min:	Minimum response time recorded
Current:	The current (most recent) response time
Timer:	Button to reset and immediately restart the service
State:	Current state of the service. The states are: ‘Disabled’, ‘Waiting to send’, ‘Waiting for reply’, ‘Got reply’ and ‘Reset’.

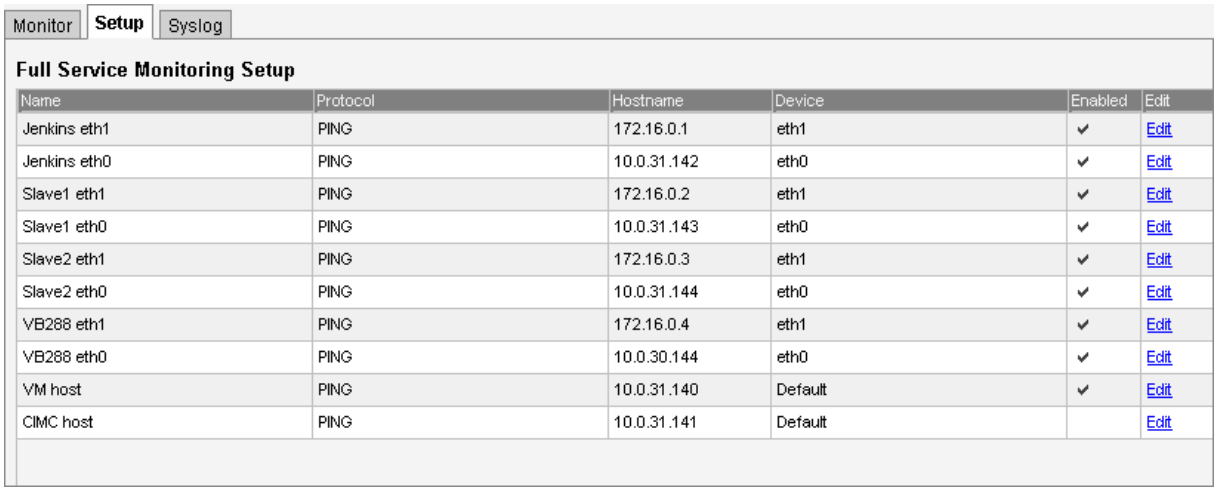
For convenience a manual ping field is located below the status table. By entering a valid IP address or host name and clicking the **Ping** button an arbitrary server may be pinged.

The **Clear all** button will clear accumulated data for all enabled FSM services, but active alarms will not be removed.

Clicking the **Traceroute** button will open a new window, allowing the user to trace the network route to a specified IP address.



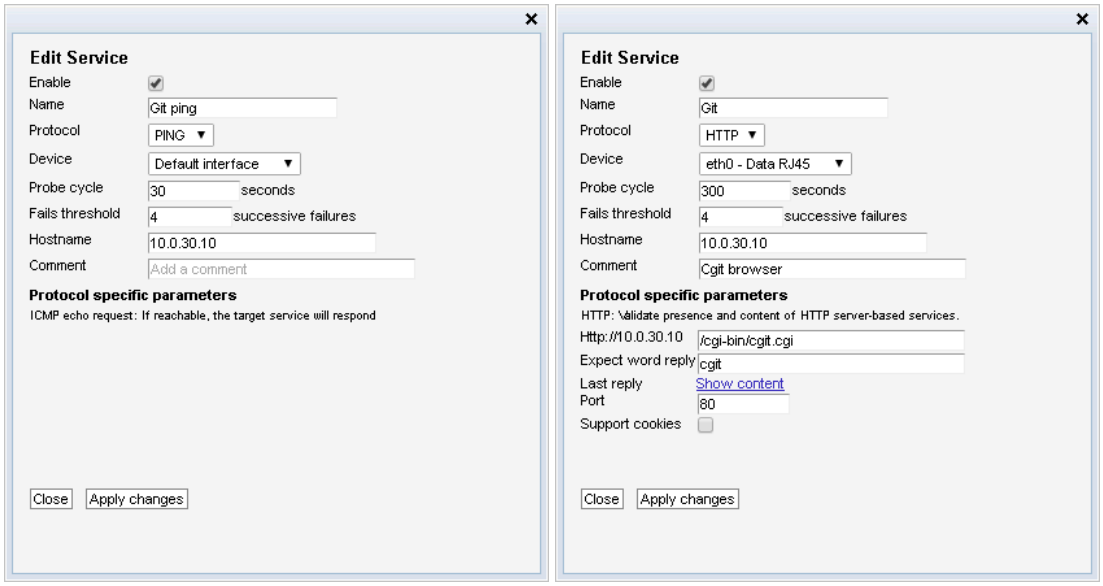
5.8.1.2 Ethernet — FSM — Setup



Name	Protocol	Hostname	Device	Enabled	Edit
Jenkins eth1	PING	172.16.0.1	eth1	✔	Edit
Jenkins eth0	PING	10.0.31.142	eth0	✔	Edit
Slave1 eth1	PING	172.16.0.2	eth1	✔	Edit
Slave1 eth0	PING	10.0.31.143	eth0	✔	Edit
Slave2 eth1	PING	172.16.0.3	eth1	✔	Edit
Slave2 eth0	PING	10.0.31.144	eth0	✔	Edit
VB288 eth1	PING	172.16.0.4	eth1	✔	Edit
VB288 eth0	PING	10.0.30.144	eth0	✔	Edit
VM host	PING	10.0.31.140	Default	✔	Edit
CIMC host	PING	10.0.31.141	Default		Edit

Each of the 10 FSM services may be defined or edited by clicking on the corresponding **Edit** button in the left hand table.

The probe supports ping and generic HTTP GET protocols for online status verification of arbitrary targets. After completing configuration of the selected service **Apply changes** must be pressed to save and apply the changes.



These fields are common for both the ping and the HTTP GET protocols:

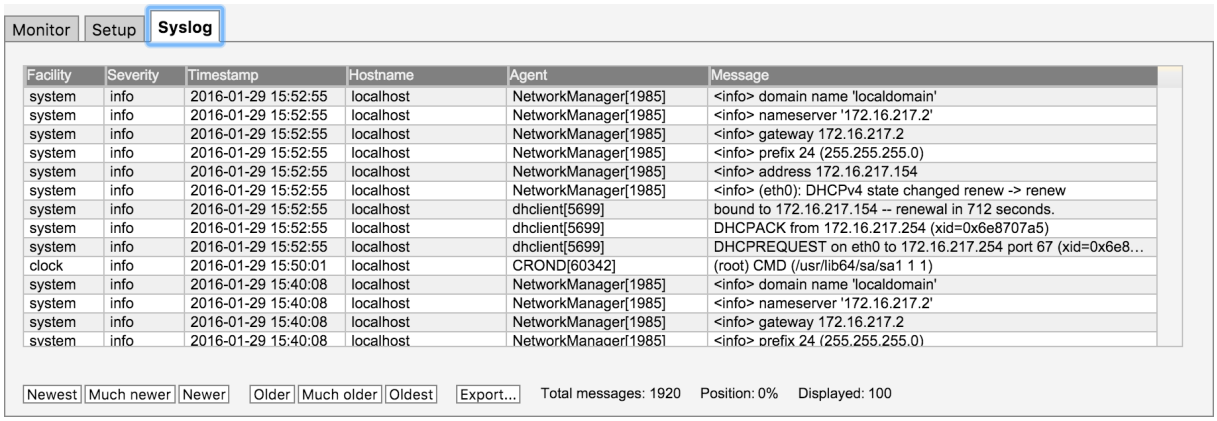
Enable:	Enable by checking toggle button.
Name:	User-defined name of service
Protocol:	Select between ping and HTTP.
Device:	Ethernet interface to use for this service.
Probe cycle:	Time interval in seconds to wait between each activation. A value below 30 is not recommended.
Fails threshold:	The number of consecutive errors needed to raise an alarm
Hostname:	The IP address for the target. Host names are supported for HTTP.
Comment:	Optional comment field – maximum 100 characters

These fields are specific for the HTTP GET protocol:

http://<IP address>:	The request to send to the target, for example index.html
Expect word reply:	A case sensitive word or sentence to be expected in the reply. To find a suitable string, use the Show content link. Leave this field empty to let the probe ignore the contents of the reply.
Last reply:	The last reply Show content link points to the last HTML file that was generated by this service.
Port:	The port used by the target server, often 80 for HTTP requests
Support cookies:	If enabled, the HTTP GET request will remember cookies returned by the target and provide them in subsequent requests.



5.8.1.3 Ethernet — FSM — Syslog



The VB330-SW has a built-in syslog server which captures all incoming messages (UDP, port 514). Messages are displayed in a pageable grid with the following columns: Facility, Severity, Timestamp, Hostname, Agent and Message. Currently displayed page can be exported as an XML-document.

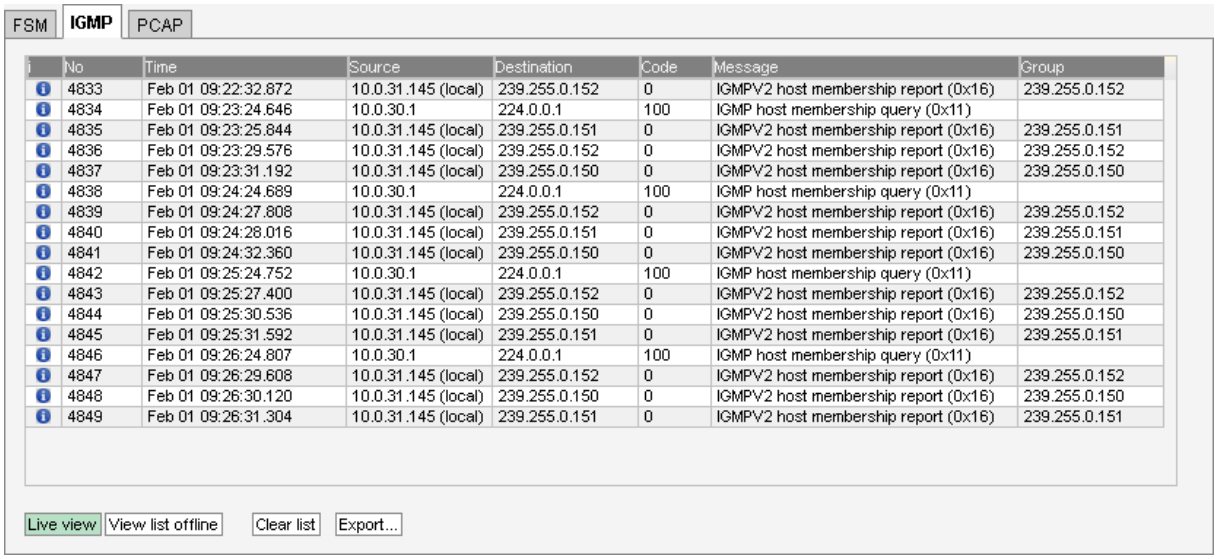
Since the syslog server typically stores about 100 pages of messages there is a group of buttons for a fast navigation:

Newest	Move to the first page
Much newer	Move 10 pages backwards
Newer	Move 1 page backwards
Older	Move 1 page forwards
Much older	Move 10 pages forwards
Oldest	Move to the last page

Syslog server has a limited capacity which is usually enough to store the latest 10,000 messages depending on the size of the syslog messages. When a new message arrives and no storage space remains the oldest messages are removed.

Note that the syslog server is very sensible to time settings, so it is strongly recommended to have a time synchronization enabled.

5.8.2 Ethernet — IGMP



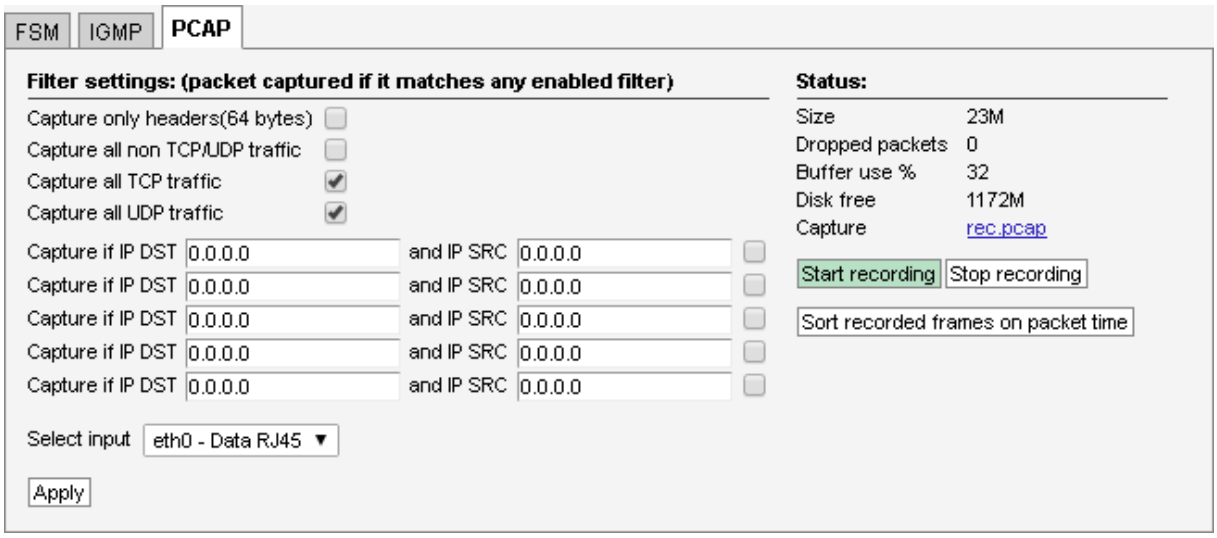
i	No	Time	Source	Destination	Code	Message	Group
ⓘ	4833	Feb 01 09:22:32.872	10.0.31.145 (local)	239.255.0.152	0	IGMPV2 host membership report (0x16)	239.255.0.152
ⓘ	4834	Feb 01 09:23:24.646	10.0.30.1	224.0.0.1	100	IGMP host membership query (0x11)	
ⓘ	4835	Feb 01 09:23:25.844	10.0.31.145 (local)	239.255.0.151	0	IGMPV2 host membership report (0x16)	239.255.0.151
ⓘ	4836	Feb 01 09:23:29.576	10.0.31.145 (local)	239.255.0.152	0	IGMPV2 host membership report (0x16)	239.255.0.152
ⓘ	4837	Feb 01 09:23:31.192	10.0.31.145 (local)	239.255.0.150	0	IGMPV2 host membership report (0x16)	239.255.0.150
ⓘ	4838	Feb 01 09:24:24.689	10.0.30.1	224.0.0.1	100	IGMP host membership query (0x11)	
ⓘ	4839	Feb 01 09:24:27.808	10.0.31.145 (local)	239.255.0.152	0	IGMPV2 host membership report (0x16)	239.255.0.152
ⓘ	4840	Feb 01 09:24:28.016	10.0.31.145 (local)	239.255.0.151	0	IGMPV2 host membership report (0x16)	239.255.0.151
ⓘ	4841	Feb 01 09:24:32.360	10.0.31.145 (local)	239.255.0.150	0	IGMPV2 host membership report (0x16)	239.255.0.150
ⓘ	4842	Feb 01 09:25:24.752	10.0.30.1	224.0.0.1	100	IGMP host membership query (0x11)	
ⓘ	4843	Feb 01 09:25:27.400	10.0.31.145 (local)	239.255.0.152	0	IGMPV2 host membership report (0x16)	239.255.0.152
ⓘ	4844	Feb 01 09:25:30.536	10.0.31.145 (local)	239.255.0.150	0	IGMPV2 host membership report (0x16)	239.255.0.150
ⓘ	4845	Feb 01 09:25:31.592	10.0.31.145 (local)	239.255.0.151	0	IGMPV2 host membership report (0x16)	239.255.0.151
ⓘ	4846	Feb 01 09:26:24.807	10.0.30.1	224.0.0.1	100	IGMP host membership query (0x11)	
ⓘ	4847	Feb 01 09:26:29.608	10.0.31.145 (local)	239.255.0.152	0	IGMPV2 host membership report (0x16)	239.255.0.152
ⓘ	4848	Feb 01 09:26:30.120	10.0.31.145 (local)	239.255.0.150	0	IGMPV2 host membership report (0x16)	239.255.0.150
ⓘ	4849	Feb 01 09:26:31.304	10.0.31.145 (local)	239.255.0.151	0	IGMPV2 host membership report (0x16)	239.255.0.151

The IGMP view shows all IGMP (version 2 or 3) messages detected by the probe. This includes IGMP query messages sent by routers, IGMP reply messages sent by the probe itself and IGMP reply messages sent by other probes and devices on the same subnet.

The live IGMP page can be paused by clicking the **View list offline** button. The IGMP messages can be exported as XML by clicking the **Export...** button, and the list is cleared by clicking the **Clear list** button.

ⓘ:	Click the blue information icon to open the IGMP record pop-up view
No:	The message number since the list was cleared
Time:	The probe time when the message occurred
Millisec:	The milliseconds timestamp
Source:	The source IP address
Destination:	The destination IP address
Code:	The timeout code
Message:	The interpreted IGMP message
Group:	The IGMP group address

5.8.3 Ethernet — PCAP



The VB330-SW can make PCAP recordings on the data interface based on simple user configurable filters. The PCAP format supports microsecond timing accuracy.

Incoming traffic is recorded if it matches one or more of the enabled filters while outgoing traffic is always recorded. So for instance, to record all OTT traffic on the data interface it is sufficient to enable the "Capture all TCP traffic" filter (since OTT uses the HTTP protocol which is always TCP).

Flags and filters	
Capture only header:	If enabled, only 64 first bytes of Ethernet frame is captured. This allows higher bitrate traffic to be recorded and over longer time.
Capture all non TCP/UDP traffic:	Check to record non-IPv4 traffic such as ARP, PIM or IPv6.
Capture all TCP traffic:	Check to capture all IPv4 TCP traffic.
Capture all UDP traffic:	Check to capture all IPv4 UDP traffic.
IP DST and IP SRC filters:	Check to activate test. Will capture stream if IP destination address matches. If SRC is specified it has to match too.

Recording	
Size:	Size of current recording.
Dropped packets:	Number of dropped packets due, usually caused by running temporarily out of buffer due to too high traffic. To allow higher bitrate recordings **Capture only headers** may be enabled.
Buffer use %:	Current buffer utilization. At 100% the **Dropped packets** will start counting.
Disk free:	Remaining disk size.
Capture:	The recorded capture. May be invalid if recording is still in progress.
Start recording:	Click to start a new recording. This will clear the current rec.pcap file.
Stop recording:	Click to stop the current recording.

Sort recorded frames on packet time:	At high bitrates, some Ethernet frames may be recorded out of order as a result of the multi-core architecture. Click to sort frames in recording according to time-stamp.

5.9 ETR 290 (Option)

The ETR 290 tab and all sub-views will only be present in the user interface provided that the probe is licensed with the ETR 290 option.

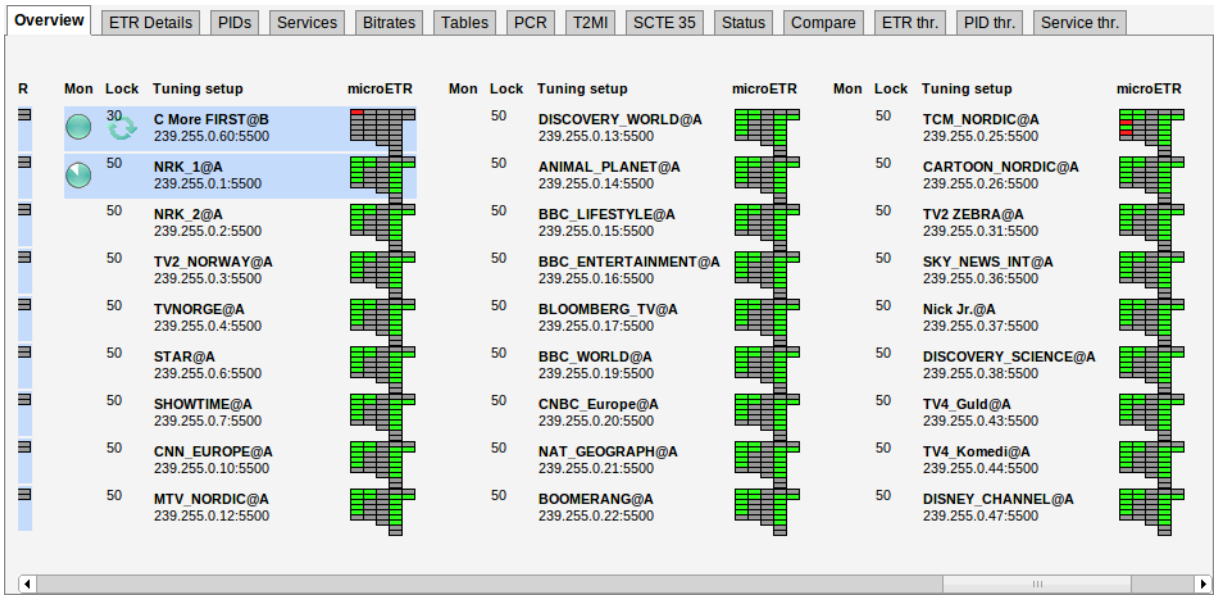
The ETR 290 views show information as reported by the ETSI TR 101 290 monitoring engines.

If ETR 290 analysis has been configured for multiple Ethernet streams to be monitored by a particular Ethernet ETR engine (refer to **Multicasts — Streams — Edit**), they will be analyzed in a round-robin fashion by the engine. A maximum of 2000 Ethernet streams may be analyzed in total.

The number of ETR 290 analysis engines depends on the license. The SW currently support up to 200 engines which are added in increments of 50. More engines make it possible to reduce the analysis round-trip time or allowing simultaneous full-time ETR analysis of many multicasts. The ETR 290 analysis engines operate in parallel.

It is possible to hide disabled inputs from being displayed in the various **ETR 290** sub-views. This setting is found in the **Setup — ETR** view.

5.9.1 ETR 290 — ETR Overview



The **ETR 290 — ETR Overview** view will show ETR 290 status for ETR 290 monitored streams. ETR 290 monitoring may be enabled for Ethernet streams in the **Multicasts — Streams — Edit** view.

The streams currently being analyzed are highlighted and a circular progress icon shows the monitoring progress.

The analysis time for each stream is set as part of the **ETR thresholds** parameters list in the **ETR 290 — ETR thr. — Edit** view.



The result of the different ETR 290 tests are shown as table entries in a condensed view called MicroETR, a scaled down version of the regular ETR display, one icon representing one stream. Green color indicates status OK whereas red color indicates an active alarm for that particular test. A white field shows that a check has not yet been performed, usually due to lack of measurement data, and grey indicates that a check is disabled. Tool-tip functionality allows the user to view the name of an individual check in the MicroETR display. Let the mouse pointer hover over the field for a moment to view the tool-tip.

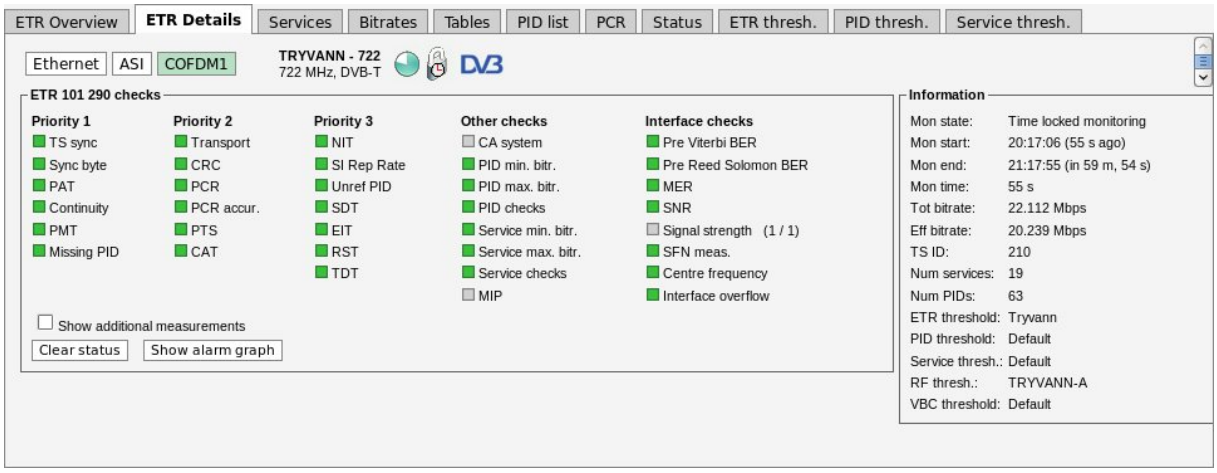
When clicking one of the MicroETR icons the detailed ETR 290 status for that stream is displayed in the **ETR 290 — ETR Details** view. By entering this view through the MicroETR, the view will remain static irrespective of the round-robin looping, thus making it easy to examine one stream in detail without interruptions. The round-robin looping and associated alarm handling will continue in the background.

Note that it is possible to deactivate individual ETR 290 alarms by defining appropriate **ETR thresholds**.

If the user wants to examine one particular Ethernet stream in more detail, he can lock the ETR 290 analysis to that stream by clicking the lock field at that stream. The round-robin operation of the ETR 290 engine will then be stopped and a lock icon will appear as an indication that the monitoring is locked to that stream. If a time limit has been set for the time lock (**Setup — ETR** view), a clock icon will be superimposed on the lock icon. To re-activate the round-robin cycling the lock icon should be clicked. Note that locking the ETR 290 processing to one stream will affect alarm handling and all ETR 290 views. Active alarms for streams that are not currently being analyzed will freeze (remain active) until the processing lock is deselected and ETR 290 analysis eventually shows that the error state is cleared.

The user can select one input to be displayed exclusively by clicking the corresponding **Show only this input** button. This does not affect ETR 290 processing or alarming.

5.9.2 ETR 290 — ETR Details



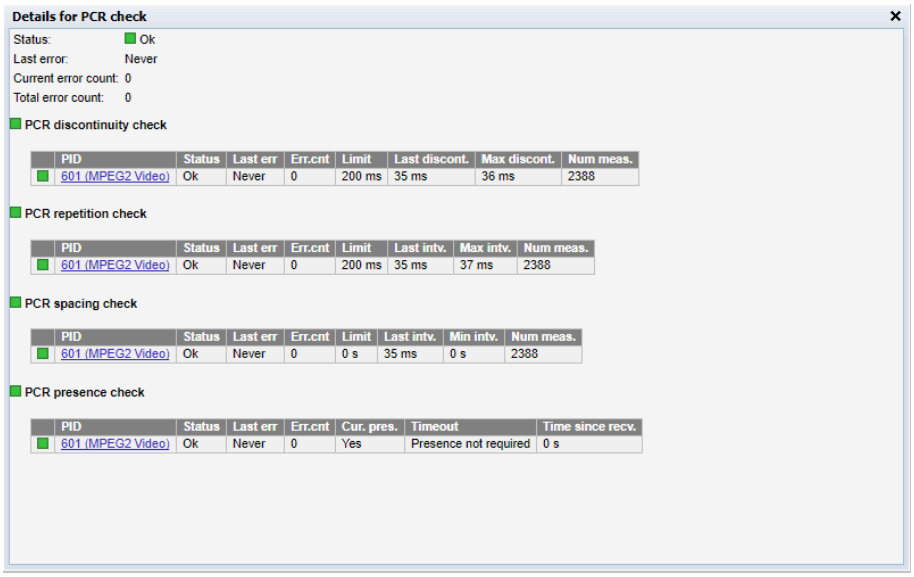
The **ETR Details** view shows the ETR 290 status for the current stream of the user-selected input. The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon the round-robin tuning process is stopped (locked to the current frequency) or resumed. A DVB or ATSC icon indicates the analysis mode. The analysis mode is defined as part of the ETR threshold template.

The ETR 290 parameters are grouped into five different categories. The first three groups are defined in the ETSI TR 101 290 guidelines. The fourth category contains checks defined by Bridge Technologies allowing CA system checks, custom PID and service checks, content checks (checking the video for

freeze-frames etc) and the Gold TS reference checks. The last category contains checks of the input interfaces.

For each check a bulb indicates the current status of that parameter check: green indicates status OK whereas red indicates an active alarm. When the probe has not yet received data relevant for a particular check, the corresponding bulb is white. Grey color indicates that the check has been deactivated (as set in **ETR 290 — ETR thr. — Edit**).

When clicking one of the ETR 290 parameters, details about the current status can be viewed for that item.



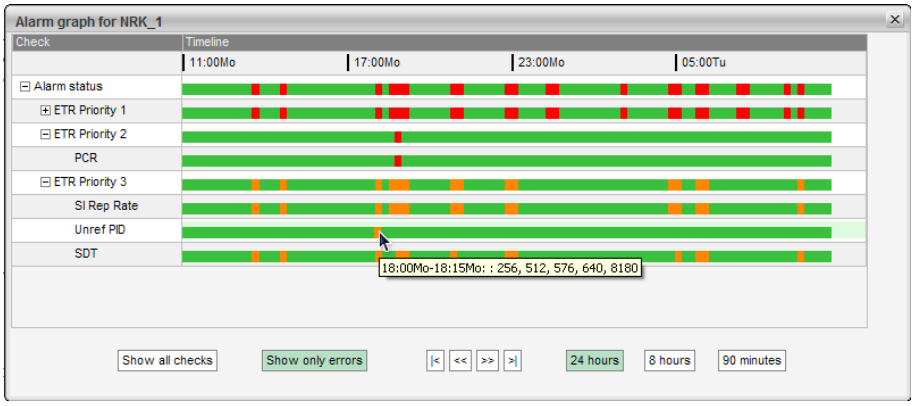
Enable the **Show additional measurements** checkbox to view additional measurements that are done but which are ignored when determining the alarm status. These will appear with a 'half-bulb' icon indicating that the check is disabled whilst also showing the status of this element. As an example this can be used to view the BAT section repetition interval and section gap, or to view a list of PIDs with CC errors including the PIDs for which this check has been manually disabled.

Click a PID in a PID list to view PID details. Similarly you can click on a service to view service details.

If the **Clear status** button is clicked the error counts are reset and the ETR 290 analysis restarts.

The details of the individual ETR 290 measurements are described in a separate document called **Bridge Technologies ETR 290 Details — Extended ETSI TR 101 290 Testing**.

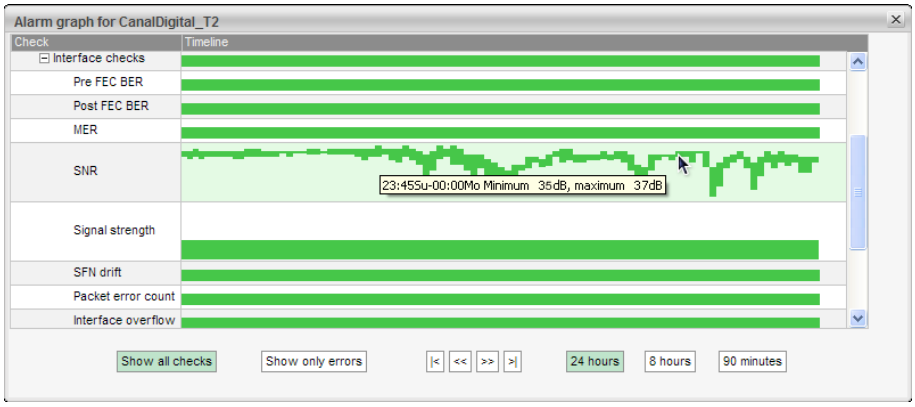
Clicking the **Show alarm graph** button opens the Alarm graph pop-up view.



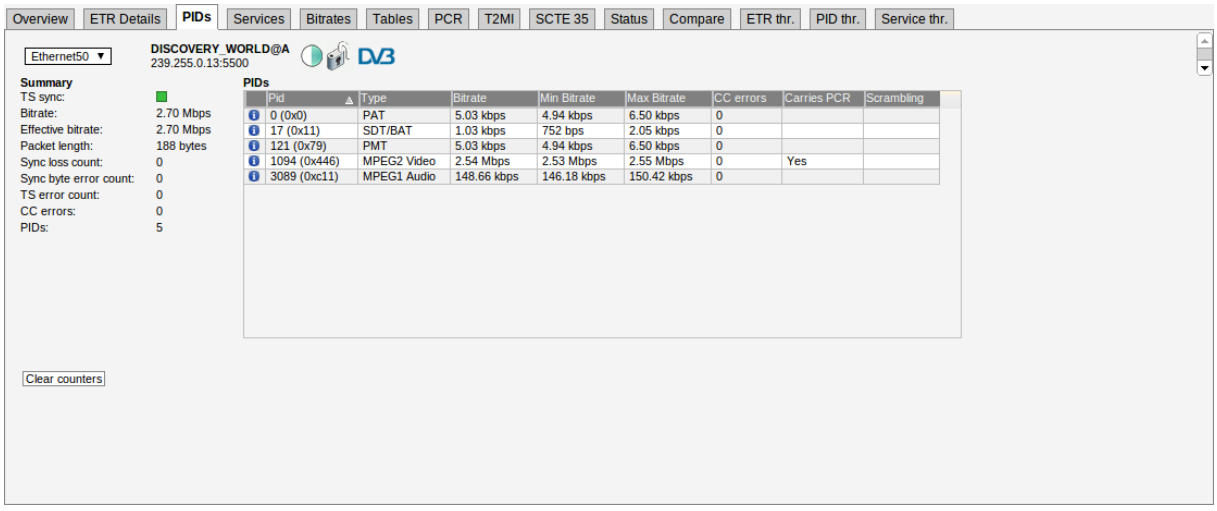
The alarm graph shows the transport stream ETR alarm status over time in the form of a status timeline. The timeline bar shows the stream status for a time span of 90 minutes, 8 hours or 24 hours as selected by clicking the time selection buttons below the timelines. The stream bar reveals any alarm that has been present during the selected time period. The bar color is either green for OK or colored in accordance with the alarm severity if an alarm has occurred. Refer to section 5.2.2 for a description of the alarm color representation. Periods of time when the stream has not been ETR monitored due to round-robin operation are represented by grey. By using the arrow buttons it is possible to view alarm occurrences up to 24 hours back in time even if the highest graph time resolution is selected.

If alarms have occurred during the selected time period, the status timeline will not be all green. In this case it is possible to expand the timeline tree by clicking the plus sign at the timeline. Individual timelines for different ETR priorities and for different alarms may be viewed as the tree is expanded into several levels. Tooltips reveals details about an error incident.

By default the 'Show only errors' mode is selected, and only timelines that are not all green will be displayed.



5.9.3 ETR 290 — PIDs



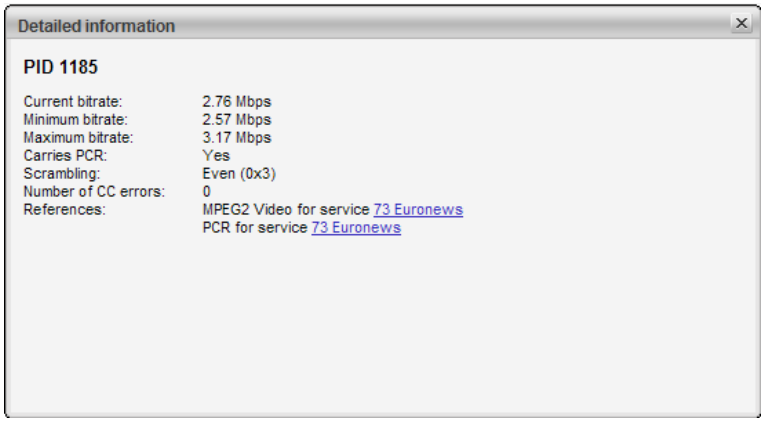
This view lists the PIDs of the currently active stream of the selected input. The PID list can be sorted by clicking a table column header.

The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon the round-robin cycling is

stopped or resumed. A DVB or ATSC icon indicates the analysis mode. The analysis mode is defined as part of the ETR thresholds.

By clicking the button **Clear counters** the minimum and maximum bitrates and the CC error counters will be reset. Note that this cannot be undone.

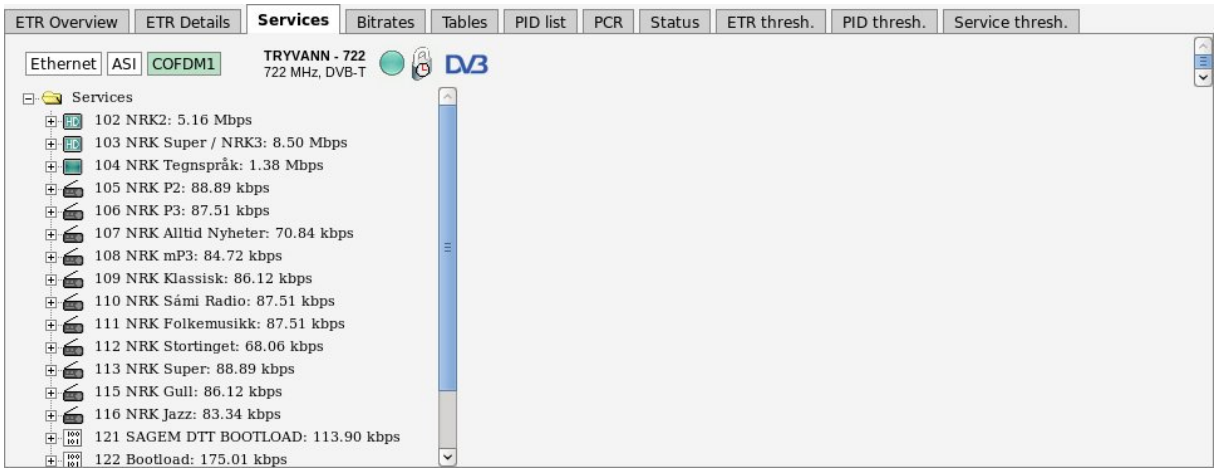
When clicking the blue information icon associated with a PID details concerning that PID will be displayed. All services referring to the PID are listed, and scrambling information is shown.



The following PID details are displayed:

PID Details:	
PID:	The PID for which the following parameters apply
Current bitrate:	The current bitrate measurement for this PID. The bitrate is averaged over 1 second.
Minimum bitrate:	The minimum bitrate measurement for this PID since the start of the monitoring period. (I.e. when the probe tuned to the frequency or when the monitoring of this frequency was restarted by the user clicking on 'Clear status' in the 'ETR Overview'.)
Maximum bitrate:	The maximum bitrate measurement for this PID since the start of the monitoring period.
Carries PCR:	If the PID carries Program Clock Reference information, this field will be set to Yes. If PCR analysis is enabled in the ETR threshold template a link will be shown to bring up the PCR histogram data for this PID.
Scrambling:	If the PID is scrambled, this field will show if it is scrambled with Odd or Even control word.
Number of CC errors:	The number of CC errors for the specified PID. For the Ethernet interface the number of CC errors is measured from when the probe started to monitor the multicast or when the user clicked 'Clear counters' in the 'Mon' page.
References:	All the references for this PID in the PSI/SI/PSIP tables. This will show the reference type and the service that refers the PID (if applicable). The service can be clicked to show the detailed service information.

5.9.4 ETR 290 — Services

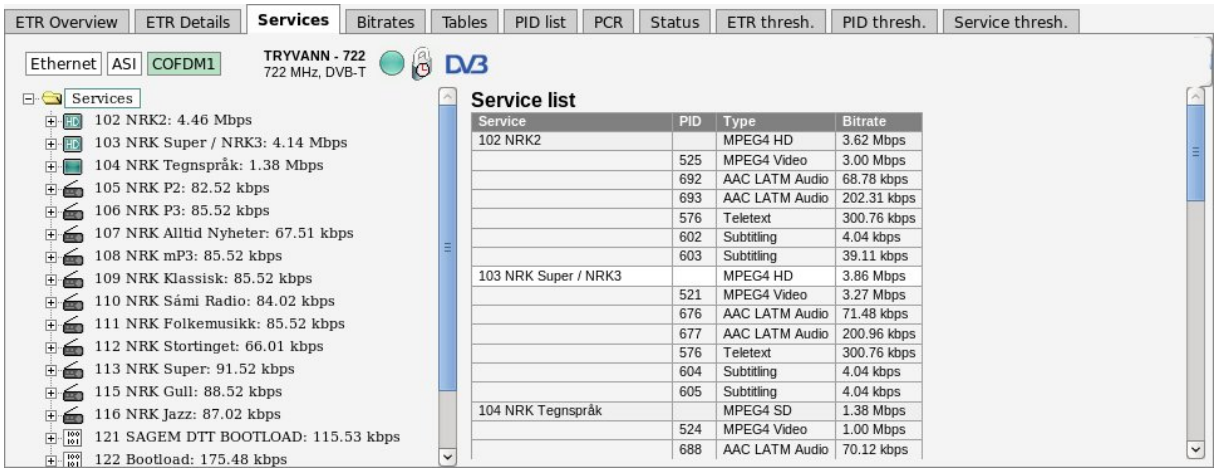


The **ETR290 — Services** view lists the services and service components of the current stream of the selected input.

The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon, the round-robin cycling is stopped or resumed. A DVB or ATSC icon indicates the analysis mode. The analysis mode is defined as part of the ETR thresholds.

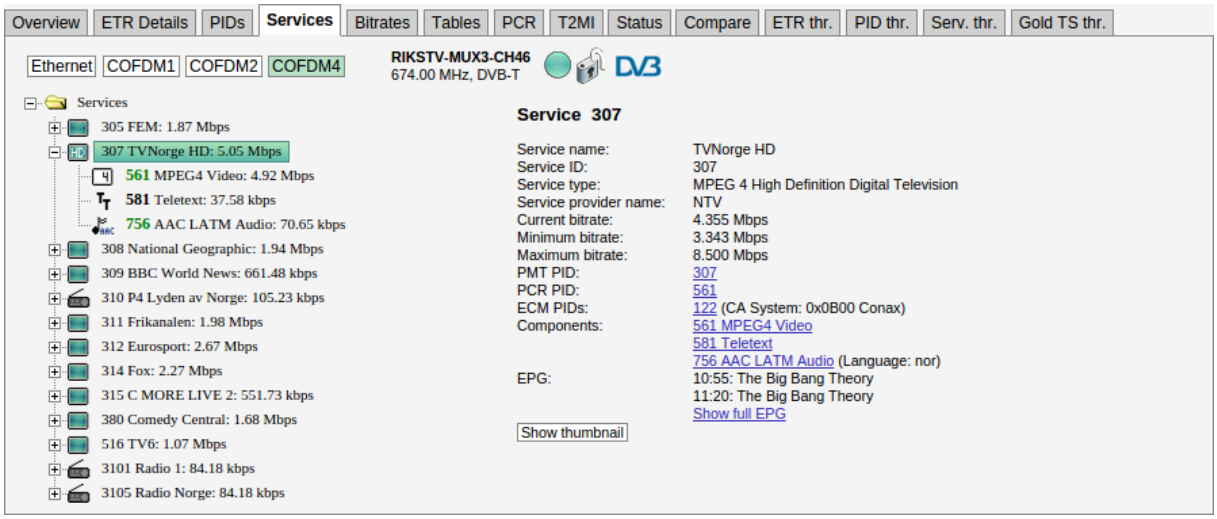
When tree nodes are selected, detailed information will be displayed on the right hand side of the view.

If the service tree 'Services' top node is clicked, a summary list of stream services and PIDs is displayed. Each service's service ID and each component's PID value and bitrate are displayed together with individual PID and service bitrates.



Services top node	
Service:	Service name and service ID
PID:	Service component PID value
Type:	Service and component encoding format
Bitrate:	Individual current bitrate of services and components

When clicking a service, details about the service and service components will be displayed.



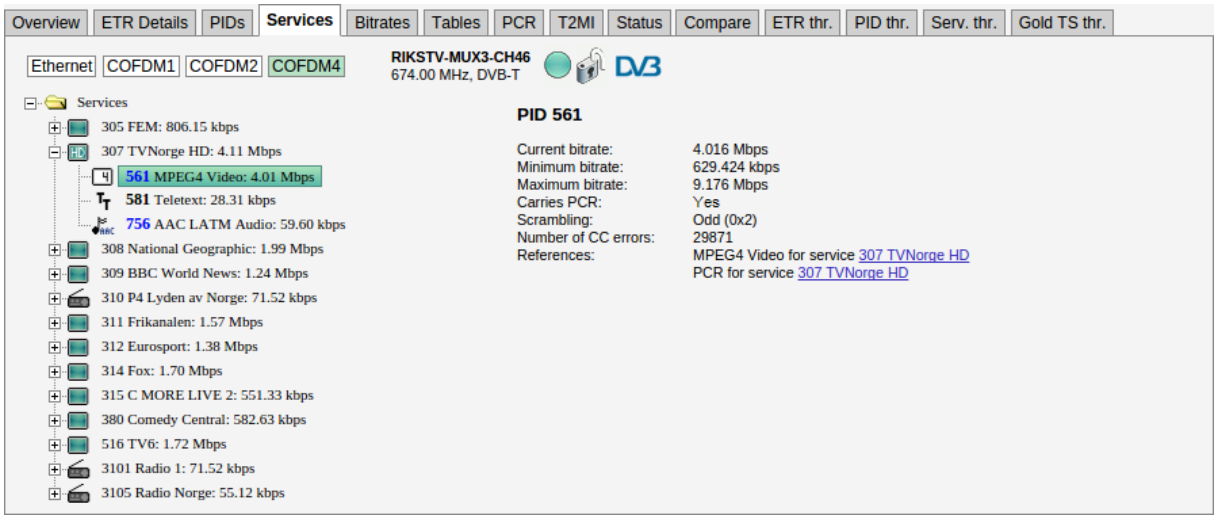
If a PID is scrambled this is indicated in the service tree by the color green or blue (for even and odd scrambling respectively). A missing PID is indicated by the color red. If one of the blue PID links is clicked, PID details are shown.

Click the Show thumbnail button to view a thumbnail of the selected service. Thumbnails can only be shown for services that are not scrambled.

Service node	
Service name:	Name of the highlighted service, as signaled in SDT or VCT
Service ID:	Service ID number
Service type:	Service type as signaled in SDT
Service provider name:	The name of the service provider as signaled in SDT. Not applicable for ATSC streams.
Current bitrate:	The current bitrate measurement for this service. The bitrate is averaged over 1 second.
Minimum bitrate:	The minimum bitrate measurement for this service since the start of the monitoring period. (I.e. when the probe tuned to the frequency or when the monitoring of this frequency was restarted by the user clicking on 'Clear status' in the 'ETR Overview'.)
Maximum bitrate:	The maximum bitrate measurement for this service since the start of the monitoring period.
PMT PID:	The service's PMT PID
PCR PID:	The service's PCR PID
ECM PIDs:	The service's ECM PID(s) and name of CA system(s). This information will only be displayed if ECM PIDs are signaled in the PMT table, usually only done when one or more service components are scrambled.
Components:	A list of the component PIDs and reference types. For PIDs which have a language descriptor (typically audio PIDs) the language code is also shown.
EPG:	If DVB EIT is present in the stream and EIT table IDs are configured in the **Setup — ETR** view, EIT present/following is displayed. If EIT schedule is present in the stream, a blue 'Show full EPG' link is displayed. By clicking the link it is possible to view the EIT schedule information.

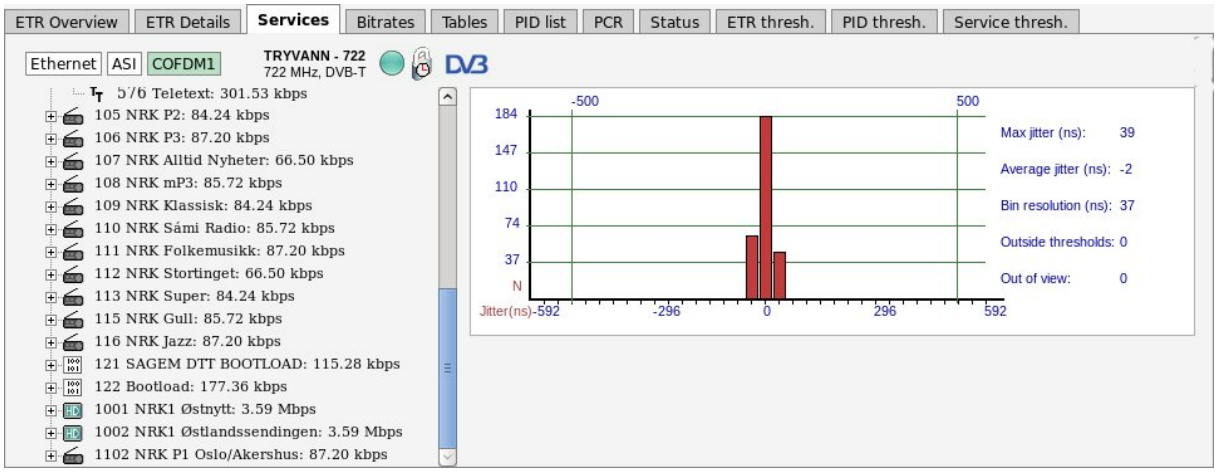
Show thumbnail	Opens the **Thumbnail view** for this service. Thumbnails are only decoded automatically if the **Extract thumbnails** option has been enabled in the associated multicast setup, or if content check alarming (Content Extraction and Alarming option) has been enabled in the ETR threshold template. The same pop-up details are displayed as when opened from the **Main — Thumb overview** view.

When clicking a service component, associated key parameters and references will be displayed.

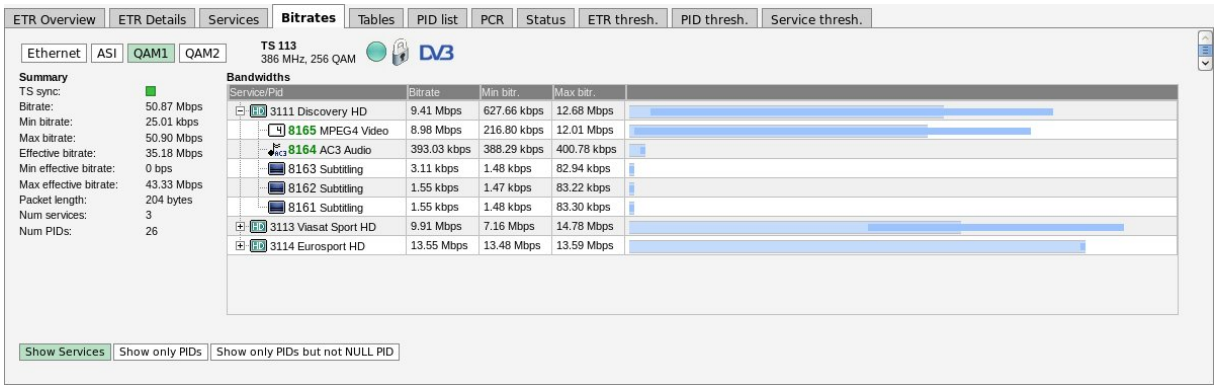


For PIDs carrying PCR it is possible to view a PCR jitter histogram by clicking the blue ‘show histogram’ link. If one of the blue service links is clicked, service details are shown.

Service component node	
Current bitrate:	The current bitrate measurement for this component. The bitrate is averaged over 1 second.
Minimum bitrate:	The minimum bitrate measurement for this component since the start of the monitoring period. (I.e. when the probe tuned to the frequency or when the monitoring of this frequency was restarted by the user clicking on ‘Clear status’ in the ‘ETR Overview’.)
Maximum bitrate:	The maximum bitrate measurement for this component since the start of the monitoring period.
Carries PCR:	An indication of whether the PID carries PCR or not. The value may be ‘Yes’ or ‘No’. If PCR is carried by the PID, a blue ‘show histogram’ link is displayed. By clicking this link it is possible to view the PCR jitter histogram.
Scrambling:	An indication of whether the PID is scrambled or not. If the PID is not scrambled, the value will be ‘No’. If the PID is scrambled, information about the current control word is displayed: ‘Even 0x3’ or ‘Odd 0x2’.
Number of CC errors:	The number of CC errors detected during the monitoring period
References:	A list of PSI/SI references to the component PID. When one of the blue service links is clicked, detailed service information is displayed.



5.9.5 ETR 290 — Bitrates



This view shows a graphical representation of service and PID bitrates. The current bitrate is shown as the length of the light blue bar whereas the dark blue bar represents bitrate variation, spanning from minimum to maximum measured bitrate.

The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon the round-robin tuning process is stopped (locked to the current frequency) or resumed. A DVB or ATSC icon indicates the analysis mode. The analysis mode is defined as part of the ETR thresholds.

The user may select to view a list of services and component PIDs, to view PIDs only or to view PIDs without the null PID. This is selected by clicking the **Show Services**, **Show only PIDs** or **Show only PIDs but not NULL PID** button respectively.

5.9.6 ETR 290 — Tables

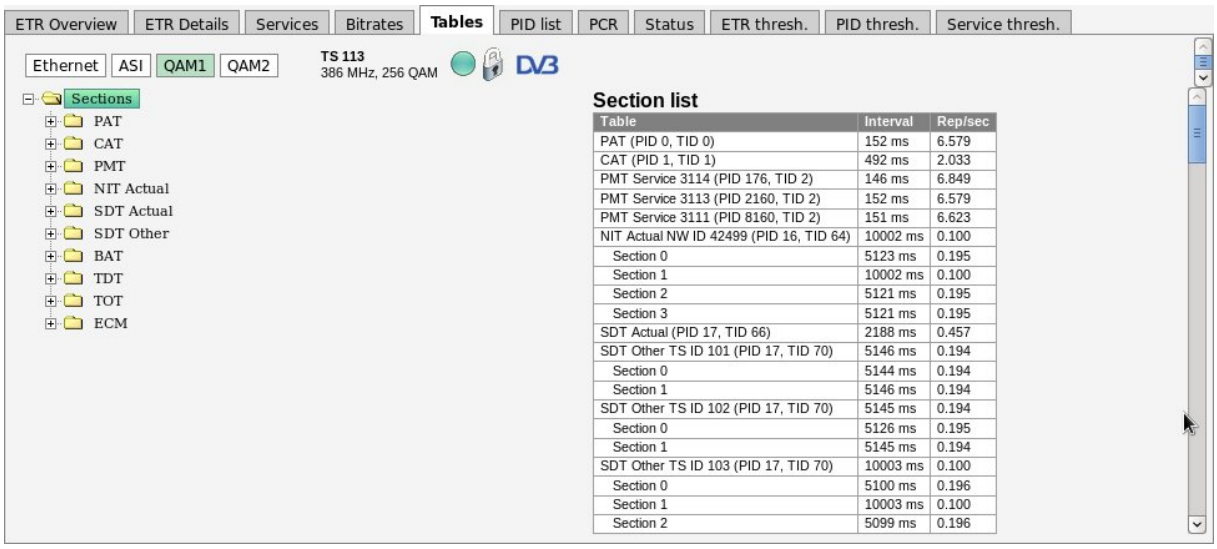


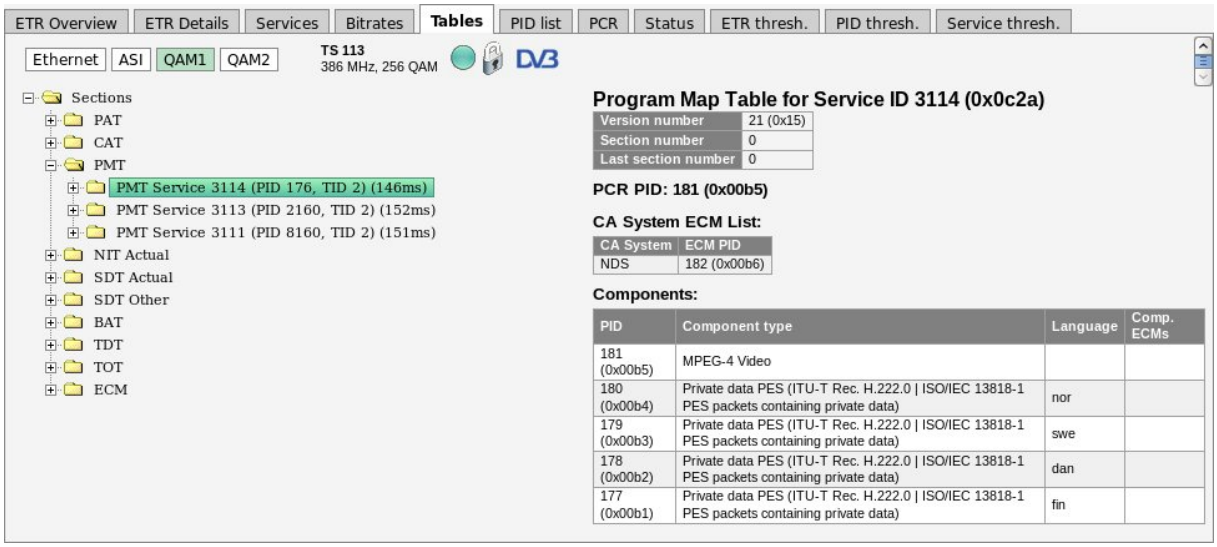
Table	Interval	Rep/sec
PAT (PID 0, TID 0)	152 ms	6.579
CAT (PID 1, TID 1)	492 ms	2.033
PMT Service 3114 (PID 176, TID 2)	146 ms	6.849
PMT Service 3113 (PID 2160, TID 2)	152 ms	6.579
PMT Service 3111 (PID 8160, TID 2)	151 ms	6.623
NIT Actual NW ID 42499 (PID 16, TID 64)	10002 ms	0.100
Section 0	5123 ms	0.195
Section 1	10002 ms	0.100
Section 2	5121 ms	0.195
Section 3	5121 ms	0.195
SDT Actual (PID 17, TID 66)	2188 ms	0.457
SDT Other TS ID 101 (PID 17, TID 70)	5146 ms	0.194
Section 0	5144 ms	0.194
Section 1	5146 ms	0.194
SDT Other TS ID 102 (PID 17, TID 70)	5145 ms	0.194
Section 0	5126 ms	0.195
Section 1	5145 ms	0.194
SDT Other TS ID 103 (PID 17, TID 70)	10003 ms	0.100
Section 0	5100 ms	0.196
Section 1	10003 ms	0.100
Section 2	5099 ms	0.196

This view lists the PSI and SI or ATSC tables and table contents of the currently active stream of the selected input.

The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon the round-robin cycling is stopped or resumed. A DVB or ATSC icon indicates the analysis mode. The analysis mode is defined as part of the ETR thresholds.

Clicking the ‘Sections’ node displays detected tables and associated repetition rates.

Clicking a table enables viewing the table contents in a readily readable format.



Version number	21 (0x15)
Section number	0
Last section number	0

PCR PID: 181 (0x00b5)

CA System ECM List:

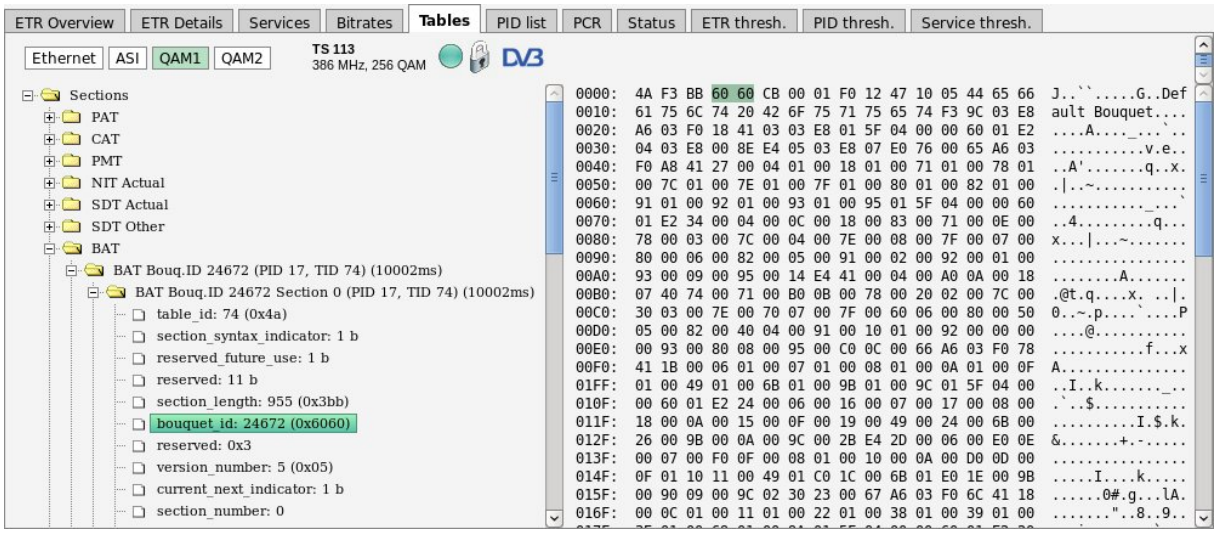
CA System	ECM PID
NDS	182 (0x00b6)

Components:

PID	Component type	Language	Comp. ECMs
181 (0x00b5)	MPEG-4 Video		
180 (0x00b4)	Private data PES (ITU-T Rec. H.222.0 | ISO/IEC 13818-1 PES packets containing private data)	nor	
179 (0x00b3)	Private data PES (ITU-T Rec. H.222.0 | ISO/IEC 13818-1 PES packets containing private data)	swe	
178 (0x00b2)	Private data PES (ITU-T Rec. H.222.0 | ISO/IEC 13818-1 PES packets containing private data)	dan	
177 (0x00b1)	Private data PES (ITU-T Rec. H.222.0 | ISO/IEC 13818-1 PES packets containing private data)	fin	

By clicking the plus-icon at a table the table contents is displayed in detail.

Clicking one of the table entries will allow viewing the table contents as a hexadecimal dump for detailed inspection.

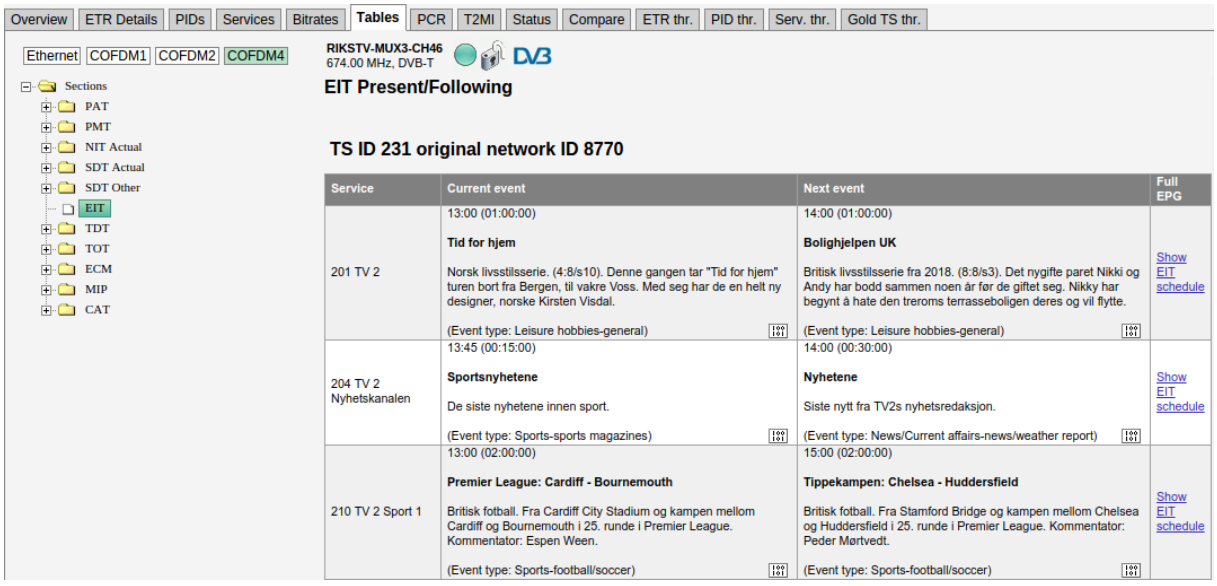


The selected table entry is highlighted in the table dump. Note that values shown in the table list may not correspond directly to the highlighted hex dump byte(s), because some of the table entries do not add up to whole bytes.

By hovering the cursor over the items in the tree a tooltip is displayed showing the start position of the data in the hexadecimal dump and the length of data. Press the save icon to download and save the raw table data on your computer.

A description of each PSI/SI table is beyond the scope of this manual, please refer to the specifications for more information about PSI/SI.

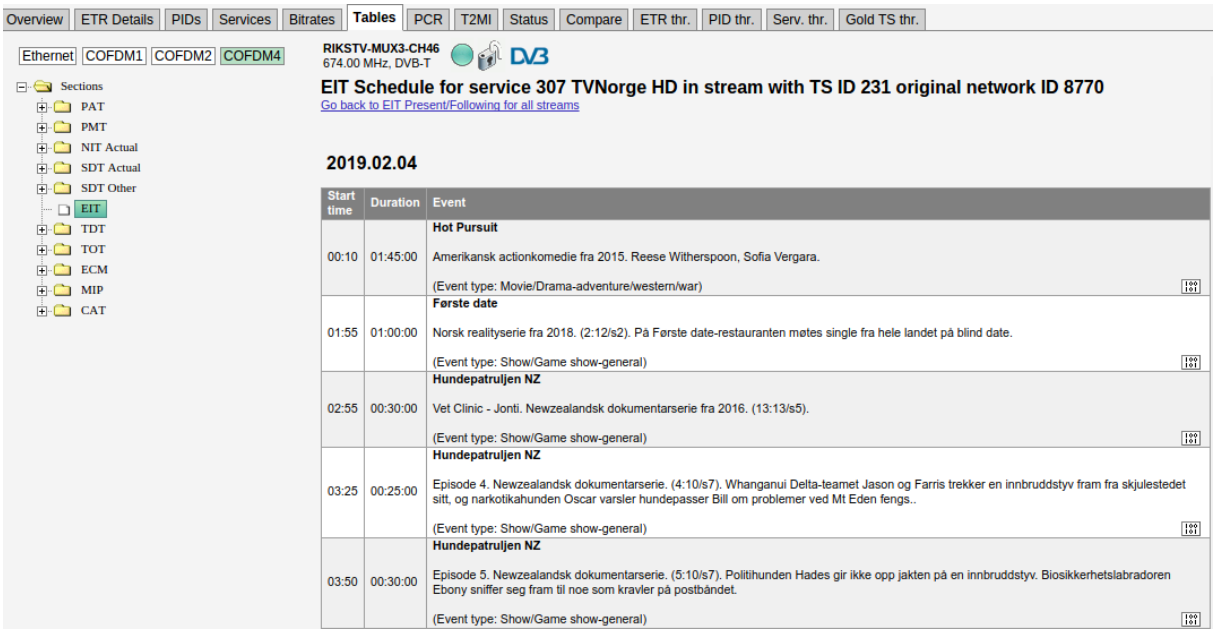
If you get “Unknown descriptor” in the table parsing it could be that the stream contains additional descriptors that can be enabled. Make a note of the descriptor_tag and go to **Setup — ETR** to enable the parsing of the descriptor.



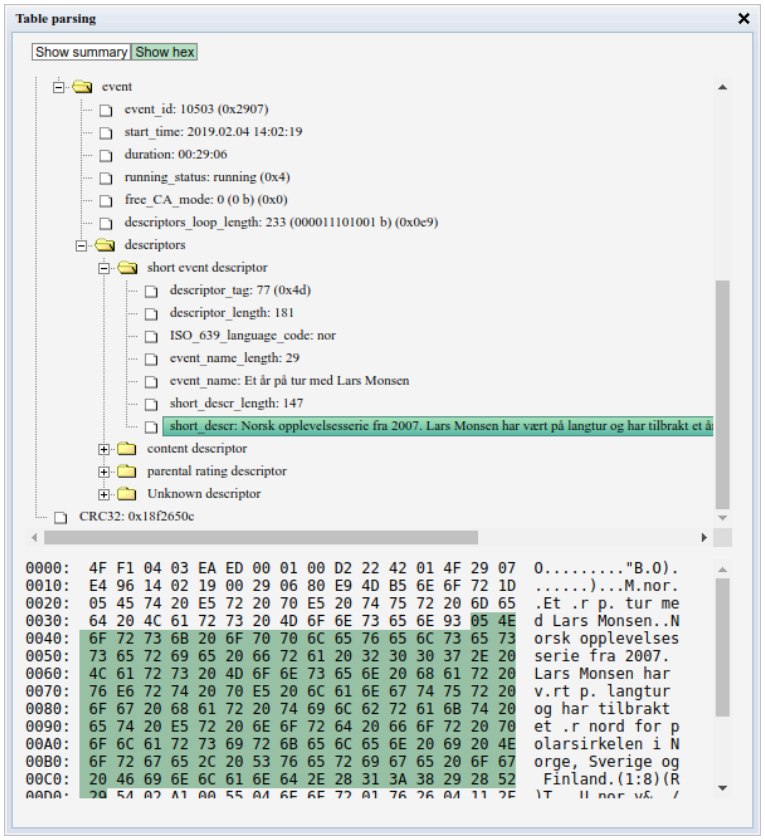
For streams which have electronic program guide information in the EIT table and the extraction of this information is enabled (in **ETR thresholds** and in **Setup — ETR**) the tree will show the text **EIT**. Clicking on this will bring up the list of present/following events (the current program and the next program to be broadcast) for the current stream will be displayed. If the stream has EIT p/f other information (and



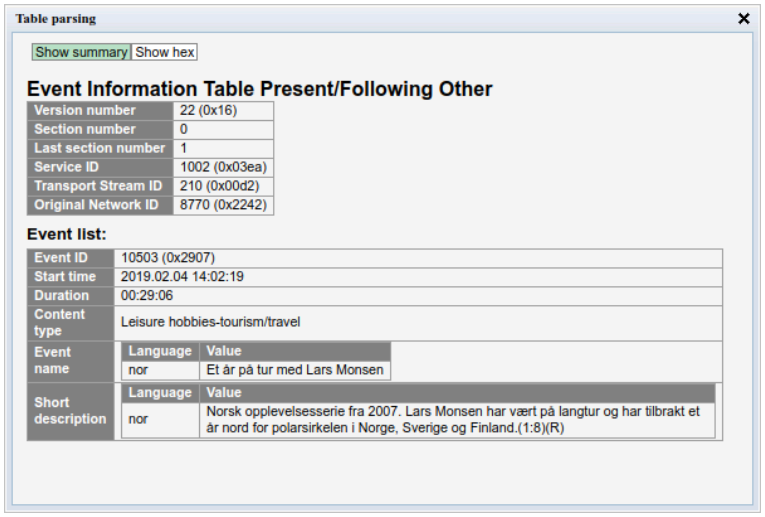
this table is enabled in **Setup — ETR**) then the list will also contain EPG present/following for other streams. If the stream has EIT schedule information for the actual and/or other streams (and these tables are enabled in **Setup — ETR**) then the list will also contain the link **Show EIT schedule**. Clicking this will show the full schedule for the selected service. The amount of data shown depends on the signal. A common practice is to send EPG for 7 days ahead.



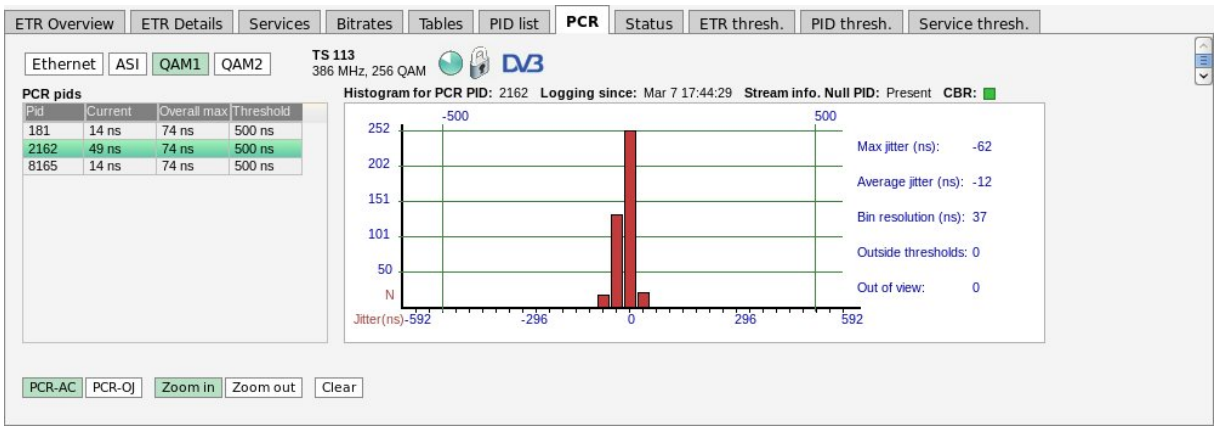
To get detailed information about one event, click the binary symbol . This will open a popup window with parsing of the underlying EIT table. The information can be displayed either in detailed hex mode:



Or in summary mode:



5.9.7 ETR 290 — PCR



The PCR jitter histogram displays PCR jitter as measured by the probe. A list of detected PCR PIDs in the selected stream is shown together with their current and maximum PCR jitter values. A PCR PID is selected for histogram presentation by clicking the associated table entry. The histogram shows the number of received PCR values versus jitter. PCR jitter is by default measured as PCR-AC for all interfaces. By creating an ETR threshold template that enables PCR-OJ and assigning this template to a stream it is possible to select PCR-OJ measurement mode by clicking the **PCR_OJ** button. The PCR_OJ measurement is not relevant for Ethernet streams.

Please note PCR analysis will be disabled if none of the PCR-AC, PCR-OJ, PCR Accuracy or PCR Jitter checks are enabled in the **ETR thresholds**. So to use the **ETR 290 — PCR** functionality this needs to be enabled.

The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon the round-robin cycling is stopped or resumed. The pushbuttons **Zoom in** and **Zoom out** enables rescaling of the graph. This makes it possible to view PCR jitter values that are outside the range defined by the auto-scaling. Clicking the **Clear** button will clear historical data from the histogram.

Tooltip functionality provides information about each histogram bar: the number of samples, the percentage of total number of samples and the jitter interval represented by the bar. For PCR measurements to be



valid it is essential that the signal be stuffed with null packets (PID 8191) to obtain an absolutely constant bitrate. The stream info above the histogram shows if the analyzed stream contains null packets or not. A color indicator above the PCR jitter histogram indicates whether the signal is of constant bitrate or not, as perceived by the PCR filter in the processing engine. Green indicates OK, red indicates that the PCR jitter measurements are not valid due to the bitrate not being constant.

Note that PCR jitter measurements for Ethernet streams are very sensitive to packet loss, and packet loss results in a large jitter values – often for all PCR PIDs of an MPTS.

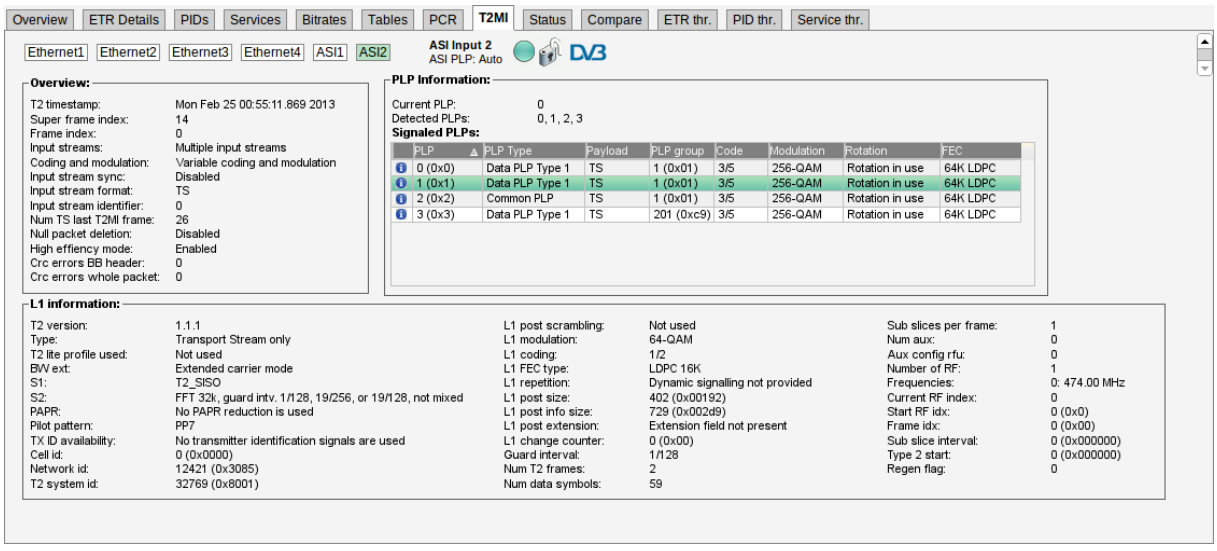
The PCR PID list displays the following parameters:

PID:	The PID for which the following parameters apply.
Current:	The last PCR jitter value measured.
Overall max:	The maximum PCR jitter value measured since transport stream sync was obtained. Note that this may not correspond to the maximum value for PCR jitter in the histogram, as the histogram displays values measured from the time when a PCR PID was selected.
Threshold:	The PCR jitter threshold currently valid for the stream, as defined in the associated ETR threshold template.

In addition to the histogram itself, the following parameters are displayed:

Max jitter (ns):	The maximum jitter value measured from the time the PID was selected.
Average jitter (ns):	The average jitter in nanoseconds.
Bin resolution (ns):	The width of the jitter interval spanned by each histogram bar.
Outside thresholds:	The number of PCR values that are outside the PCR jitter thresholds (defined by the user as part of the ETR threshold template).
Out of view:	The number of PCR values that are out of the currently displayed view.

5.9.8 ETR 290 — T2MI (requires T2MI-OPT)





T2MI monitoring is a licensing option available for transport streams over Ethernet. T2MI is enabled on a per stream basis, most of the information is found in this GUI extracted from the L1 current packets in the T2MI streams. The full parsing of this information table is found in the 'Tables' section.

Please note that the T2MI stream needs to have either a relative or an absolute T2 Timestamp to be received properly. Signals without timing information can not be received.

Overview:	
T2 timestamp:	The last received T2 timestamp. The probe supports both relative and absolute timestamps.
Super frame index:	The last received superframe index.
Frame index:	The index of the last received frame.
Input streams:	Indicates whether Single or Multiple Input Streams are used.
Coding and modulation:	Whether the stream uses Constant Coding and Modulation or Adaptive Coding and Modulation.
Input stream sync:	The Input Stream Synchronizer (ISSY) value.
Input stream format:	The format of the input stream. Will normally be 'TS'.
Input stream identifier:	The input stream identifier for the current stream.
Num TS pkt. last T2MI frame:	The number of transport stream packets that was in the last T2MI frame.
Null packet deletion:	Whether null packet deletion is in use or not.
High efficiency mode:	Whether high efficiency mode is active or not.
Crc Errors BB header:	The number of CRC errors on the BB header detected since the monitoring of the stream started.
Crc Errors whole packet:	The number of CRC errors calculated over the whole T2MI packet since the monitoring of the stream started.

L1 information:	
T2 version:	The version of the T2 spec used. Up to version 1.3.1 is supported including T2 lite.
Type:	The type of data carried in the Transport stream.
T2 lite profile used:	Set to true if the T2 lite profile is used for sending power efficient broadcasts to portable clients.
BW ext:	The carrier mode (normal or extended).
S1:	T2-SISO, T2-MISO or Non-T2.
S2:	FFT mode and guard interval.
PAPR:	The PAPR reduction mode (if any).
Pilot pattern:	Pilot pattern PP1 to PP8.
TX ID availability:	Should always be set to 'No transmitter identification signals are used'.
Cell id:	The cell ID for the transmitter.
Network id:	The network id for this DVB-T2 network.
T2 system id:	The T2 system id.

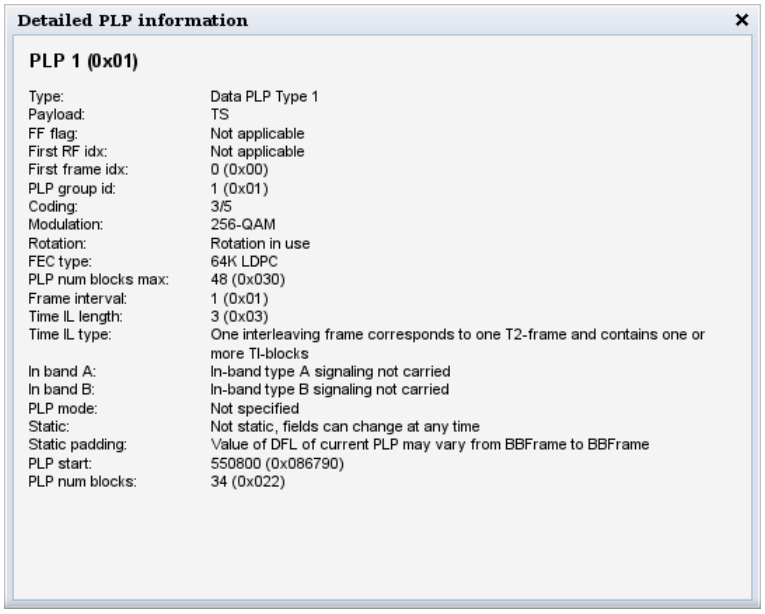


L1 post scrambling:	Says whether post scrambling is used or not.
L1 modulation:	The L1 modulation type used. BPSK, QPSK, 16-QAM or 64-QAM.
L1 FEC type:	The L1 fec type in use. Only 'LDPC 16K' is currently supported in DVB-T2.
L1 repetition:	Shows if dynamic signaling is provided.
L1 post size:	The L1 post size.
L1 post info size:	The L1 post info size.
L1 post extension:	Shows if extension field is provided.
L1 change counter:	The value of the L1 change counter.
Guard interval:	The guard interval used for the transmission. 1/32, 1/16, 1/8 or 1/4.
Num T2 frames:	The number of T2 frames signaled.
Num data symbols:	The number of data symbols signaled.
Sub slices per frame:	How many sub slices are used per T2 frame.
Num aux:	The number of auxiliary channels transmitted.
Aux config rfu:	The aux config rfu number.
Number of RF:	The number of RF frequencies used to transmit the signal.
Frequencies:	The list of frequencies used to transmit the signal. Normally only one frequency will be used.
Current RF index:	The index of the frequency currently being used for the transmission.
Start RF idx:	The starting RF index.
Frame idx:	The frame index.
Sub slice interval:	The interval between sub slices.
Type 2 start:	The value of the type 2 start parameter.
Regen flag:	The value of the regen flag.

PLP (Physical Layer Pipes) information:	
Current PLP:	The PLP currently being received. If a specific PLP was configured the interface settings T2MI extraction (**Multicasts — Streams**), this will be used. If auto mode is used the first PLP detected will be used.
Detected PLPs:	The detected PLP ids in the T2MI stream. In some error situations this may differ from the list of Signaled PLPs show below.
Signaled PLPs:	Lists the PLPs signaled in the stream.
PLP type:	The signaled type of the PLP. Data PLP Type 1 is the most common, some signals can have a common PLP as well as well as other PLP types.
Payload:	Payload type of this PLP. Will typically be the Transport Stream format
PLP Group:	The group signaled for this PLP. The PLPs in a group shares one common PLP and when analyzing a PLP both the data in the specified PLP and the common PLP in the same group (if present) are extracted. The PLP contains PIDs which are shared such as PAT, SDT, NIT, CAT and EMMs. In the example above , analyzing PLP 0 will also analyze PLP 2.
Code:	The FEC coding scheme used for this PLP.

Modulation:	Modulation for the the PLP.
Rotation:	Specifies if IQ rotation is enabled.
FEC:	Specifies the FEC coding type for this PLP.

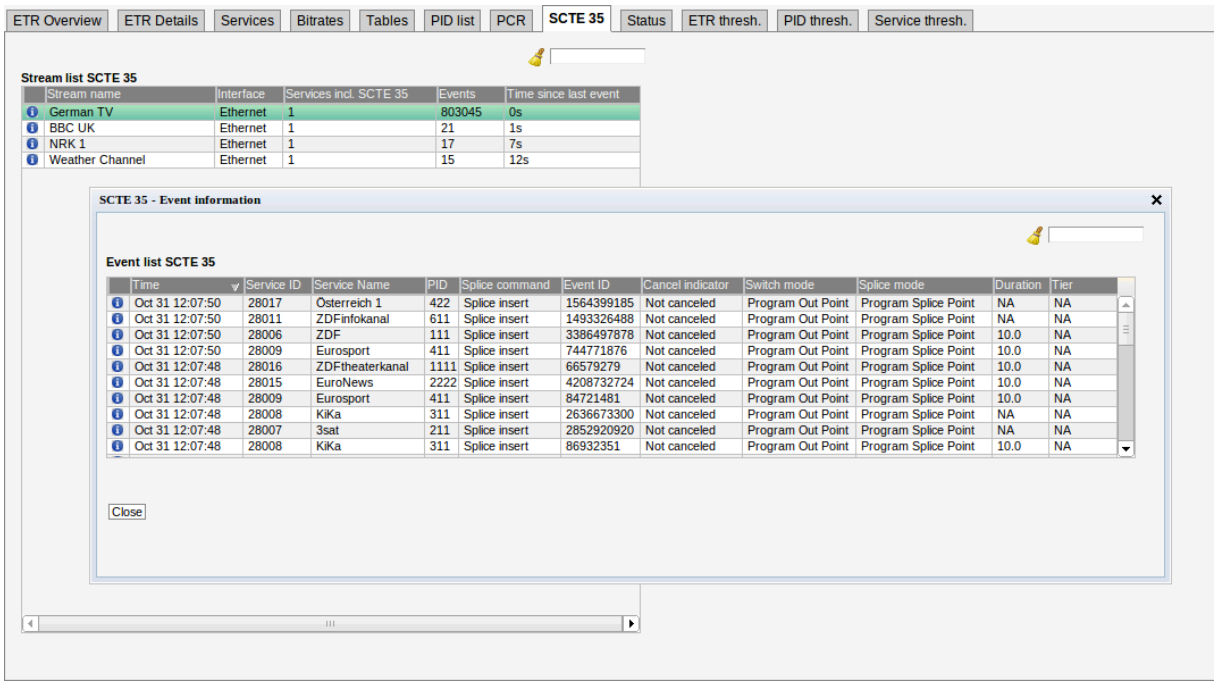
Clicking the blue information symbol in the PLP list will bring up more detailed information for that PLP.



Detailed PLP information:	
PLP:	The ID of the signaled PLP.
Type:	The signaled type of the PLP. Data PLP Type 1 is the most common, some signals can have a common PLP as well as well as other PLP types.
Payload:	Payload type of this PLP. Will typically be the Transport Stream format
FF flag:	The FF flag value.
First RF idx:	The first first RF index used for transmitting this PLP.
First frame idx:	The first frame index used to transmit this PLP.
PLP group id:	The group signaled for this PLP. The PLPs in a group shares one common PLP and when analyzing a PLP both the data in the specified PLP and the common PLP in the same group (if present) are extracted. The PLP contains PID which are shared such as PAT, SDT, NIT, CAT and EMMs.
Coding:	The FEC coding scheme used for this PLP.
Modulation:	Modulation used for transmitting this PLP.
Rotation:	Specifies if IQ rotation is enabled for this PLP.
FEC type:	Specifies the FEC coding type for this PLP.
PLP num blocks max:	The maximum number of blocks which can be used by this PLP.
Frame interval:	The frame interval for this PLP.
Time IL length:	The length of the time interleaver.
Time IL type:	The time interleaving type in use.

In band A:	Says if in-band type A signaling is used for this PLP.
In band B:	Says if in-band type B signaling is used for this PLP.
PLP mode:	The PLP mode for this PLP.
Static:	Says whether the PLP bandwidth is static or not static.
Static padding:	Says whether the padding is static or can change between each BB frame.
PLP start:	The start value for the PLP in the stream.
PLP num blocks:	The number of blocks used for this PLP.

5.9.9 ETR 290 — SCTE 35 (requires SCTE35-OPT)



SCTE 35 is a specification which allows equipment to splice in local content at specific times, SCTE 35 is basically just the signaling mechanism the equipment uses to know when to switch from the master transmission to insert local content. It can be used to allow insertion of local advertising at certain points in time or to allow the local operator to insert their own programs such as local news transmission.

SCTE 35 requires a license for the probe and also an ETR 290 engine to connect it to.

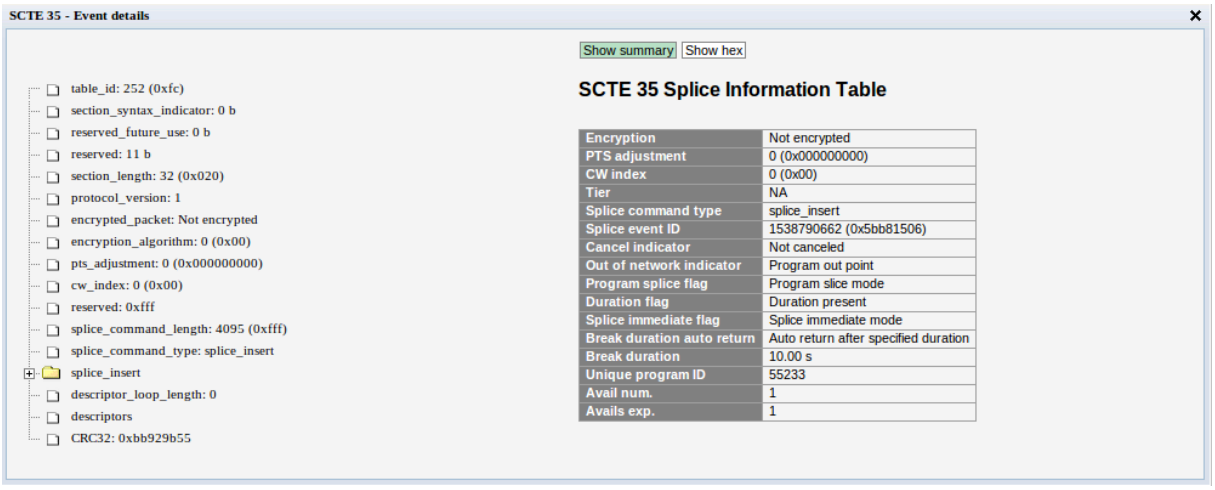
The SCTE 35 option enables monitoring of SCTE 35 events of all streams captured by the ETR engines. It is recommended to have one ETR engine dedicated to each SCTE 35 streams to get continuous monitoring.

The stream list parameters	
Stream name:	Name specified by the user when adding a multicast or tuning.
Interface:	The input source of the transport stream.
Services incl. SCTE 35:	The number of services in the transport stream which has SCTE 35 information.
Events:	The number of SCTE 35 events occurred in a transport stream.
Time since last event:	The time since last SCTE 35 event specified in seconds, minutes, hours or days.

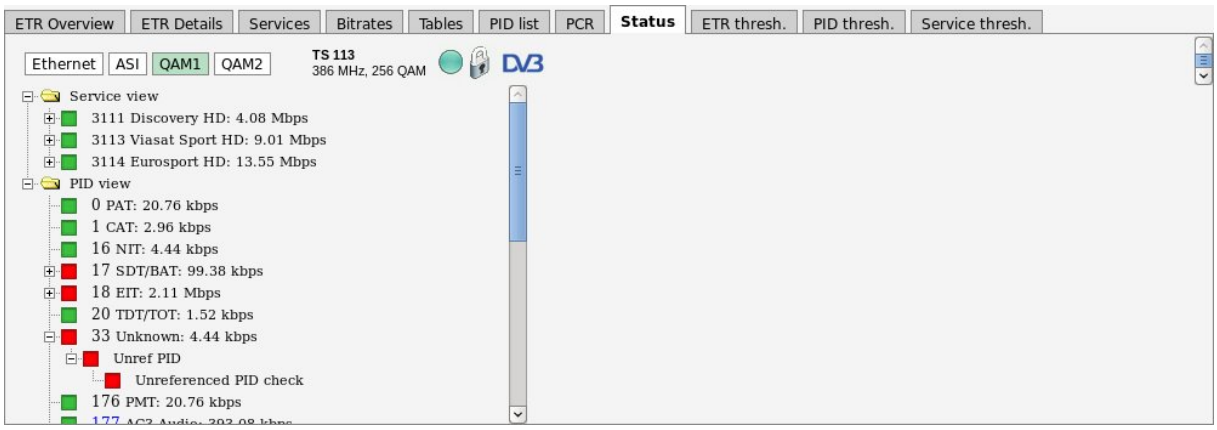
If an ETR engine is monitoring a transport stream containing SCTE 35 information, the current stream will be added to the list in the SCTE 35 view. By pressing the blue information button a new pop-up will show up, the pop-up will give specific information about events in the specified transport stream.

The event information list parameters:	
Parameter	***Description***
Time:	When the event occurred.
Service ID:	The ID of the service for which the event applies.
Service name:	The name of the service for which the event applies.
PID:	The PID carrying the SCTE 35 information. A service can have multiple SCTE 35 PIDs signaled in the PMT table.
Splice command:	The type of the splice command.
Event ID:	Id of the specific event.
Canceled indicator:	If set it indicates that this splice message cancels a previously sent splice message.
Switch mode:	Specifies whether it is a splice in (switch to local content/ads) or splice out event (switch back to the audio/video in the stream).
Splice mode:	Specifies whether the splice message applies to the entire service (Program splice mode) or individual PID(s).
Duration:	The time when a splice occurred to its end.
Tier:	Specifies which tier group are to use this splice message. Multiple splice messages can be sent addressed to different tier groups to allow switching at different times.

When pressing the information button for a specific event a new window will pop-up with detailed information about the event. The pop-up will show a log of the SCTE 35 events signaled for the specified transport stream. Splice NULL messages are not logged.



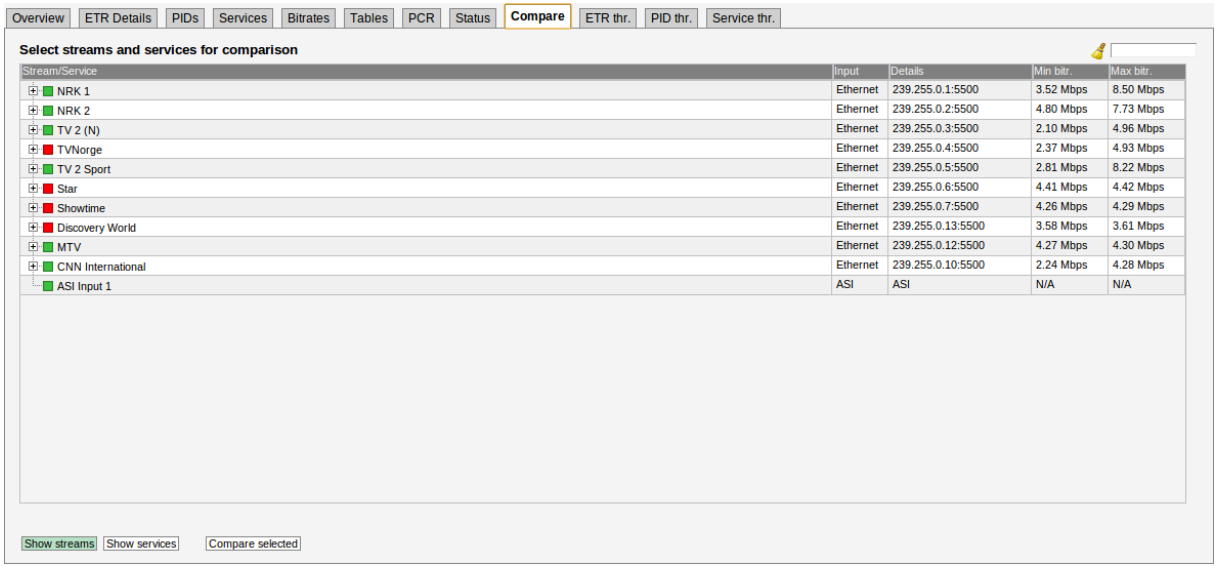
5.9.10 ETR 290 — Status



The **ETR 290 — Status** view shows a stream content overview linked to current alarms, making it easy to view what services and PIDs are currently affected by errors.

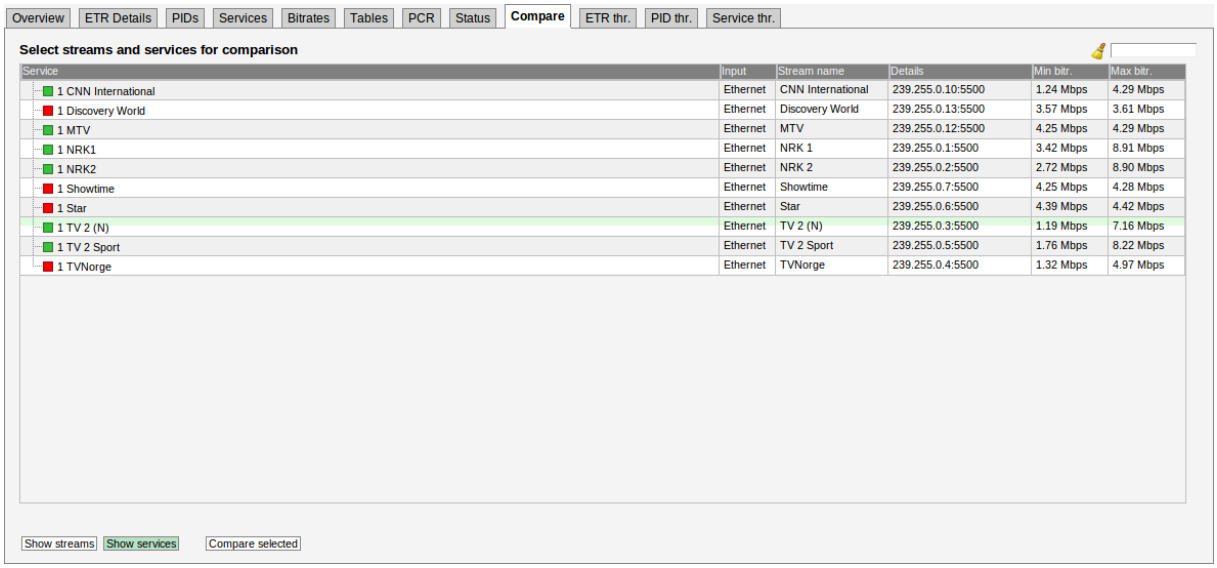
By clicking any of the 'view', service or PID nodes, more information will be displayed on the right hand side of the table. This information is described in **ETR 290 — Services**.

5.9.11 ETR 290 — Compare

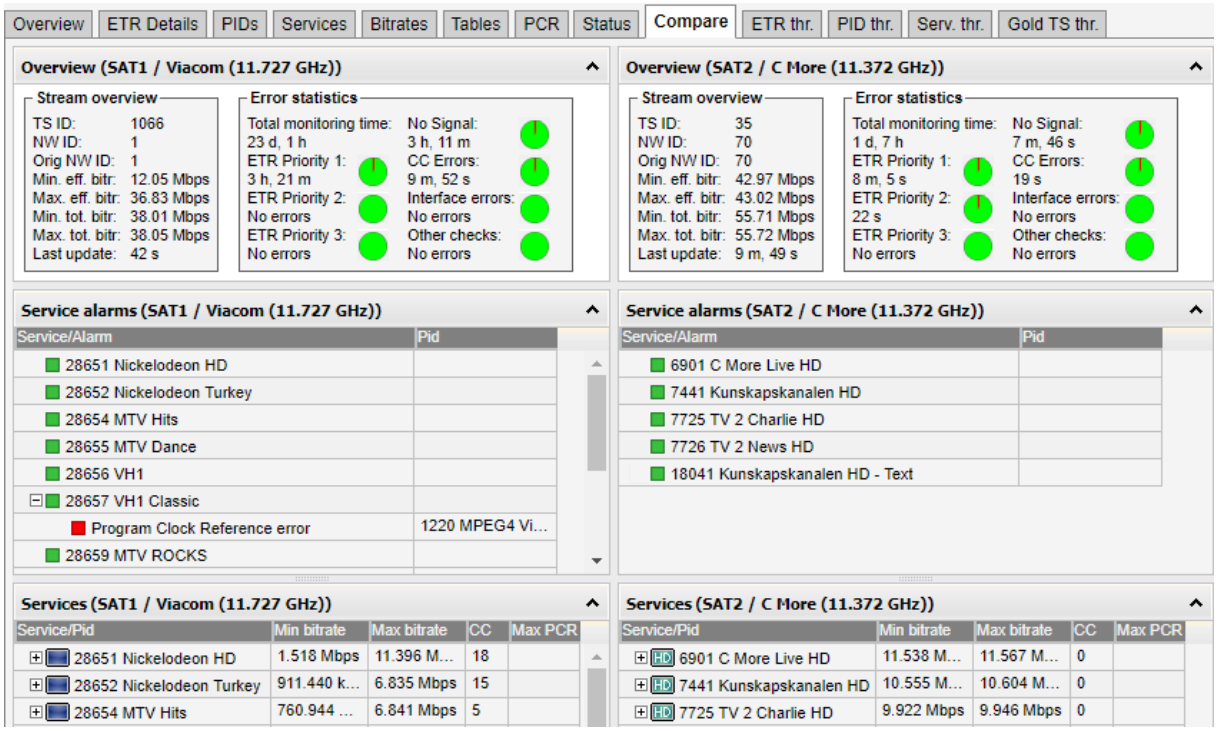


The **Compare** view is based on analysis performed by the ETSI TR 101 290 engine and only the streams monitored by ETR will be listed.

The **Compare** view allows comparison of services or transport streams across different probe interfaces. Clicking **Show streams** results in a list of selectable transport streams and services, and clicking **Show services** results in a list of selectable services. Note that the screen is not auto-refreshed, click the **Compare** tab to perform an active refresh.

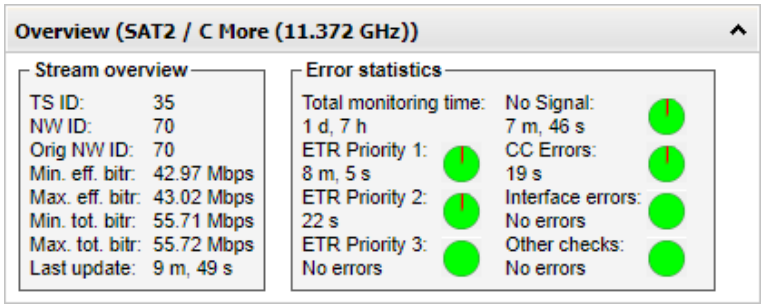


One or more services or transport streams are selected by clicking and later Ctrl + clicking items from the list. Clicking the **Compare selected** button will launch a condensed overview page that allows status parameters for services or streams to be viewed side by side. Key parameters are presented in one column for each service/stream, and it is easy to recognize differences in signal contents or alarm status. The number of streams that can be compared depends on screen size.



The compare column consists of several sub-views:

Stream overview



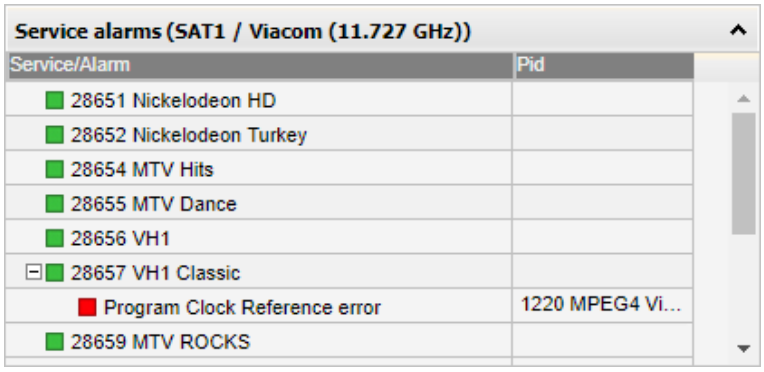
Stream overview shows a number of key parameters for the selected stream/service.

Stream overview	
TS ID:	The transport stream ID of the selected stream or the stream containing the selected service
NW ID:	The network ID of the selected stream or the stream containing the selected service
Orig NW ID:	The original network ID of the selected stream or the stream containing the selected service
Min. eff. bitr:	The minimum effective bitrate (null packets removed) measured for the selected stream or the stream containing the selected service
Max. eff. bitr:	The maximum effective bitrate (null packets removed) measured for the selected stream or the stream containing the selected service
Min. tot. bitr:	The minimum total bitrate (including null packets) measured for the selected stream or the stream containing the selected service
Max. tot. bitr:	The maximum total bitrate (including null packets) measured for the selected stream or the stream containing the selected service
Last update:	The time since the last update. The information will be updated when the round robin ETR engine stops monitoring a stream or once every minute for streams which are permanently monitored.

Error statistics	
Total monitoring time:	The total time the stream has been monitored by the ETR engine
ETR Priority 1:	The time the stream has been affected by ETSI TR 101 290 Priority 1 errors
ETR Priority 2:	The time the stream has been affected by ETSI TR 101 290 Priority 2 errors
ETR Priority 3:	The time the stream has been affected by ETSI TR 101 290 Priority 3 errors
No signal:	The time the stream has been affected by ‘No signal’ alarm
CC errors:	The time the stream has been affected by ‘CC error’ alarm
Interface errors:	The time the stream has been affected by ‘Interface error’ alarm
Other checks:	The time the stream has been affected by miscellaneous ‘Other’ alarms

Pie charts indicate for how long the stream has been affected by errors compared to the total monitoring time, green color representing ‘OK’ and red color ‘Error’.

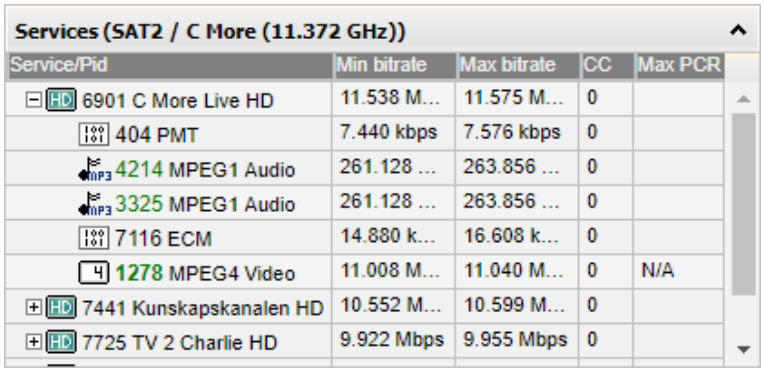
Service alarm



If a transport stream is selected for comparison the **Service alarms** subview displays a list of services present in the stream. If there is one or more active alarms for a service this will be indicated by a red 'bulb' whereas a green 'bulb' indicates no active alarms. If a service is affected by one or more active alarms these alarms may be viewed by expanding the service tree. If relevant the PIDs affected by alarms are also displayed. Note that only alarms detected during the last monitoring period are displayed.

If a service is selected for comparison this subview simply shows the selected service and any active alarms affecting the service.

Services

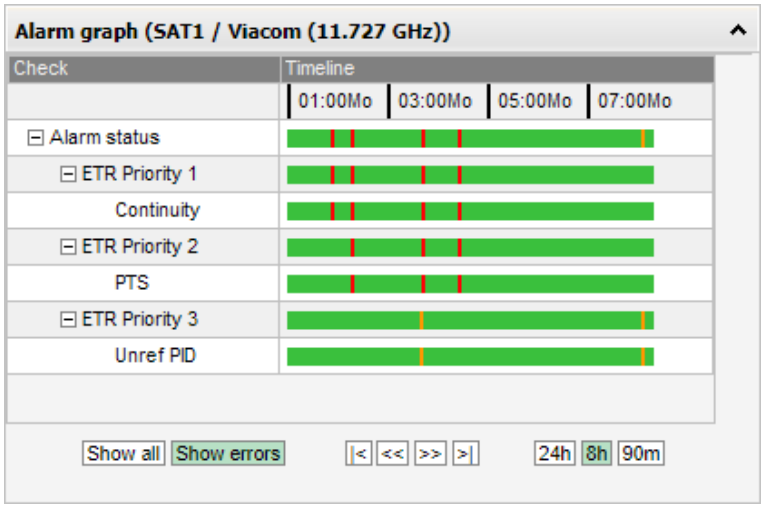


If a transport stream is selected for comparison the **Services** subview displays a list of services present in the stream. Clicking the plus icon at a service will expand the service tree, displaying the service's individual components. The minimum and maximum effective bitrates of a service/component are also shown, in addition to the number of continuity counter errors and the maximum measured PCR jitter (if relevant).

Colored PIDs indicate scrambling; blue and green representing odd and even scrambling respectively.

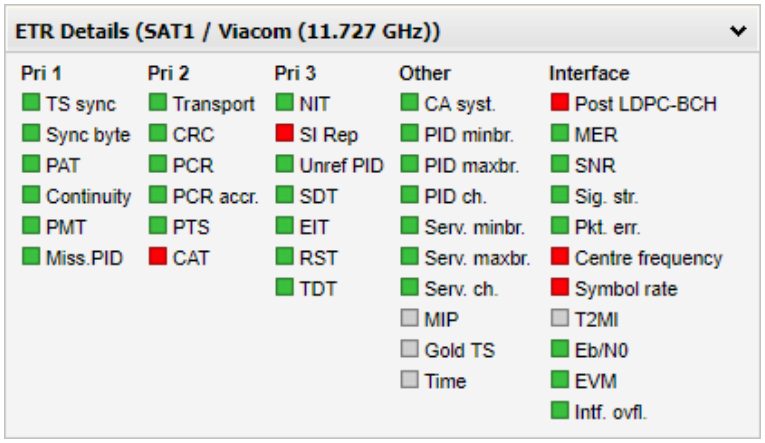
Note that all references to a PID will result in a PID entry, i.e. one PID may be displayed several times in the list.

Alarm graph



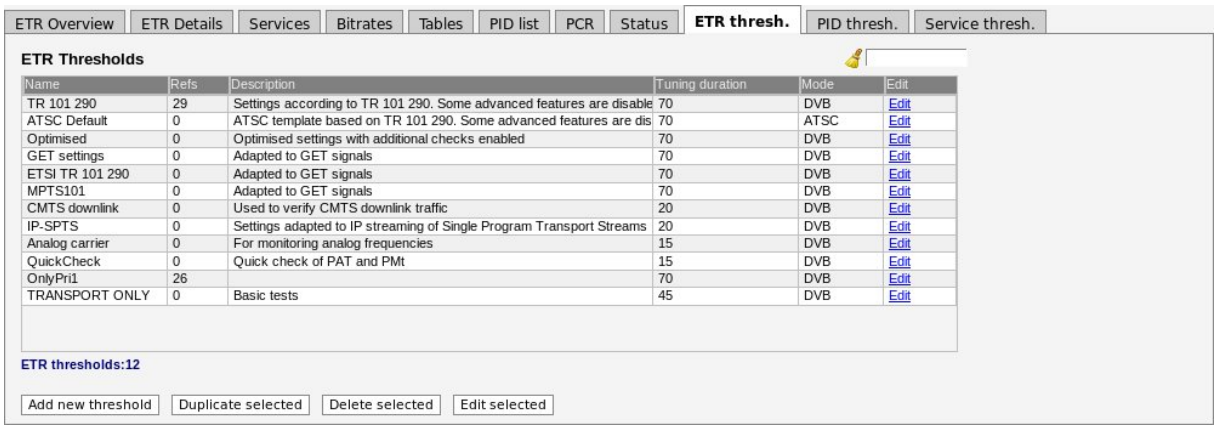
The Alarm graph subview shows similar alarm graphs as the **ETR 290 — ETR Details — Alarm graph popup** view. Please refer to the **ETR 290 — ETR Details** section of this User's Manual for a comprehensive description of this view.

ETR Details



The ETR details subview shows the same alarm overview as the **ETR 290 — ETR Details** view. Clicking a check will open a pop-up view displaying alarm details. Please refer to the **ETR 290 — ETR Details** section of this user's manual for a comprehensive description of this view.

5.9.12 ETR 290 — ETR threshold





The **ETR thresholds** make it possible to define detailed conditions for ETR 290 alarm triggering on a per-stream basis. There are seven predefined ETR threshold templates that are write-protected and cannot be edited by the operator:

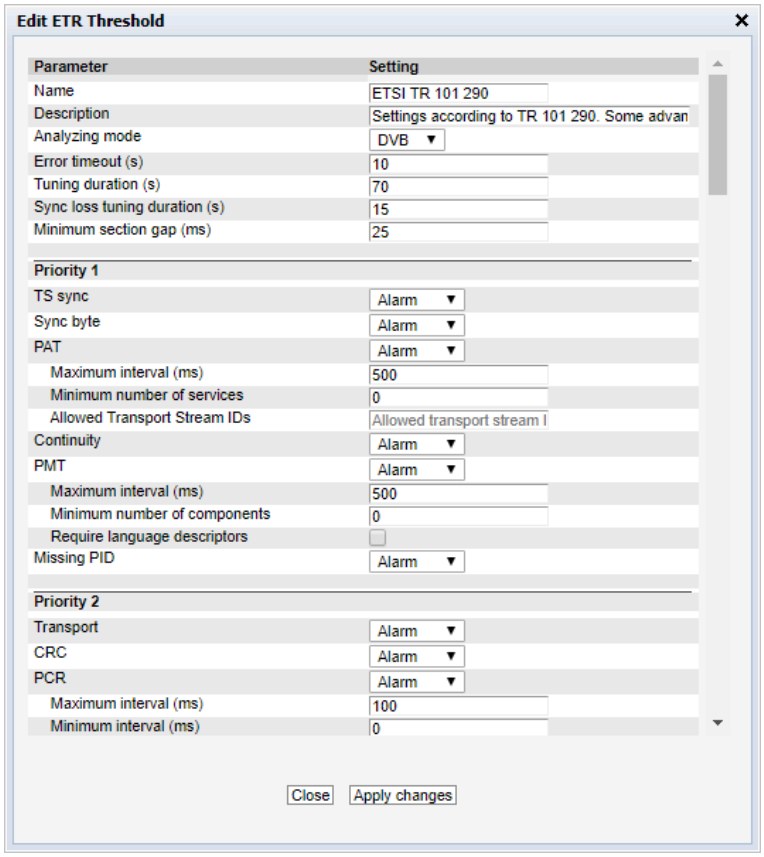
- Default
- ETSI TR 101 290
- ATSC Default
- Optimised
- IP-SPTS
- CMTS downlink
- Analog carrier

These predefined thresholds may be used when defining a monitoring configuration, but it is a good idea to create editable copies of these threshold templates and use these copies rather than the originals. Doing so will allow fine-tuning of parameters later on.

There are two different ways of creating user-defined thresholds. To create a new threshold template from scratch the operator should click the **Add new threshold** button. A pop-up window will appear allowing the user to define alarm conditions and set the round-robin cycling time. The default values of the different parameters settings are in accordance with the template **Default**. Another way of creating a user-defined threshold template is by highlighting one of the threshold templates already defined and then click the **Duplicate highlighted** button. The copy created this way may be edited during the fine-tuning phase of system configuration.

Deleting an ETR threshold template is done by highlighting the threshold template that should be removed and clicking **Delete highlighted**. Note that if the deleted threshold template is assigned to a stream currently being monitored, the new threshold for that stream will default to the predefined **Default** threshold template.

It is possible to perform multi-editing of existing threshold templates by selecting several threshold templates (using the regular *Ctrl + click* or *Shift + click* functionality) and clicking **Edit selected**. Parameters that differ between the threshold templates will be represented by an asterisk in the **Edit ETR threshold** view. Changes made will affect all selected threshold templates.



The ETR threshold template has the following settings:

ETR Thresholds — Parameters:	
Name:	A text field with the name of the ETR threshold template
Description:	Text field that should contain a meaningful description of the threshold
Analyzing Mode:	The mode of table analysis. DVB, ATSC or ISDB may be selected.
Error timeout (s):	The number of seconds an alarm stays active before it is cleared, if no new alarms are generated. For all table related alarms the actual alarm timeout used is the sum of the Error timeout parameter and the maximum table repetition period. E.g. the TDT (Time Date Table) with table repetition set to 30 seconds will have an effective error timeout of 40 seconds. This avoids toggling of alarms for tables that are sent infrequently. Default value: 10 s

Tuning duration (s):	The time (in seconds) the probe will stay tuned to a frequency/multicast during the round-robin loop. For setting the tuning duration, use the following expression: max_table_rep*2 + 10 Use the maximum table repetition, multiply it by 2 and then add 10 seconds. E.g. with TDT repetition set to 30 seconds, use 30*2+10=70 seconds tuning duration. In order to speed up the tuning process tables should be transmitted more frequently. For instance if TDT, which is usually the least frequently transmitted table, is sent every 10 seconds, a tuning duration of 30 seconds may be used. For signals without TDT (common in SPTS) the TDT check can be disabled and the tuning duration may be reduced. If the tuning duration is set too low the checks for tables with long table repetition periods will still be in an unknown state as the probe does not have enough measurements to determine the state for these. Tuning duration should never be set to less than 10 seconds for Ethernet streams and 15 seconds for all other streams (the minimum for RF steams depends on the setup). Default value: 70 s
Sync loss tuning duration (s):	The time (in seconds) the probe will stay tuned to a frequency/multicast with TS Sync loss during the round-robin tuning process. Usually there is no need to stay tuned to a frequency/multicast once the probe has established that there is no signal on the tuning setup. When monitoring a tuning setup with signal loss, the probe will use the lowest value of 'Tuning duration' and 'Sync loss tuning duration', e.g. if the former is set to 60 seconds and the latter to 1000 seconds, 60 seconds will be used. Default value: 15 s
Minimum section gap (ms):	The minimum gap between transmission of two consecutive sections with the same table ID. If the sections are transmitted too rapidly the STB may not be able to process the data in time and various problems can occur. However newer STBs can normally handle lower section gaps than the default value of 25ms. The section gap time is measured as the time between reception of the last TS packet of two consecutive (complete) sections. This section gap setting is used for PAT, PMT, CAT, NIT, RST, TDT, MGT, VCT, PIM/PNM, RRT, ATSC EIT, ETT and STT. There are separate gap settings for SDT and EIT. Default value: 25 ms

ETR Thresholds — Priority 1:	
TS sync:	Enable or disable alarming of no signal error (TS sync loss)
Sync byte:	Enable or disable alarming of sync byte errors
PAT:	Enable or disable alarming of Program Association Table errors
PAT – Maximum interval (ms):	The maximum allowed section repetition interval for the PAT table. Default according to ETSI TR 101 290: 500 ms
PAT – Minimum number of services:	The minimum number of services that must be present in the PAT. Set to 0 to disable this check. Default: 0



PAT – Allowed Transport Stream IDs:	When this field is left blank all TS IDs are considered valid. If one or more TS IDs are specified (separated by commas or as a range) only these IDs are considered valid, and any other TS ID will trigger an alarm. Example of a valid field: '100-120, 300,320'
Continuity:	Enable or disable alarming of Continuity Counter errors
PMT:	Enable or disable alarming of Program Map Table errors
PMT – Maximum interval (ms):	The maximum allowed section repetition interval for the PMT tables. Default according to ETSI TR 101 290: 500 ms
PMT – Minimum number of components:	The minimum number of components that must be present in all services. Set to 0 to disable this check. Default: 0
PMT – Require language descriptors:	If enabled it requires a language descriptor to be present for all audio components signaled in the PMT. Default: Disabled
Missing PID:	Enable or disable alarming of missing PID errors

Note that errors affecting individual PIDs may be effectively masked by creating suitable PID threshold templates that are associated with these PIDs. This is particularly useful for PIDs affected by continuity counter errors, missing PID errors and unreferenced PID errors.

ETR Thresholds — Priority 2:	
Transport:	Enable or disable alarming of Transport error indicator errors
CRC:	Enable or disable alarming of checksum errors for tables
PCR:	Enable or disable alarming of Program Clock Reference errors
PCR – Maximum interval (ms):	The maximum interval between reception of PCR values. Default according to ETSI TR 101 290: 40 ms
PCR – Minimum interval (ms):	The minimum interval between reception of PCR values. Normally this setting should be 0. Default: 0 ms
PCR – Discontinuity threshold (ms):	The maximum change in the PCR value between two adjoining PCR values (where the discontinuity indicator flag has not been set). Default according to ETSI TR 101 290: 100 ms
PCR – Require presence of PCR:	When enabled an alarm will be raised if a PID signaled as PCR in the PMT does not carry PCR information
PCR Accuracy:	Enable or disable alarming of PCR Accuracy (PCR Jitter) errors for OCR_AJ and PCR_OJ. PCR_OJ is not relevant for Ethernet streams.
PCR Accuracy – Maximum PCR_AC jitter (ns):	The maximum allowed PCR jitter for PCR_AC measurements. Default according to ETSI TR 101 290: 500 ns
PCR Accuracy – Maximum PCR_OJ jitter (ns):	The maximum allowed PCR jitter for PCR_OJ measurements. PCR_OJ measurement does not apply to IP streams. Default according to ETSI TR 101 290: 500 ns

PTS:	Enable or disable alarming of Presentation Time Stamp errors
PTS – Maximum interval (ms):	The maximum allowed interval between the reception of two PTS values. Default according to ETSI TR 101 290: 700 ms
CAT:	Enable or disable alarming of Conditional Access Table errors
CAT – Maximum interval (ms):	The maximum allowed section repetition interval for the CAT table. Default according to ETSI TR 101 290: 500 ms

ETR Thresholds — Priority 3:	
NIT:	Enable or disable alarming of Network Information Table errors. Only relevant when DVB mode is selected.
NIT – Maximum interval Actual (ms):	The maximum allowed section repetition interval for the NIT Actual table. Default according to ETSI TR 101 290: 10 s
NIT – Maximum interval Other (ms):	The maximum allowed section repetition interval for the NIT Other table. Default according to ETSI TR 101 290: 10 s
NIT – Require network id:	If enabled the probe will require that the network ID found in the NIT matches the configured value. Default: Disabled
NIT – Require orig. netw. id:	If enabled the probe will require that the original network ID found in the NIT matches the configured value. Default: Disabled
NIT – Min. num. transport streams:	The minimum number of transport streams that must be present in the NIT. Set to 0 to disable this check. Default: 0
NIT – Cable descriptor (DVB-C):	If set to 'Required' an alarm will be generated if a DVB-C Cable descriptor is not present in the NIT for the monitored frequency. Similarly if set to 'Not allowed', an alarm will be generated if the DVB-C Cable descriptor is present. Default: Optional
NIT – Cable descriptor (DVB-C2):	If set to 'Required' an alarm will be generated if a DVB-C2 Cable descriptor is not present in the NIT for the monitored frequency. Similarly if set to 'Not allowed', an alarm will be generated if the DVB-C2 Cable descriptor is present. Default: Optional
NIT – Satellite descriptor (DVB-S):	If set to 'Required' an alarm will be generated if a DVB-S Satellite descriptor is not present in the NIT for the monitored frequency. Similarly if set to 'Not allowed', an alarm will be generated if the DVB-S Satellite descriptor is present. Default: Optional
NIT – Satellite descriptor (DVB-S2):	If set to 'Required' an alarm will be generated if a DVB-S2 Satellite descriptor is not present in the NIT for the monitored frequency. Similarly if set to 'Not allowed', an alarm will be generated if the DVB-S2 Satellite descriptor is present. Default: Optional



NIT – Terrestrial descriptor (DVB-T):	If set to 'Required' an alarm will be generated if a DVB-T Terrestrial descriptor is not present in the NIT for the monitored frequency. Similarly if set to 'Not allowed', an alarm will be generated if the DVB-T Terrestrial descriptor is present. Default: Optional
NIT – Terrestrial descriptor (DVB-T2):	If set to 'Required' an alarm will be generated if a DVB-T2 Terrestrial descriptor is not present in the NIT for the monitored frequency. Similarly if set to 'Not allowed', an alarm will be generated if the DVB-T2 Terrestrial descriptor is present. Default: Optional
NIT – Compare with reference NIT:	If enabled the NIT will be compared with the NIT on the reference frequency, and an alarm will be generated if a mismatch is found. The first frequency in the tuning list will be used as the reference frequency. Both the CRC values of the different sections and the number of sections must be identical. Default: Disabled
SI Repetition Rate:	Enable or disable alarming of SI Repetition Rate errors.
Unreferenced PID:	Enable or disable alarming of Unreferenced PID errors. To mask Unreferenced PID alarms for a PID create a PID threshold template where this error is masked.
SDT:	Enable or disable alarming of Service Description Table errors. Only relevant when DVB mode is selected.
SDT – Maximum interval Actual (ms):	The maximum allowed section repetition interval for the SDT Actual table. Default according to ETSI TR 101 290: 2 000 ms
SDT – Maximum interval Other (ms):	The maximum allowed section repetition interval for the SDT Other table. Default according to ETSI TR 101 290: 10 000 ms
SDT – Minimum gap interval (ms):	The minimum allowed section gap interval for the SDT table. Default according to ETSI TR 101 290: 25 ms
SDT – Verify SDT against PAT:	If enabled an alarm will be generated if a service found in the PAT is not listed in the SDT. Default: Disabled
SDT – Require service name:	If enabled an alarm will be generated if a service found in the PAT does not have a service name or if the service name is empty. Default: Disabled
SDT – Require BAT Presence:	If enabled an alarm will be generated if BAT is not present in the stream. Default: Disabled
EIT:	Enable or disable alarming of Event Information Table errors. Only relevant when DVB mode is selected.
EIT – Maximum interval Actual (ms):	The maximum allowed section repetition interval for the EIT Actual table. Default according to ETSI TR 101 290: 2 000 ms
EIT – Minimum gap interval (ms):	The minimum allowed section gap interval for the EIT tables. Default according to ETSI TR 101 290: 25 ms



EIT – Required Table IDs:	If one or more table IDs are specified an alarm will be generated if these table IDs are not present in the stream on the EIT PID. Entries should be separated by commas, or a range may be specified. Example: '78,79,80-85' Default: Disabled
EIT – Verify that present event is transmitted	If enabled, an alarm will be raised if one or more services don't have a present event transmitted in the EIT (i.e. no EPG for the current program)
EIT – Check valid time for present event	If enabled, an alarm will be raised if time signaled for the present event (the current program) is not correct. The maximum offset from the current time can be configured.
EIT – Maximum timing error for present event(s)	The maximum timing error to allow for the present event. If the current time is not inside the program start/stop times by this margin then an alarm will be raised.
EIT – Verify that following event is transmitted	If enabled, an alarm will be raised if one or more services don't have a following event transmitted in the EIT (i.e. no EPG for the next program)
RST:	Enable or disable alarming of Running Status Table errors. Only relevant when DVB mode is selected.
RST – Maximum interval (ms):	The maximum allowed section repetition interval for the RST table. Default according to ETSI TR 101 290: 20 s
TDT:	Enable or disable alarming of Time Date Table errors. Only relevant when DVB mode is selected.
TDT – Maximum interval (ms):	The maximum allowed section repetition interval for the TDT and TOT tables. Default according to ETSI TR 101 290: 30 000 ms
TDT – Require TOT presence:	Check this checkbox if TOT presence is required. Default: disabled
MGT:	Enable or disable alarming of Master Guide Table errors. Only relevant when ATSC mode is selected.
MGT – Maximum interval (ms):	The maximum allowed section repetition interval for the MGT table. Default: 150ms
VCT:	Enable or disable alarming of Virtual Channel Table errors. Only relevant when ATSC mode is selected.
Require TVCT:	Require presence of the Terrestrial Virtual Channel Table.
Require CVCT:	Require presence of the Cable Virtual Channel Table.
VCT – Maximum interval (ms):	The maximum allowed section repetition interval for the VCT table. Default: 400ms
PIM/PNM:	Enable or disable alarming of Program Information Message and Program Name Message tables. Only relevant when ATSC mode is selected.
Require PIM:	Require presence of the Program Information Message table.



Maximum interval PIM (ms):	The maximum allowed section repetition interval for the PIM table. Default: 500ms
Require PNM:	Require presence of the Program Name Message table.
Maximum interval PNM (ms):	The maximum allowed section repetition interval for the PNM table. Default: 1000ms
RRT:	Enable or disable alarming of Rating Region Table errors. Only relevant when ATSC mode is selected.
RRT – Maximum interval (ms):	The maximum allowed section repetition interval for the RRT table. Default: 30000ms
STT:	Enable or disable alarming of System Time Table errors. Only relevant when ATSC mode is selected.
STT – Maximum interval (ms):	The maximum allowed section repetition interval for the STT table. Default: 1000ms
ATSC EIT:	Enable or disable alarming of ATSC Event Information Table errors. Only relevant when ATSC mode is selected.
ATSC EIT – Maximum interval EIT–0 (ms):	The maximum allowed section repetition interval for the ATSC EIT–0 table. Default: 500ms
ATSC EIT – Maximum interval EIT–1 to EIT–3 (ms):	The maximum allowed section repetition interval for the ATSC EIT–1 to EIT–3 tables. Default: 5000ms
ATSC EIT – Maximum interval EIT–4 to EIT–127 (ms):	The maximum allowed section repetition interval for the ATSC EIT–4 to EIT–127 tables. Default: 30000ms
ETT:	Enable or disable alarming of Extended Text Table errors. Only relevant when ATSC mode is selected.
ETT – Maximum interval ETT–0 (ms):	The maximum allowed section repetition interval for the ATSC ETT–0 table. Default: 2000ms
ETT – Maximum interval ETT–1 to ETT–3 (ms):	The maximum allowed section repetition interval for the ATSC ETT–1 to ETT–3 tables. Default: 5000ms
ETT – Maximum interval ETT–4 to ETT–127 (ms):	The maximum allowed section repetition interval for the ATSC ETT–4 to ETT–127 tables. Default: 30000ms

ETR Thresholds — Other checks:	
CA system checks:	Enable or disable alarming of Conditional Access System errors.

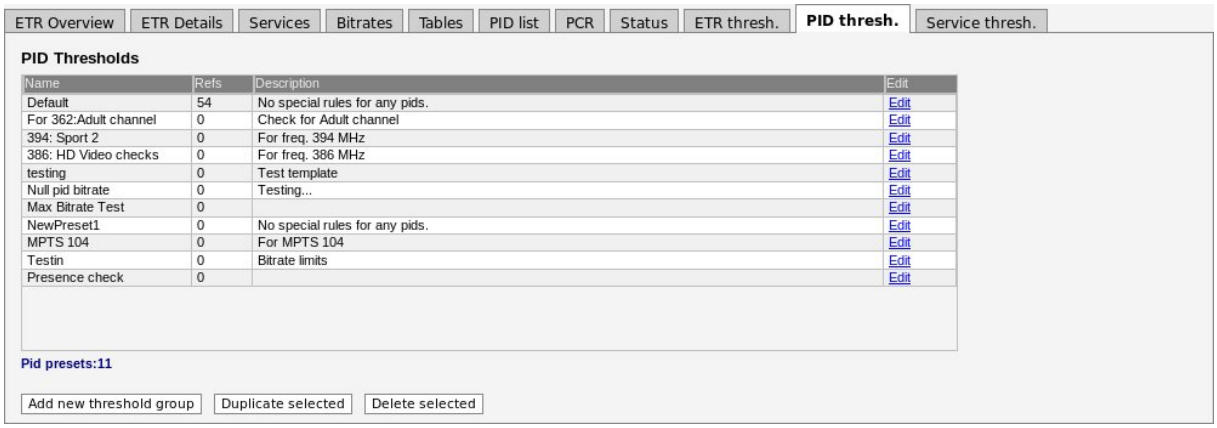
CA system checks – Maximum ECM interval (ms):	The maximum allowed ECM repetition interval. Default: 500 ms
CA system checks – Maximum ECM change period (ms):	The maximum time allowed between ECM changes. Default: 25000ms
CA system checks – Minimum avg. EMM bitrate (bps):	The minimum allowed average EMM bitrate. Default: 1000 bps
CA system checks – EMM bitrate average period (s):	The averaging period used to calculate EMM bitrate. Note that the average period must be at least 20s less than the round-robin tuning period, e.g. with a round-robin tuning period of 70s the maximum EMM bitrate average period is 50s. Default: 10s
CA system checks – Maximum control word period (ms):	The maximum allowed control word period (the maximum time that can go by without a change in the scrambling control bits for scrambled PIDs). Default: 25 000 ms
PID minimum bitrate checks:	Enable or disable alarming of PID minimum bitrate. The bitrates are set in the PID threshold template.
PID maximum bitrate checks:	Enable or disable alarming of PID maximum bitrate. The bitrates are set in the PID threshold template.
PID checks:	Enable or disable alarming of PID presence errors, scrambling/clear requirements and PID type checks. The checks are set in the PID threshold template.
Service minimum bitrate checks:	Enable or disable alarming of service minimum bitrate errors. Requirements are specified in the service threshold template associated with the stream.
Service maximum bitrate checks:	Enable or disable alarming of service maximum bitrate errors. Requirements are specified in the service threshold template associated with the stream.
Service checks:	Enable or disable alarming of service presence, scrambling/clear required, service type, service name and service ID errors. Requirements are specified in the service threshold template associated with the stream.
Service checks – Only allow services listed in service template:	Check this box to enable service ID checks against the service ID list specified in the service threshold template associated with the stream.
MIP check:	Enable or disable alarming of errors related to the Megaframe Insertion Packet.
MIP checks – Require presence of MIP:	Check this box to enable an alarm if the MIP table is missing for the stream.



MIP checks – Max MIP timing error(μs):	The maximum MIP timing error before raising an alarm. The unit is μs. Default: 10 μs
Content check:	(Content Extraction and Alarming Option) Enable or disable alarming of freeze-frame and color-freeze errors. Requirements are specified in the service threshold template associated with the stream.
Gold TS check:	Enable or disable alarming for tables failing Gold TS reference checking.
Gold TS check – Also check version number and CRC:	When enabled an alarm will be raised for any change, including a change in the table version number and CRC.
Gold TS check – Verify PAT table:	Do verification of the PAT table against the stored reference PAT table.
Gold TS check – Verify PMT tables:	Do verification of the PMT tables against the stored reference PMT tables.
Gold TS check – Verify CAT table:	Do verification of the CAT table against the stored reference CAT table.
Gold TS check – Verify SDT actual table:	Do verification of the SDT actual table against the stored reference SDT actual table.
Gold TS check – Verify SDT other tables:	Do verification of the SDT other tables against the stored reference SDT other tables.
Gold TS check – Verify BAT table:	Do verification of the BAT table against the stored reference BAT table.
Gold TS check – Verify NIT actual table:	Do verification of the NIT actual table against the stored reference NIT actual table.
Gold TS check – Verify NIT other tables:	Do verification of the NIT other tables against the stored reference NIT other tables.
Time information check:	Enable or disable alarming if there are errors in the time information sent in the streams. Probe should use NTP time sync to use this functionality.
Time information check – Check TDT:	Check the time in the TDT table and alarm if it is wrong.
Time information check – Check TOT:	Check the time in the TOT table and alarm if it is wrong.
Time information check – Check LTC:	Check the time in the Logical Time Code table and alarm if it is wrong.
Time information check – Max time offset:	The maximum number of seconds the time information provided in the stream can deviate from the probe time before an alarm is raised.

Time information check – Max repetition time:	The maximum time without any time information before an alarm is raised.

5.9.13 ETR 290 — PID thresholds

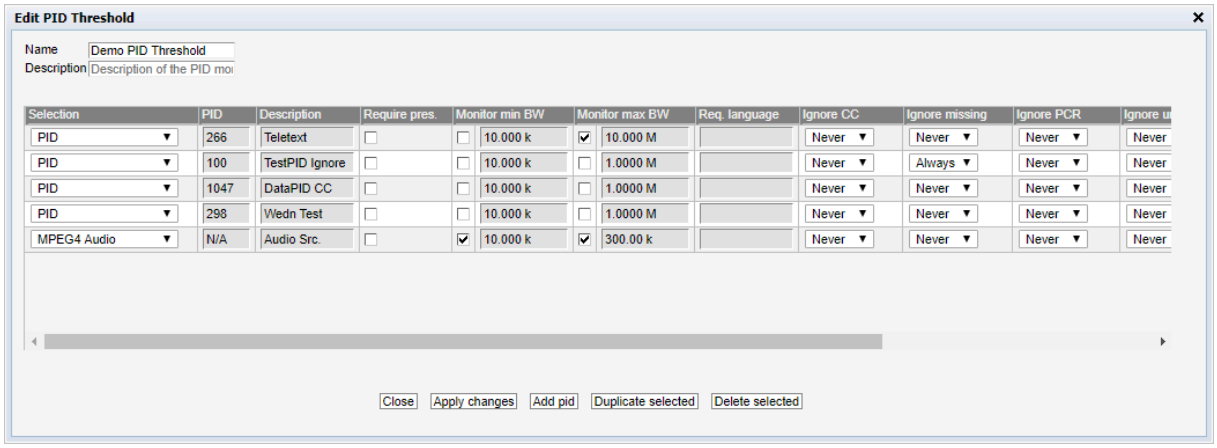


The **PID thresholds** make it possible to define detailed conditions for alarm triggering on a PID or PID type basis. There is one predefined PID threshold template that cannot be edited by the operator: 'Default'. The 'Default' PID threshold template contains no PID definitions and will therefore not alter alarming for any service.

By associating scheduling templates to checks it is possible to disable alarming at pre-selected time intervals. Scheduling templates are defined in the **Setup — Scheduling** view and will be available from a selection drop-down menu for some of the checks.

In the 'PID Thresholds' table, the 'Refs' column shows how many streams are associated with each threshold template.

There are two different ways of creating user-defined thresholds. To create a new threshold template from scratch the operator should click the **Add new threshold** template button. A pop-up window will appear allowing the user to define alarm conditions. Another way of creating a user-defined threshold template is by highlighting one of the templates already defined and then click the **Duplicate highlighted** button.



Deleting a PID threshold template is done by highlighting the threshold template that should be removed and clicking **Delete highlighted**. Note that if the deleted threshold template was assigned to a stream



being monitored, the new threshold for that stream will default to the predefined **Default** threshold template.

The PID threshold template has the following settings:

Edit PID Threshold:	
Name:	The name of the PID threshold template
Description:	Text field that should contain a meaningful description of the threshold template

PID Threshold Parameters:	
Selection:	The user selects if the requirements should apply for a specific PID or for all PIDs of a specified type. Note that the PID type detection depends on correct PSI/SI/PSIP signaling.
PID:	The PID for which the specified requirements apply. If a PID type is selected in the 'Selection' column, this field will update to read N/A when the **Apply changes** button is clicked.
Description:	A text field describing the PID or PID type requirement.
Require pres.:	If this field is checked an alarm will be raised provided that the specified PID is not present in the transport stream. Note that this check is only available for specified PIDs and not for PID types.
Monitor min BW:	An alarm is raised if the PID bandwidth goes below the specified minimum bandwidth (bandwidth in kbit/s or Mbit/s) and monitoring is enabled.
Monitor max BW:	An alarm is raised if the maximum PID bandwidth specified is exceeded (bandwidth in kbit/s or Mbit/s) and monitoring is enabled.
Req. language:	If the PID need to have a certain language code signaled in the language descriptor it can be set here. An alarm will be raised if a wrong language is signaled or if the language is not signaled.
Ignore CC:	Select a scheduling template different from 'Never' for the probe to ignore CC errors for the specified PID or PID type.
Ignore missing:	Select a scheduling template different from 'Never' for the probe to ignore that the specified PID or PID type is signaled in PSI but missing in the stream.
Ignore PCR:	Select a scheduling template different from 'Never' for the probe to ignore any PCR errors for this PID or PID type.
Ignore unref.:	Select a scheduling template different from 'Never' for the probe to ignore that the specified PID is present in the stream but unreferenced in PSI.
Ignore all:	Select a scheduling template different from 'Never' for the probe to ignore all errors for a specified PID or PID type.
Scrambling:	An alarm will be raised provided that the specified PID is scrambled when 'require clr' has been selected. Similarly an alarm will be raised if the specified PID is clear when 'require scr' has been selected. The default setting is to ignore whether the PID or PID type is scrambled or not.

5.9.14 ETR 290 — Service thresh.



The **Service thresholds** make it possible to define detailed conditions for alarm triggering on a per-service basis. There is one predefined service threshold template that cannot be edited by the operator: **Default**. The Default service threshold template contains no service definitions and will therefore not alter alarming for any service.

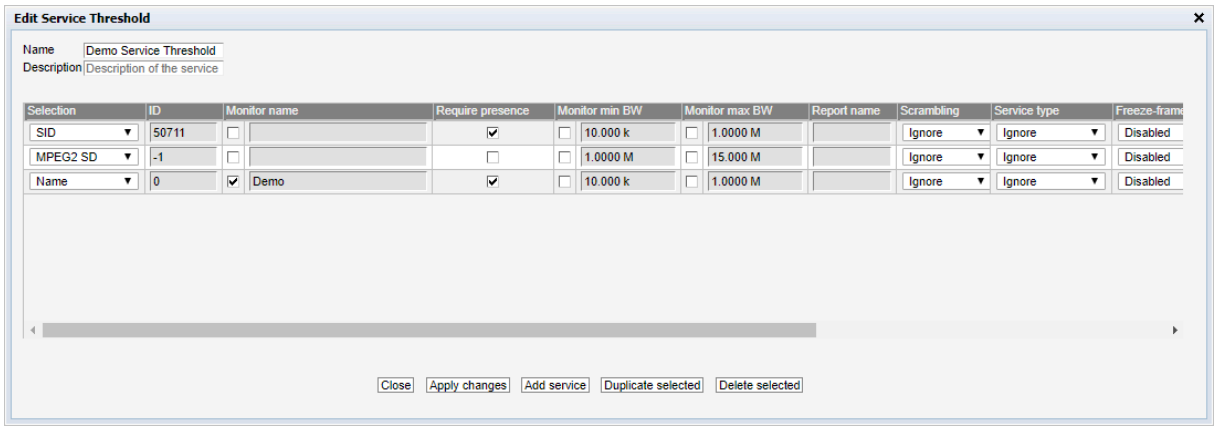
By associating scheduling templates to service threshold templates it is possible to disable alarming at pre-selected time intervals. Scheduling templates are defined in the **Setup — Scheduling** view and will be available from the schedule drop-down menu.

In the 'Service Thresholds' table, the 'Refs' column shows how many streams are associated with each threshold template. Thresholds are associated with each stream in the **Multicasts — Streams — Edit** view.

There are two different ways of creating user-defined thresholds. To create a new threshold template from scratch the operator should click the **Add new threshold group** button. A pop-up window will appear allowing the user to assign a name and value to the new threshold and define the alarm conditions. Another way of creating a user-defined threshold template is by highlighting one of the templates already defined and then click the **Duplicate selected** button.

Deleting a service threshold template is done by highlighting the template that should be removed and clicking **Delete selected**. Note that if the deleted threshold template was assigned to a stream being monitored, the new threshold template for that stream will default to the **Default** template.

The settings **Service checks** and **Content check** in the ETR threshold template controls whether or not to report alarms based on the service threshold template parameters. Please note that content check alarming (freeze-frame and color-freeze) are disabled in all default ETR threshold templates.





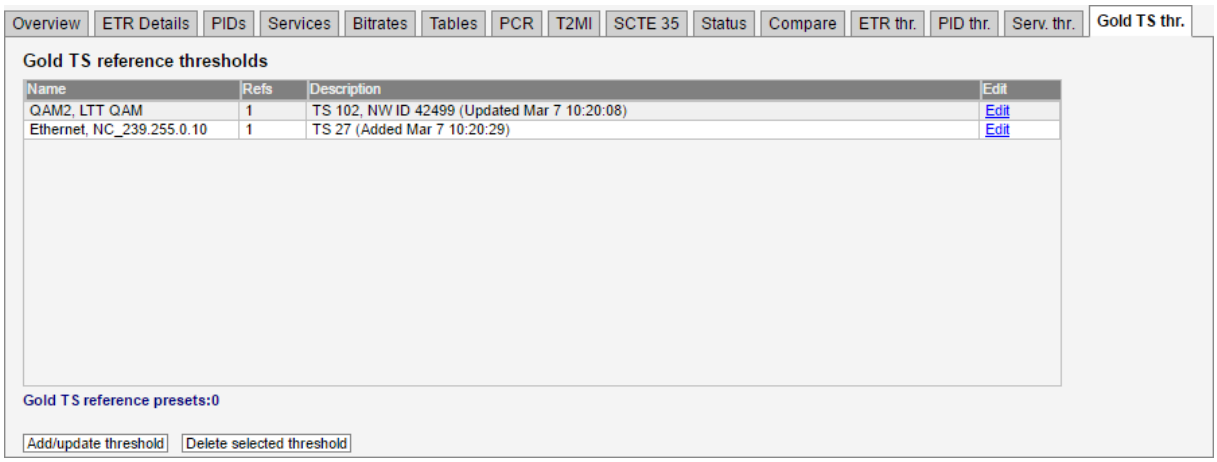
Edit Service Threshold	
Name:	A text string that identifies the service threshold group
Description:	Text field that should contain a meaningful description of the threshold

Service Threshold Parameters	
Selection:	The user selects if the requirements should apply for a specific service ID (as specified in the **ID** column), for all services of a specified type or for a service with a specified service name (as specified in the **Monitor name** column). Note that the service type detection depends on correct PSI/SI/PSIP signaling.
ID:	The service ID for which the associated thresholds should apply. For an SPTS the service ID will generally be 1; adding several list entries with different service IDs allows different thresholds to apply for different services within an MPTS. This value only applies if 'SID' is selected in the **Selection** column.
Monitor name:	A text string may be specified that should match the service name of the associated service ID, as analyzed from the received SDT. Note that the check is case sensitive. An alarm will be raised if there is not a perfect match.
Require presence:	If this field is checked an alarm will be raised provided that the specified service is not present in the stream. This check only requires that the service is present in the PAT, the other ETR checks will give alarms if there are other problems with the service, such as missing PMT or missing components. Note that this check is only available for specified services and not for service types.
Monitor min BW:	If enabled an alarm is raised provided that the minimum service bandwidth goes below the specified bandwidth (in kbit/s or Mbit/s).
Monitor max BW:	If enabled an alarm is raised provided that the maximum service bandwidth specified (in kbit/s or Mbit/s) is exceeded.
Report name:	It is possible to define the service name that should be used for alarm traps and for alarm reporting to the VBC Controller. This can be convenient to be able to track a service that changes name (as signaled in PSI/SI) in the signal chain, when services within an MPTS are unnamed (no service names in the SDT) or when services should be recognized by the VBC Controller under a different name than indicated in the SDT. Note that this functionality will only work for services specified by service ID or by name (specified in the Selection column).
Scrambling:	If a value different from 'Ignore' is selected an alarm will be raised if the service scrambling status differs from the requirement. A service is considered scrambled if one of its components is scrambled.
Service type:	If a value different from 'Ignore' is selected it should match the service type detected by analyzing the received SDT. An alarm will be raised if the service types differ.

Freeze-frame sensitivity:	(Content Extraction and Alarming Option) Picture matching in video streams is not an exact science, as noise can be introduced in many of the stages the stream goes through. This setting makes it possible to define how much noise is allowed when performing freeze-frame detection. When set to **Disabled**, the freeze-frame detection is disabled. When set to **Trigger seldom**, only a small amount of noise is allowed when deciding whether the picture has changed or not. This means that the pictures have to be close to identical before the freeze-frame alarm is raised. **Normal** is the recommended setting and should be used in most cases. **Trigger often** allows a high amount of noise. This means that it allows pictures to be quite different while still classifying them as identical, which may result in too many freeze-frame alarms.
Color-freeze sensitivity:	(Content Extraction and Alarming Option) This settings makes it possible to define how much noise is allowed when performing color-freeze detection. When set to **Disabled**, the color-freeze detection is disabled. When set to **Trigger seldom**, only a small amount of noise is allowed when comparing to the list of solid colors. **Normal** is the recommended setting, whereas **Trigger often** allows a high amount of noise, which may result in too many color-freeze alarms.
Ignore EIT:	Ignore missing EIT errors for this service. This is used for services which does not have EIT data. By ignoring EIT alarms on these services, false EIT alarms are avoided.
Schedule:	The Schedule drop-down menu allows the user to associate a scheduling scheme to a service, in effect masking alarms during selected intervals. Scheduling templates are defined in the **Setup — Scheduling** view. The predefined scheduling templates 'Never' and 'Always' will always be selectable, and these will result in service alarms never and always being masked, respectively. Note that if a PID is shared between several services and alarm masking is defined for one of the services, no alarms will be raised due to errors affecting this service.

Note that it is possible to create a service threshold template that allows probe alarming if a new service appears in a stream. This is done by creating a threshold template listing the service IDs that are allowed to be present in a stream, and associating it to the stream. A complementary ETR threshold template should be created, that has the 'Only allow services listed in service template' check enabled. This ETR threshold template should also be associated with the stream.

5.9.15 ETR 290 — Gold TS thresholds



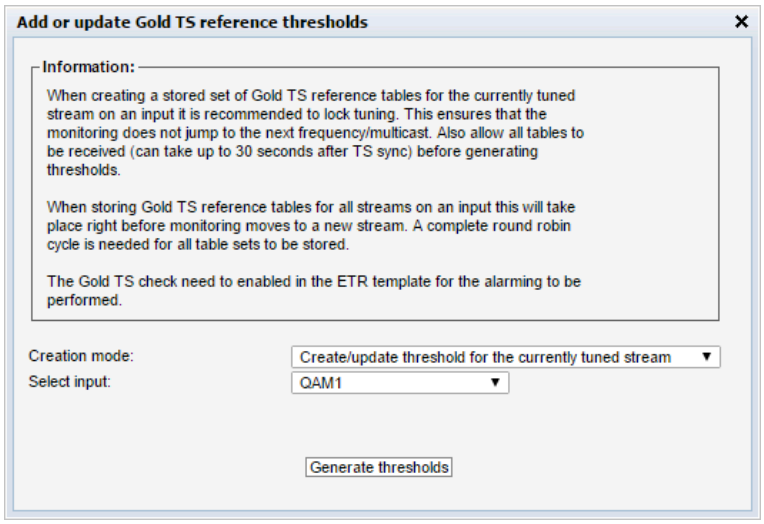
The Gold TS reference feature is used to compare the tables in the transport stream with a set of stored reference tables. This allows the operator to be notified of any changes in the PSI/SI tables such as:

- A service disappearing
- A new service being added
- Language descriptors suddenly changing
- Changes in service names
- Changes in frequencies used to transmit the signals
- And lots of misconfigurations in multiplexers

To use the Gold TS reference functionality, first store away tables for a stream or a set of streams. Go to **ETR 290 — Gold TS thr.**.

Here you can see the reference thresholds currently stored on the probe and they can be renamed or edited.

To add new reference thresholds or update the existing thresholds click on the button named **Add/update threshold**. The following dialog is then shown:



There are two different ways of creating a Gold TS reference template:

- Creating a template for the currently tuned stream on a specific input
- Creating a template for all streams on a specific input (or all inputs)

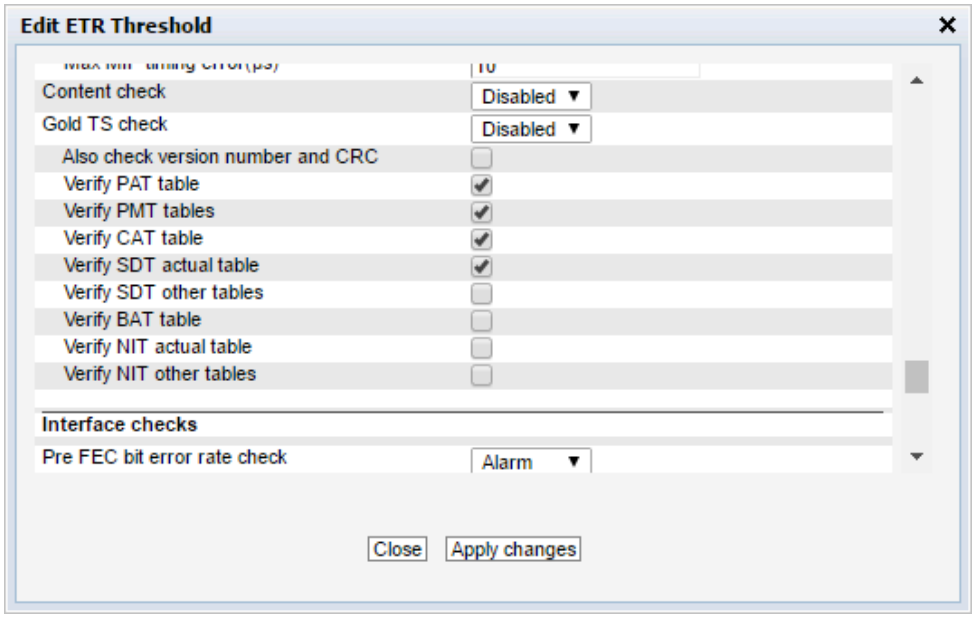
When creating a template for a specific stream the table set is saved immediately. It is therefore recommended that the ETR tuning is locked to this stream to avoid the round-robin operation from tuning to a new frequency just before the table set is stored. It can take 30 seconds after tuning to receive all tables.

When creating templates for all streams on an input this is done as a part of the round robin cycle at the end if the tuning period. It can then take a while for all thresholds to be generated (or updated) depending on the number of streams on that input.

When the reference template have been created it is automatically associated with the stream for which it was generated.

The operation of the Gold TS reference thresholds are controlled by the ETR threshold template associated with the stream. No settings are changed here when creating the reference templates so this needs to be done manually by going to **ETR 290 — ETR thr.**

If needed a new template can be created and associated with the stream(s). Or the existing template(s) can be changed.



The reference check needs to be set to alarm if the Gold TS reference checking are to be performed.

The settings are as follows:

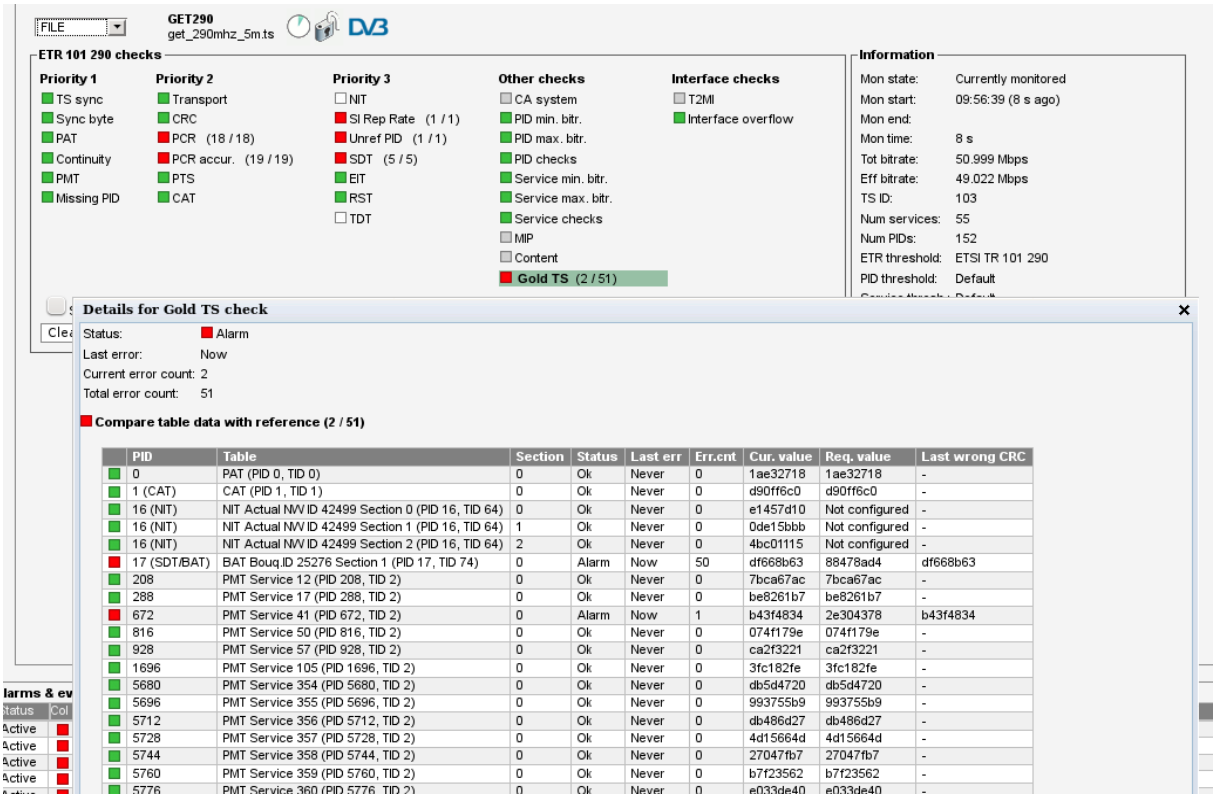
Also check version number and CRC	By default the version number and the original CRC of the tables are not checked. In many systems the version number can be updated even if no other changes are performed (for instance if a multiplexer is rebooted). So for most cases this should be left disabled.
Verify PAT table	When enabled the Program Allocation Table will be checked. This allows the operator to catch addition and removal of services as well as changes to the PMT PIDs used for the different services.



Verify PMT table	When enabled the Program Map Table will be checked. This allows the operator to catch lots of changes to the different services: • Addition or removal of the various components such as audio and video PIDs. • Changes in language descriptors • Changed PCR PIDs • Changed or removed ECM PID • Lots of changes in the descriptors can be detected
Verify CAT table	When enabled the Conditional Access Table will be checked. This allows the operator to catch errors related to the signaling for the CA Systems such as EMM PID disappearing or the CA System ID being changed
Verify SDT actual table	When enabled the SDT table for the current stream will be checked. This allows the operator to catch changes is service and operator names, service types and the various descriptors, both DVB defined and private descriptors
Verify SDT other tables	When enabled the SDT tables for the other streams will be checked. Checking is not enabled as default. This allows the operator to catch changes is service and operator names, service types and the various descriptors, both DVB defined and private descriptors
Verify BAT table	When enabled the Bouquet Association Table will be checked. The BAT table is not checked as default.
Verify NIT actual table	When enabled the Bouquet Association Table will be checked. The BAT table is not checked as default When enabled the Network Information Table for the current network will be checked. This allows the operator to catch changes such as: • Changes in frequency • Changes in modulation parameters • Network name • Changes in service lists per transport stream • Changes in private as well as MPEG/DVB defined descriptors

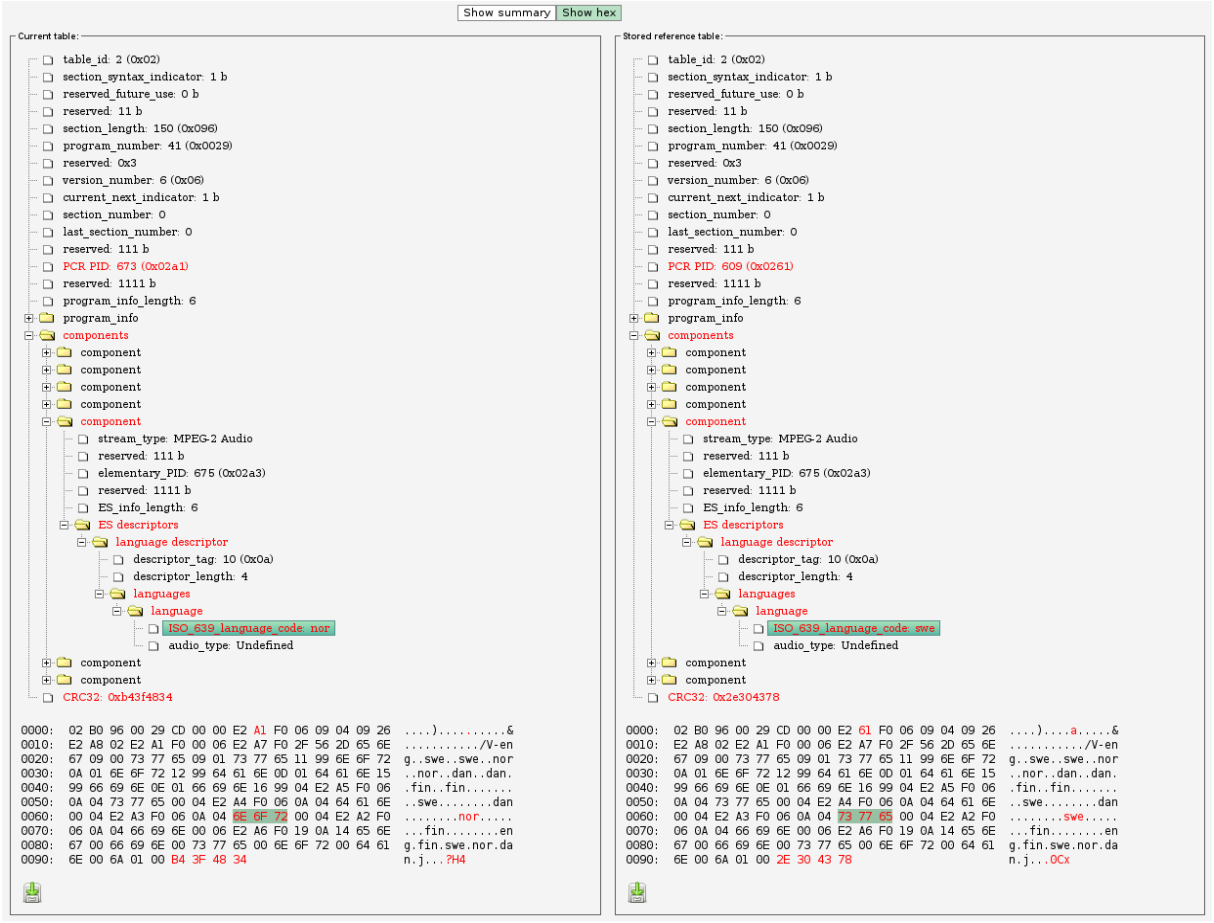
Verify NIT actual tables	When enabled the Network Information Tables for the other networks will be checked. This is disabled as default. This allows the operator to catch changes such as: • Changes in frequency • Changes in modulation parameters • Network name • Changes in service lists per transport stream • Changes in private as well as MPEG/DVB defined descriptors

The Gold TS reference checking is performed by the ETR engines and can be performed in round robin. To view the status go to the ETR Details page for the stream and click the Reference check:



All the different tables and sections monitored are listed here. If there have been any changes to the tables the check will turn red and alarms be sent.

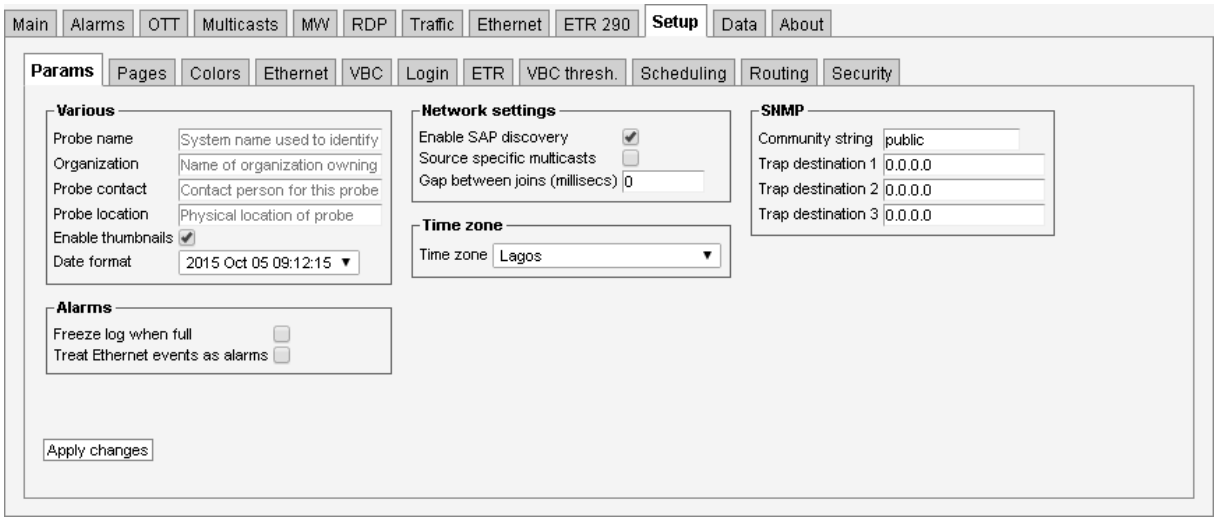
When the ETR engine is tuned to a stream it is possible to compare the tables for this stream with the stored reference tables by clicking on the entry in the list. This opens up a new window where the table data can be compared, both as a tree-breakdown and as a hexadecimal dump:



If the tables are inspected and the change found to be OK the operator can then go back to **ETR 290 — Gold TS thr.** and update the stored table set to the new version.

5.10 Setup

5.10.1 Setup — Params



The **Setup — Params** view is used to configure basic parameters for the 10G Software Probe. This page is displayed by default when accessing the web interface, until the configuration has been saved by clicking the **Apply changes** button.

Various	
Probe name:	Each probe can be assigned a user defined name. It is part of the probe's MIB. The name is shown in the **Main — Summary** view, which is the probe default page, as well as in the browser's title line. The name is also used for identifying the system when verifying the license on-line, see G Appendix: On-line License Verification for more details.
Organization:	The name of the organization (usually the company name) that is running the probe. This name is only used for identifying the system when verifying the license on-line.
Probe contact:	The probe contact is part of the probe's MIB, and this parameter is relevant for SNMP use only. It is used to identify the contact person responsible for this probe.
Probe location:	The probe location is part of the probe's MIB. It is used to identify the physical location of the probe. The probe location is also shown in the **Main — Summary** view and in the browser's title line. This name is also used for identifying the system when verifying the license on-line.
Enable thumbnails:	Enable or disable thumbnail generation globally. Thumbnails are only decoded automatically if the **Extract thumbnails** option has been enabled in the associated OTT or multicast setup, or if content check alarming (Content Extraction and Alarming option) has been enabled in the ETR threshold template. For high bitrates (above 700 Mbit/sec) the probe may feel more responsive if thumbnail picture generation is switched off. This does not affect the accuracy of the measurements.
Date format:	The date format used in the user interface can be changed here. Dates exported through machine-readable interfaces are not affected by this setting.

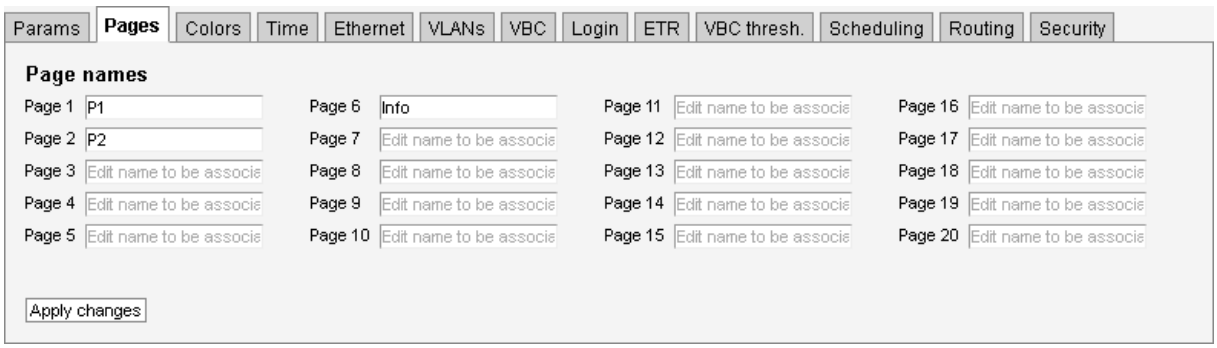
Alarms	
Freeze log when full:	When enabled the alarm list will freeze when full (an event will show that it is full). When the list is full new alarms are ignored until **Clear alarms** is pressed. This can sometimes be useful if a unit is placed unattended.
Treat Ethernet events as alarms:	When enabled each event is treated as an alarm that is active for 5 seconds. This may be useful when reporting to external systems that do not support events but only active or cleared alarms. This setting affects the local alarm list and SNMP traps.

Network settings	
Enable SAP discovery:	When enabled, the 10G Software Probe makes streams announced using the Session Announcement Protocol available through the **Multicasts — SAP** view.
Source specific multicasts:	Required for probe to support the IGMP v3 protocol.
Gap between joins (millisecs):	When monitoring a lot of multicasts, sending join requests for all of them at the same time may overload the network infrastructure. This setting specifies the minimum time, in milliseconds, between join requests.

Time zone	
Time zone:	By setting the time zone the 10G Software Probe time can be offset from the reference NTP time. Please note that this changes the global time zone on the system running the 10G Software Probe.

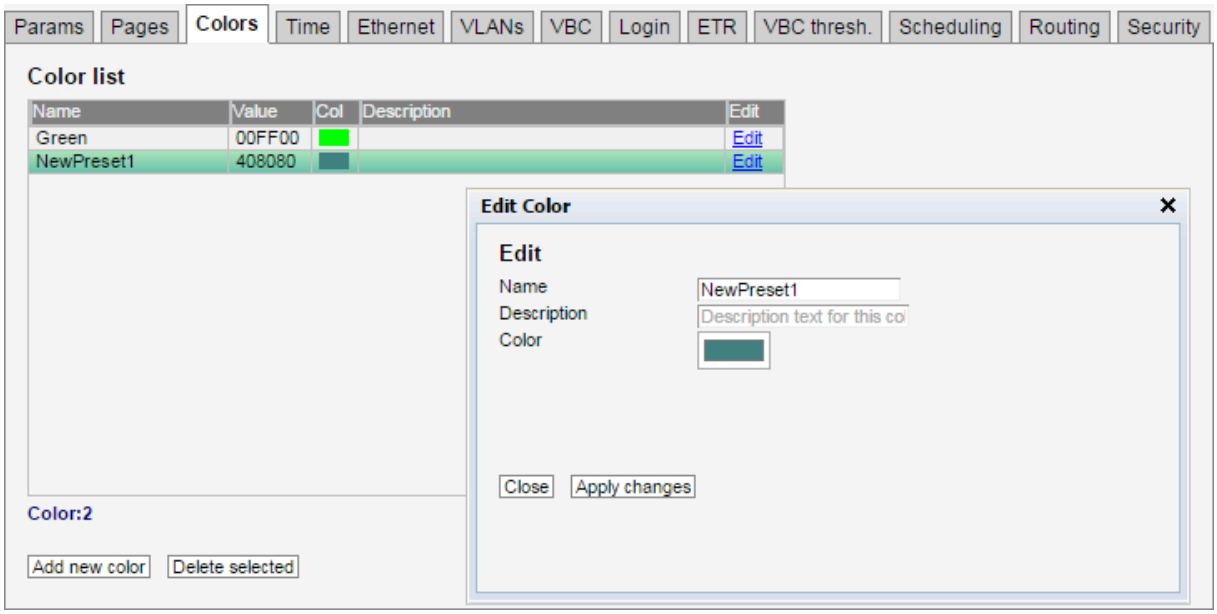
SNMP	
Community string:	The probe SNMP community string can be changed.
Trap destination 1–3:	SNMP traps will be sent to the specified destinations. Set to 0.0.0.0 to disable SNMP trap transmission.

5.10.2 Setup — Pages



The **Setup — Pages** view allows names to be associated with different pages. Individual multicasts can be assigned to different pages in the Multicasts — Streams view, to facilitate easier navigation in the different **Multicasts** views.

5.10.3 Setup — Colors (requires EXTRACT-OPT)

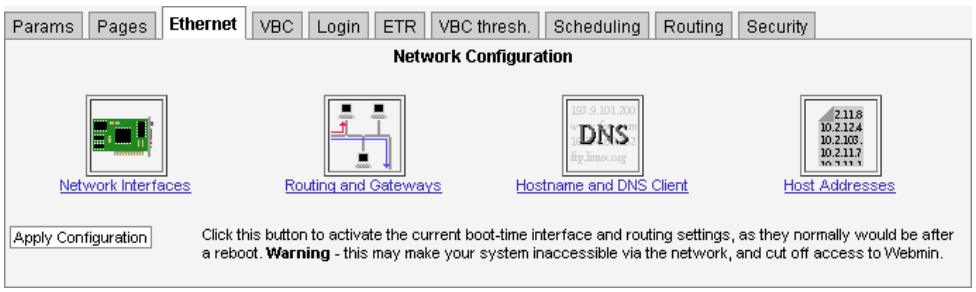


The **Setup — Colors** view allows the user to define colors that should be recognized if a color-freeze condition should occur. A mono-colored freeze frame condition may in some cases indicate what equipment is failing, resulting in the color-freeze.

A freeze color is defined by clicking the **Add new color** button and assigning an RGB value to a name. A maximum of four colors may be defined. An existing color may be modified by clicking the associated **Edit** link.

Edit color	
Name:	The color name. This name will be part of a color alarm description and the associated SNMP trap.
Description:	A description of the color or an error indication.
Color:	The RGB color on the format #XX(Red)XX(Green)XX(Blue) where XX represents a hexadecimal figure spanning 0-255 in decimal notation. If supported by the browser, clicking the color should pop up a color selection dialog.

5.10.4 Setup — Ethernet





The **Setup — Ethernet** view defines the Ethernet setup parameters for the network interfaces on the system hosting the 10G Software Probe.

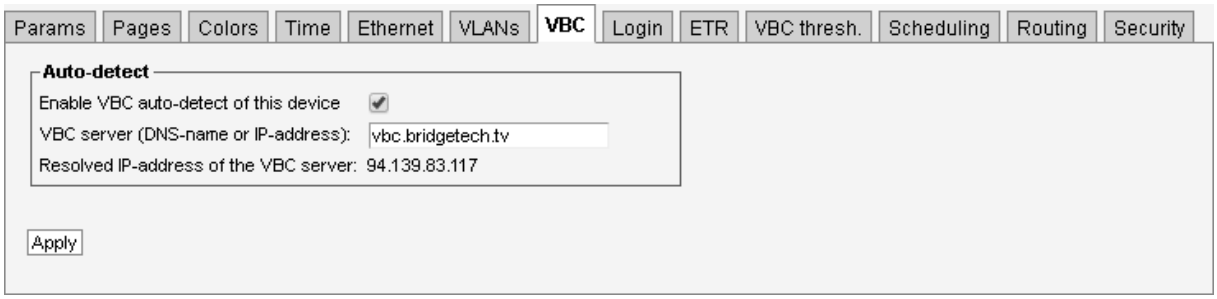
This page uses the same log-in credentials as the Software Activation interface. Please refer to chapter 3.4 for details on Software Activation.

The configuration is divided into different sections, click the appropriate icon to access the different parts.

The web-based network configuration tool is based on WebMin. Further documentation is available in the WebMin documentation[3].

If you make changes here that causes you to lose web access to the server, please see D Appendix: Network configuration for how to configure the network using the command-line tools.

5.10.5 Setup — VBC

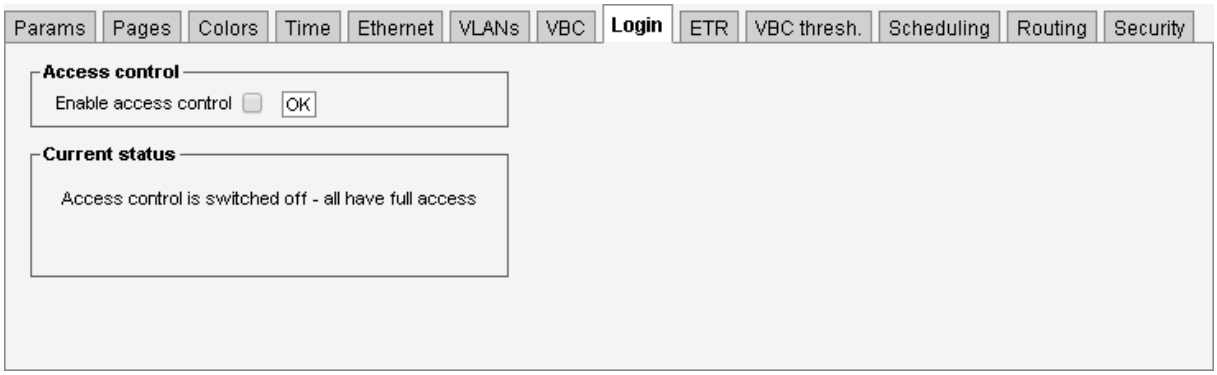


The VBC Controller can automatically detect the 10G Software Probe and add it to the VBC equipment list, provided that the auto-detect functionality is enabled and the VBC server address is known to the VB330-SW. Note that the network must be transparent to traffic between the VBC server and 10G Software Probes for auto-detection to work.

The VBC server's host name may be typed in the VBC server address field. The IP address associated with the DNS name will be displayed. If host name lookup fails, it is necessary to type the VBC server's IP address. Host name lookup is only performed if auto-detect is enabled.

When changes have been made in the **Setup — VBC** view, click the **Apply** button for changes to take effect.

5.10.6 Setup — Login



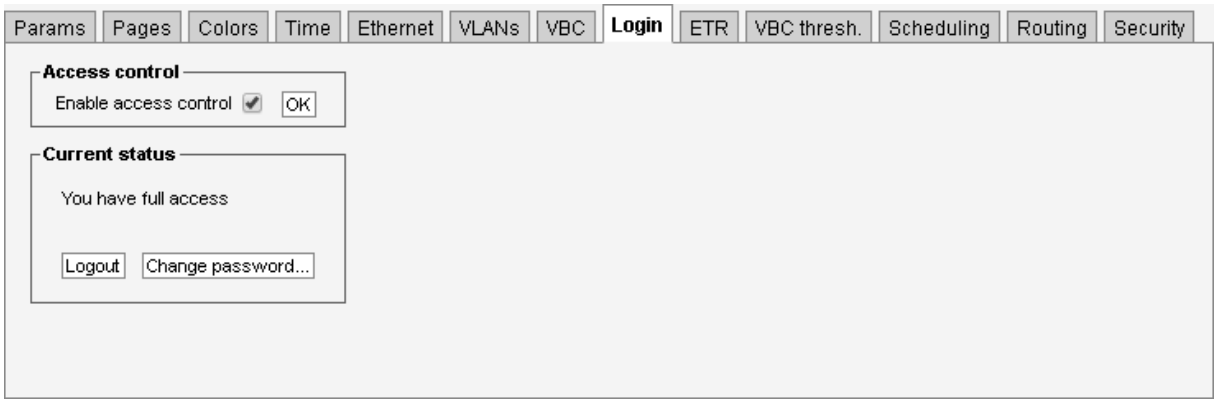
[3] https://doxfer.webmin.com/Webmin/Network_Configuration

By default, there is no access control and all users have access to all features. Access control can be enabled for the 10G Software Probe, restricting users to read-only access until they log in.

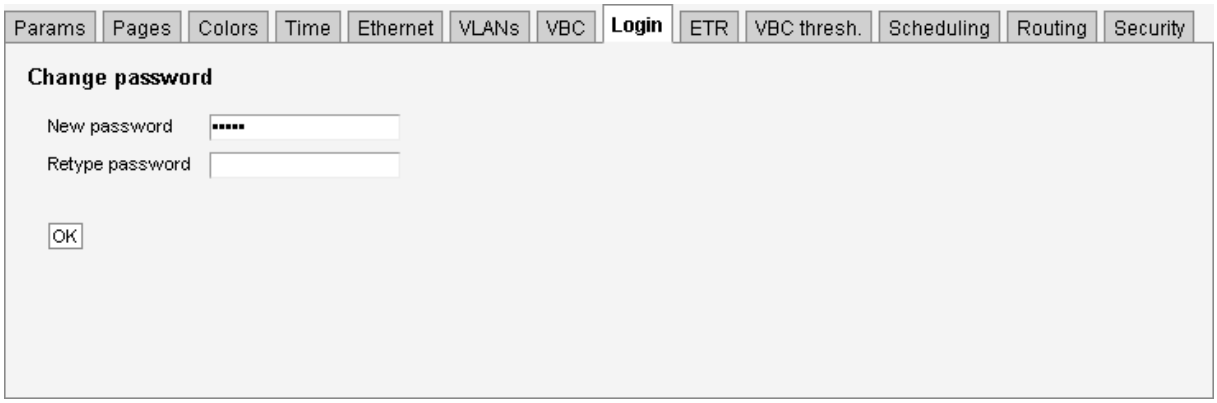
Any user can enable access control, but only users who are logged in can disable it or change the password.

The **Setup — Login** view is used to configure read-only access for the user interface. When access control is activated a **READ-ONLY access** message is displayed under the alarm list for users that are not logged in. It will be necessary to log-in each time a web browser application is launched and pointed at the VB330-SW.

When access control is activated, anyone with access to the VB330-SW can access the user interface in read-only mode. Use system firewall to whitelist or blacklist certain addresses, please refer to the Security Guide[4] for more details.



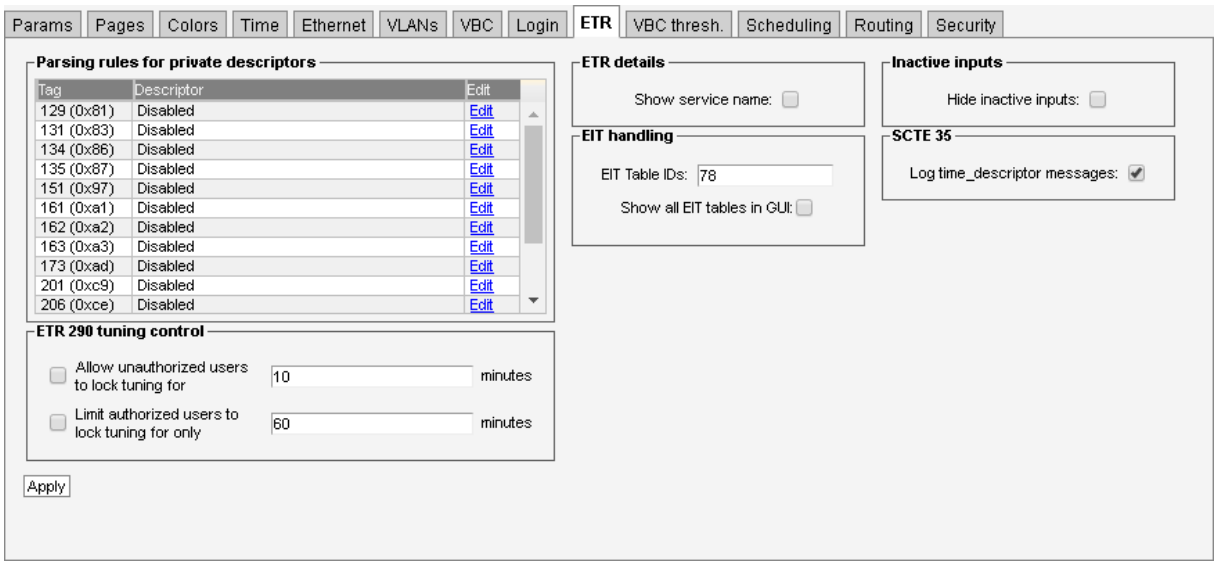
Log-in is performed by providing the correct password. The default password is **elvis**. The operator may define a new password that should be easy to remember.



Note that when logged in from the VBC, the VBC user's access rights apply.

The password defined here controls access to the VB330-SW user interface. To change the password for the Software Activation interface, please refer to chapter 3.4

[4] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-using_firewalls

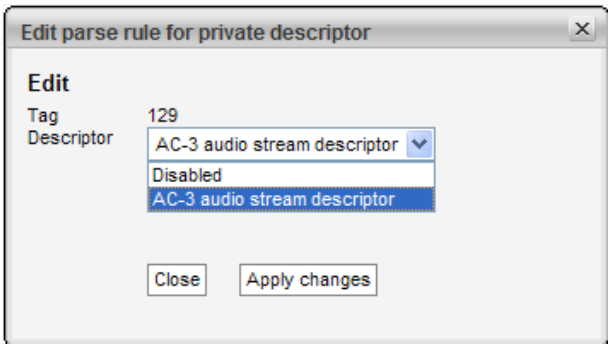


The **Setup — ETR** view allows the user to select miscellaneous ETR handling modes.

Parsing rules for private descriptors

Probe recognition of a number of selected private descriptors may be defined by the user:

129 (0x81):	'Disabled' or 'AC-3 audio stream descriptor'
131 (0x83):	'Disabled' or 'logical channel descriptor v1'
134 (0x86):	'Disabled' or 'caption service descriptor'
135 (0x87):	'Disabled', 'logical channel descriptor v2' or 'content advisory descriptor'
161 (0xa1):	'Disabled', 'service location descriptor' or 'etv_bif_platform_descriptor'
162 (0xa2):	'Disabled' or 'etv_integrated_signaling_descriptor'
231 (0xe7):	'Disabled' or 'private cable delivery system descriptor'
233 (0xe9):	'Disabled' or 'ip_delivery_system_descriptor'



The default value for private descriptors is 'Disabled'. To change this value, select a new descriptor interpretation from the drop-down menu and click the **Apply changes** button.

ETR 290 tuning control

By default authorized users will be allowed to lock the ETR 290 analysis to one stream for an infinite length of time and unauthorized users will not be allowed to lock the analysis. The **Setup — ETR** view makes it possible to time limit the locking for authorized users and unauthorized users can be granted permission to lock to a stream for a selectable time period.



If the locking mechanism works in a time limited mode a clock icon (see image above) is superimposed on the regular lock icon in the different **ETR 290** subviews. When the specified lock time is out the round-robin cycling will resume. When ETR tuning control parameters have been changed, click the **Apply** button for changes to take effect.

ETR details

The user selects if service names should be displayed in the **ETR 290 — ETR Details** view. Note that a large screen size is required for proper service name displaying.

EIT table IDs

The user defines which DVB EIT table IDs should be analyzed by the probe. By default only table ID 78 (EIT p/f actual) is analyzed.

It is possible to extend EIT analysis to include EIT schedule, however this is not recommended except for ad-hoc troubleshooting, as analysis of EIT schedule can be extremely demanding on probe processing resources. If full-time monitoring of all EIT information is required, dedicated probes should be used for this task.

Table IDs are specified as a comma separated list, or alternatively an ID range can be defined, e.g. 78, 80–95.

EIT table IDs:	
78	P/F for Actual TS
79	P/F for Other TS
80–95	Schedule for Actual TS
96–111	Schedule for Other TS

Inactive inputs

It is possible to hide disabled inputs from the **ETR 290** views. This is convenient when one ore more inputs are never used, and therefore have been disabled. Check the **Hide inactive inputs** checkbox to hide disabled inputs.

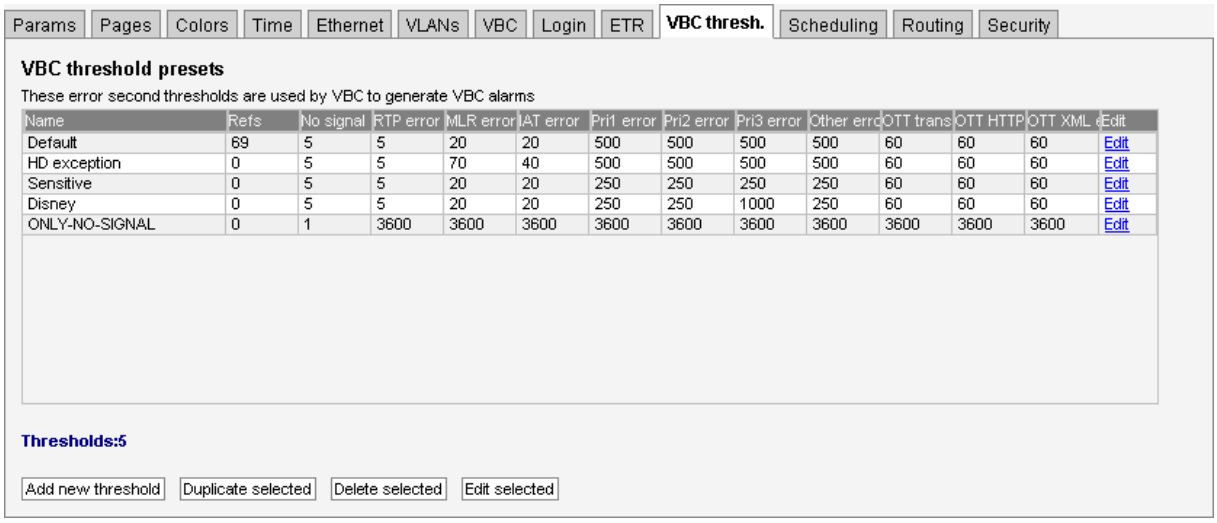
SCTE 35

The **Log time_descriptor messages** setting determines whether the SCTE35 messages containing nothing else than a time_descriptor should be included in the log of SCTE35 messages. In some systems there



are a lot of these messages (they can be used as keep alive messages to ensure that there always is some traffic on the SCTE35 PID). If the SCTE35 log is filled up with the time_descriptor messages disable logging of these messages.

5.10.8 Setup — VBC thresh.



The VBC error second thresholds are used by the VBC Controller to issue VBC specific alarms. The VBC will raise an alarm when the number of error seconds exceeds the error seconds threshold. The VBC thresholds are only relevant when a VBC Controller is part of the monitoring system.

The reason for using error second thresholds is to avoid alarms that toggle on and off, which for a large monitoring system might otherwise lead to an unintelligible user interface. The VBC thresholds will allow masking of minor error incidences thus resulting in a control system GUI that presents persistent alarms only.

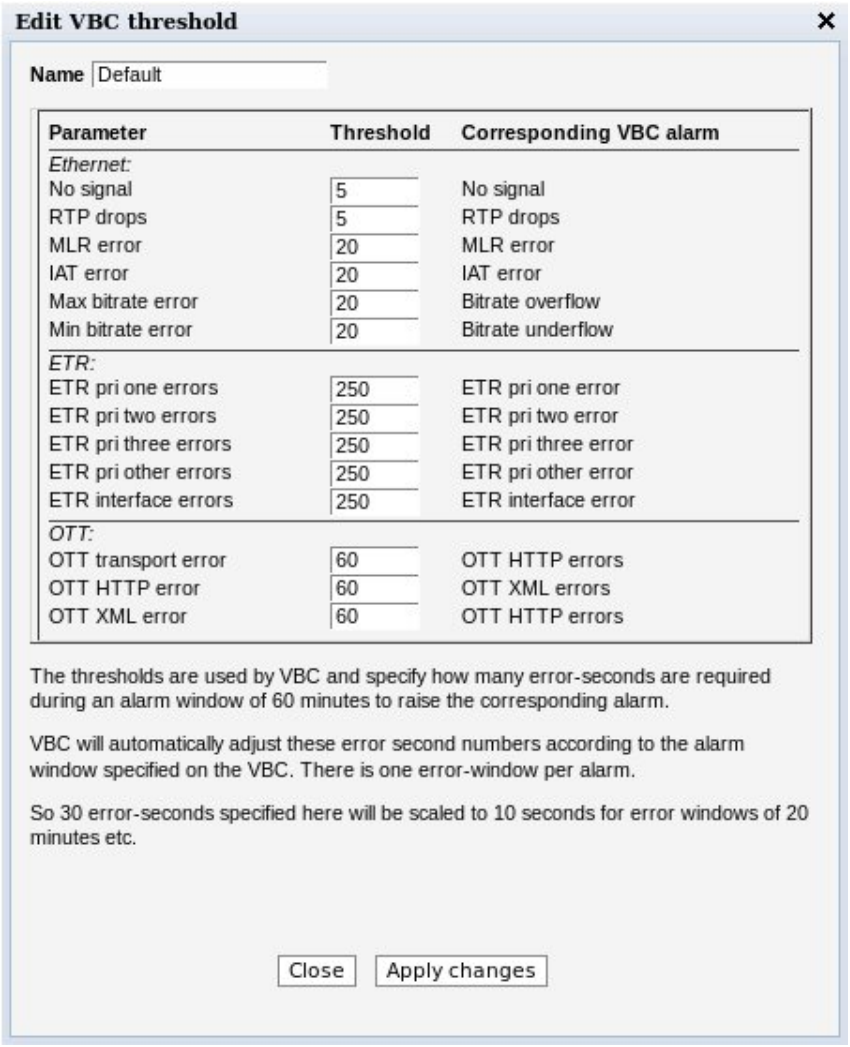
The VBC error second thresholds are specified as the number of seconds affected by an error situation. These thresholds refer to a monitoring window of one hour, meaning that if the number of error seconds summed over any one-hour period exceeds the associated error second threshold an alarm will be raised by the VBC.

If a monitoring window different from one hour is selected by the VBC user, the threshold values will be automatically recalculated to proportional values.

In the ‘VBC threshold presets’ table the ‘Refs’ column shows how many streams are associated with each VBC threshold template.

By clicking the **Add new threshold** button the user will enter a VBC thresholds edit view enabling definition of a new threshold template. It is possible to copy or delete an existing threshold template by clicking the **Duplicate selected** or **Delete selected** button respectively. To edit a highlighted threshold template, the **Edit selected** button should be clicked.

Multi-edit functionality allows editing several VBC thresholds simultaneously. Highlight the list entries that should be edited and click the **Edit selected** button.

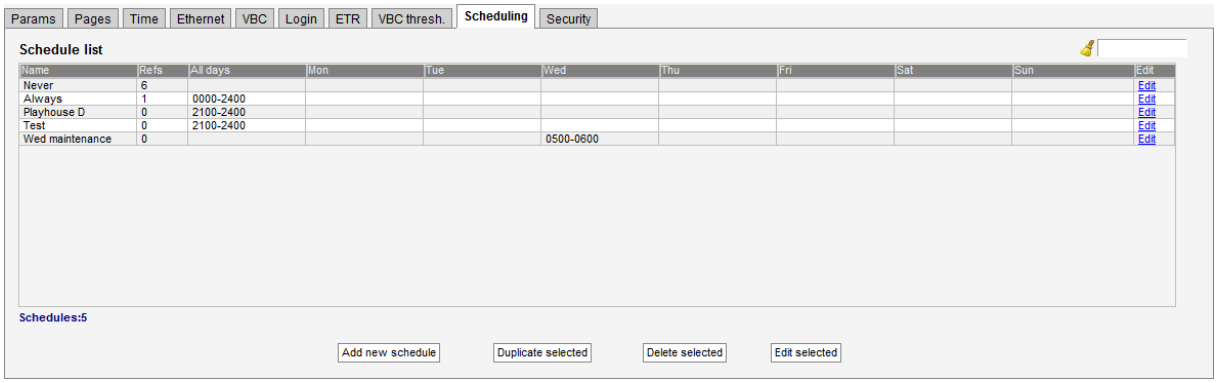


VBC thresholds	
Name:	The name of the VBC threshold template
No signal:	Number of seconds with ‘No signal’
RTP error:	Number of seconds with RTP packet drops. This measurement will be zero unless the stream is encapsulated in RTP headers
MLR error:	Number of seconds with packet drops in the TS layer (seconds when media loss rate is non-zero). This is equal to the number of error seconds with CC errors.
IAT error:	Number of seconds when the inter-packet arrival time exceeds the threshold
Max bitrate error:	Number of seconds the bitrate can exceed the error-threshold before a VBC alarm is generated
Min bitrate error:	Number of seconds the bitrate can fall below the error-threshold before a VBC alarm is generated
ETR Pri 1 errors:	Number of seconds with ETSI TR 101 290 Priority 1 alarms before a VBC alarm is generated
ETR Pri 2 errors:	Number of seconds with ETSI TR 101 290 Priority 2 alarms before a VBC alarm is generated



ETR Pri 3 errors:	Number of seconds with ETSI TR 101 290 Priority 3 alarms before a VBC alarm is generated
ETR other errors:	Number of seconds with ETR ‘other’ alarms before a VBC alarm is generated
ETR interface errors:	ETR error seconds are not relevant for the VB330-SW 10G Software Probe
OTT transport errors:	Number of seconds with OTT transport related alarms
OTT HTTP errors:	Number of seconds with OTT HTTP related alarms
OTT XML errors:	Number of seconds with OTT XML related alarms

5.10.9 Setup — Scheduling



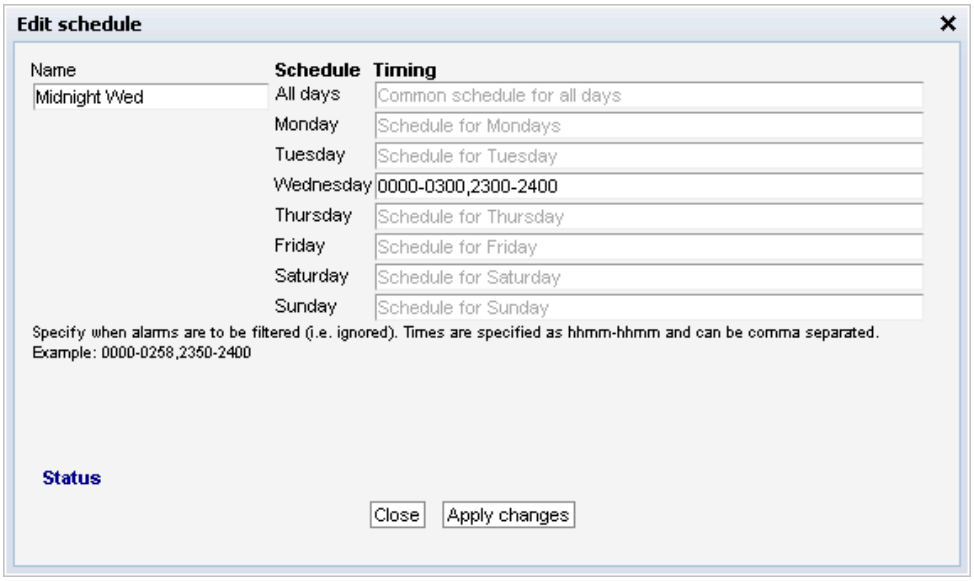
The **Setup — Scheduling** view enables definition of scheduling templates which are associated with PIDs or services using the PID threshold or service threshold template system. This way it is possible to mask alarms during selected time intervals, e.g. due to maintenance.

In the Schedule list table the ‘Refs’ column shows how many references exist for each scheduling template. References to scheduling templates may be found in PID and service threshold templates.

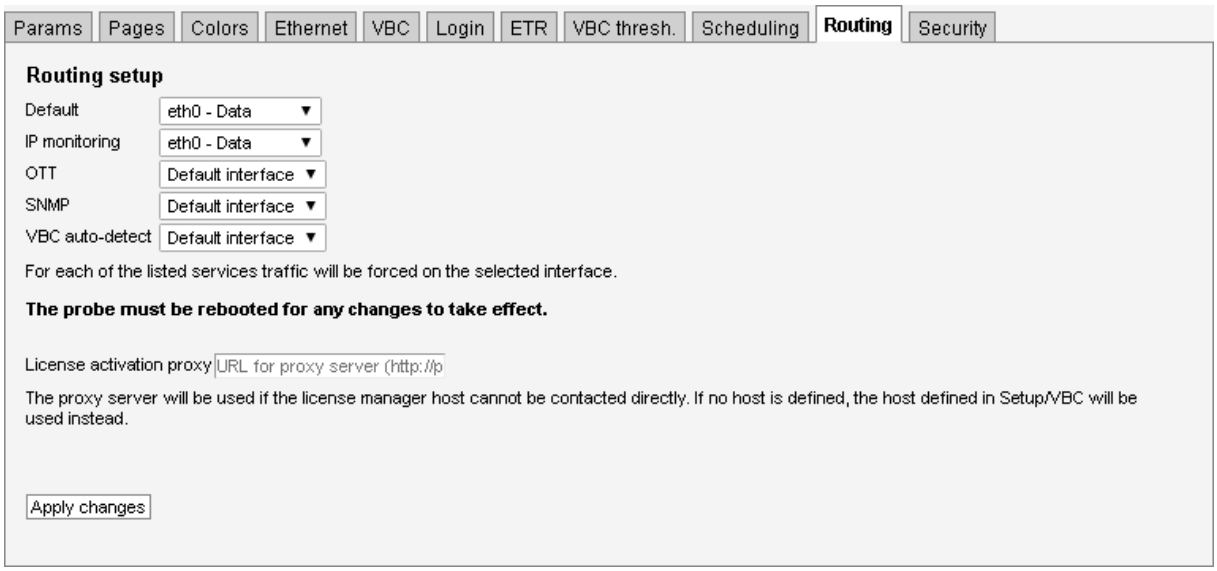
The search field in the upper right corner of the view allows the user to type a text string and the schedule list is updated to display only scheduling templates matching the specified text.

The predefined scheduling templates **Never** and **Always** result in alarms being masked never or always, respectively. A new scheduling template is created by clicking the **Add new schedule** button. It is also possible to copy an existing scheduling template by highlighting a schedule template and clicking the **Duplicate selected** button. The alarm masking intervals are defined for individual week days or for all week days. Intervals are specified on the form hhmm–hhmm, for instance the interval 1200–1400 means that alarm masking should start at noon and finish at 2 pm. Several alarm masking intervals may be specified for each day using comma separation. To edit an existing scheduling template, highlight it and click the **Edit selected** button. To delete a template, highlight it and click the **Delete selected** button.

When a scheduling template has been modified, click the **Apply changes** button. Defined scheduling templates become available as selections in the **ETR 290 — PID thresh. — Edit** and **ETR 290 — Service thresh. — Edit** views.



5.10.10 Setup — Routing



The **Setup — Routing** view allows users to override the default interface for out-going probe traffic.

To override the default interface for one or more types of traffic select the interface from the drop-down menu and click the **Apply changes** button.

Note: When monitoring both multicast (UDP) and OTT (TCP) traffic, we recommend using different network interfaces. Mixing the two traffic types on the same network can have unwanted impact on the monitored signals.

Routing setup	
Default	This setting determines the default interface.
IP monitoring	Defines the interface to use for the multicasts specified in the **Multicasts — Streams** view. The available interfaces depend on the probe license.
OTT	Interface to use for OTT channels specified in the **OTT — Channels** view.



SNMP	Interface to use for SNMP traps.
VBC auto-detect	Interface to use for VBC auto-detect, as specified in the **Setup — VBC** view.
License activation proxy	When using on-line activation, the 10G Software Probe needs to be able to connect to the license activation server. If the 10G Software Probe is not connected directly to the Internet, you can add the URL to a proxy server that it can use here. If not configured, the 10G Software Probe will try to use the proxy installed on the VBC host, as configured in the **Setup — VBC** view; see G Appendix: On-line License Verification for more details

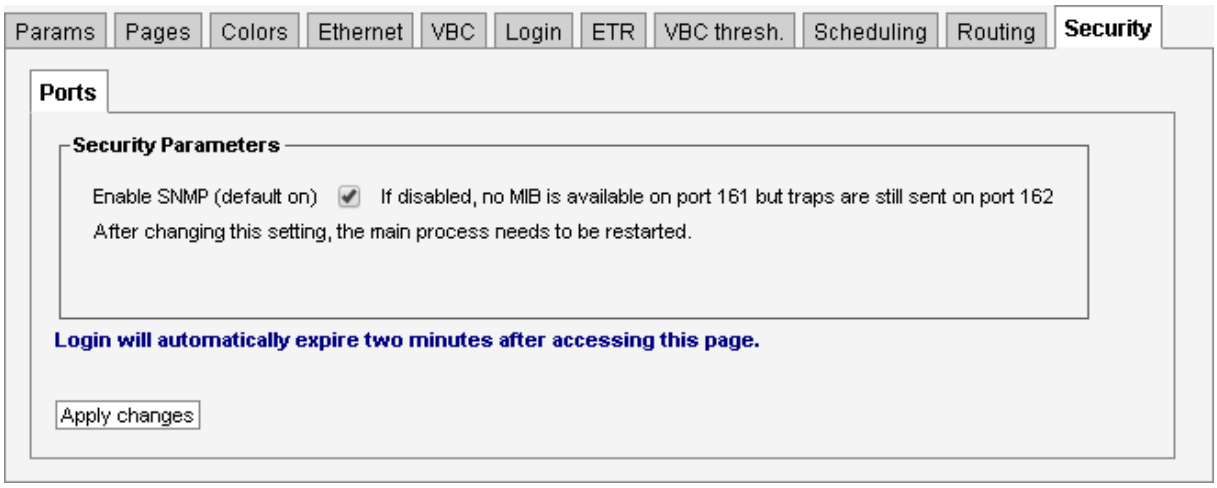
Note that routing for Full Service Monitoring (FSM) is selected in the **Ethernet — FSM — Setup — Edit** view.

5.10.11 Setup — Security

The **Setup — Security** view is a restricted section where only the administrator should have access, making it possible to disable selected communication protocols to increase safety against unauthorized access to the 10G Software Probe.

This page uses the same log-in credentials as the Software Activation interface. Please refer to chapter 3.4 for details on Software Activation.

5.10.11.1 Setup — Security — Ports



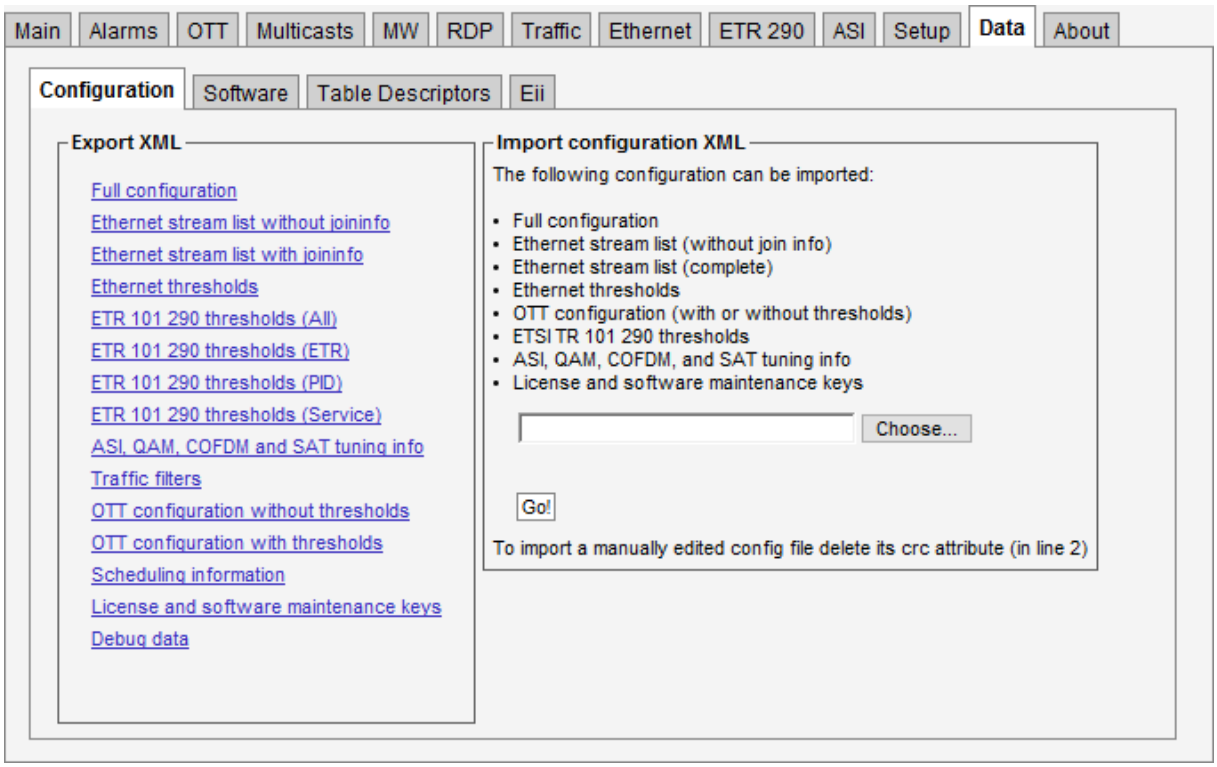
To disable a protocol deselect it by removing the associated check-mark and click the **Apply changes** button. Available security parameters are:

Security parameters	
Enable SNMP:	If SNMP is disabled, no MIB is available on port 161. However SNMP traps are sent as usual on port 162. Defaults to **on**.

By default, all web communication to and from the host running the 10G Software Probe is using unencrypted HTTP communication. Please refer to E Appendix: Enabling HTTPS for information on how to enable HTTPS.

5.11 Data

5.11.1 Data — Configuration



Full and partial configuration of the 10G Software Probe can be exported as XML documents. This is achieved by clicking one of the links inside the **Export XML** frame. A new browser window pops up containing the selected XML document. The browser will allow the contents of the page to be saved to file.

Restoring the 10G Software Probe configuration, multicast stream list or OTT channel list is just as simple. Just click the **Browse** button and select the file that contains the XML document. Then click the **Go!** button and the information in the XML document will be applied. The configuration, stream list and thresholds exports can all be imported.

Configuration files generated by a probe can be imported by the VB330-SW. Multicast stream lists, OTT channel lists and scheduling information can also be exported to and imported from the VB288 Objective QoE Content Extractor.

You can also import and export license and software maintenance keys in XML format from this page.

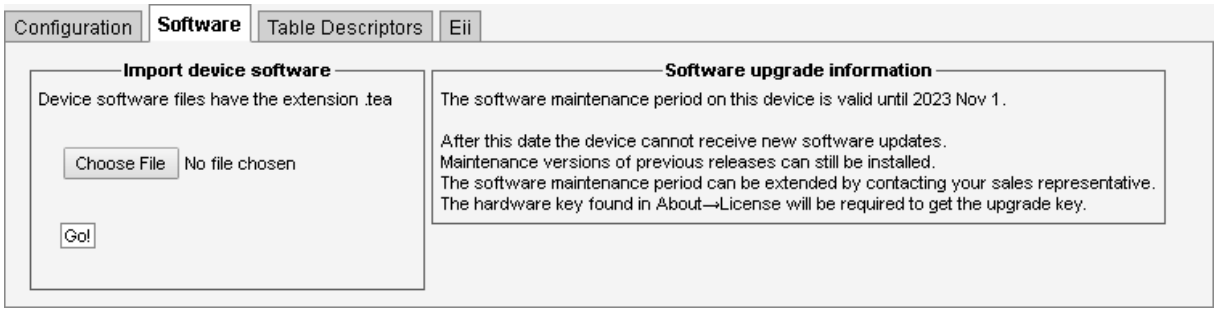
To import documents that have been manually edited the CRC attribute at the very top of the document must be deleted (i.e. delete `crc="..."` from the file). This will bypass the checksum verification mechanism.

Please refer to the document **Eii External Integration Interface** for detailed information about XML import and export.

Note that the probe name and location are not part of the XML document. Hence exporting the full configuration of one 10G Software Probe and restoring it on another will make the two 10G Software Probes identical except for the network settings.

Clicking the Debug data export option will generate a document containing debug information that may be useful if 10G Software Probe misbehavior is reported. This file should be sent along with a description of the misbehavior.

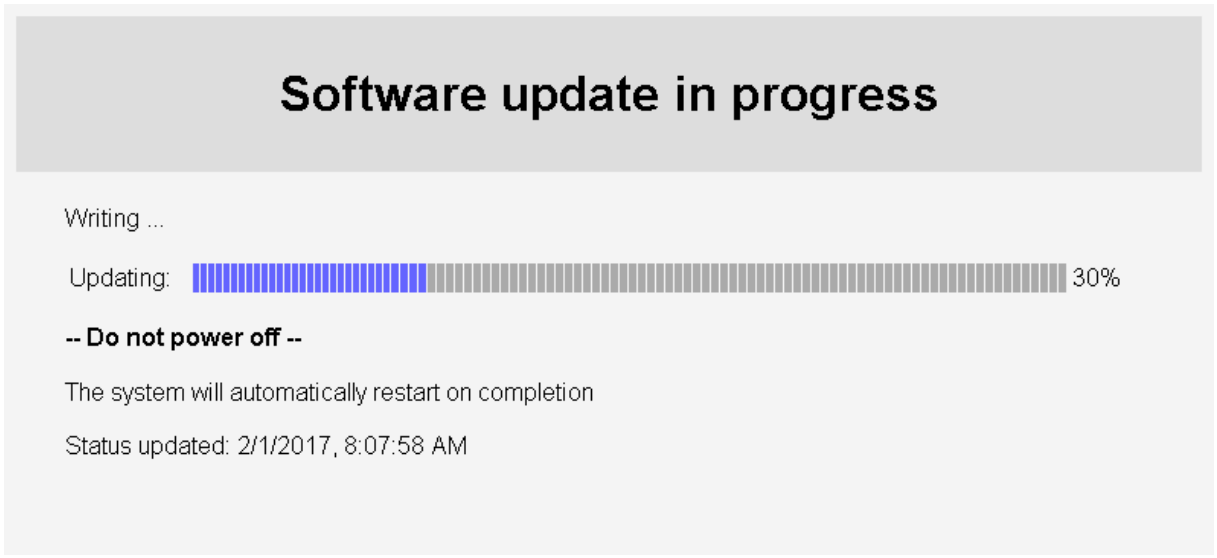
5.11.2 Data — Software



The software section allows the 10G Software Probe to be upgraded to a newer software version. Select the **.tea** file from the local PC and click **Go!** to copy the software to the VB330-SW. When the upload is complete, clicking the **Update software** button will begin the upgrade procedure. The latest version of the VB330-SW software can found the End User area at `https://www.bridgetech.tv/`.

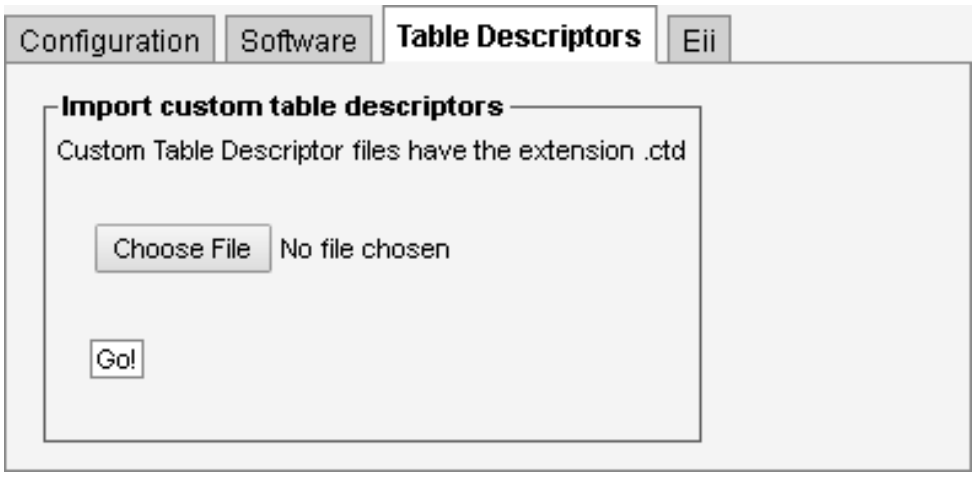
A more detailed description on the software update procedure can be found in I Appendix: Software Upload





Upgrading to a new major release requires a valid software maintenance license, please refer to H Appendix: Software Maintenance for more details. If the current software maintenance license does not cover the uploaded software version, the upgrade will be aborted and the current version is kept.

5.11.3 Data — Table Descriptors



It is possible to upload parser files to the probe adding support for private descriptors. Private descriptors should be enabled (in the **Setup — ETR** view).

Contact your Bridge Technologies reseller for more information about private descriptors.

5.11.4 Data — Eii

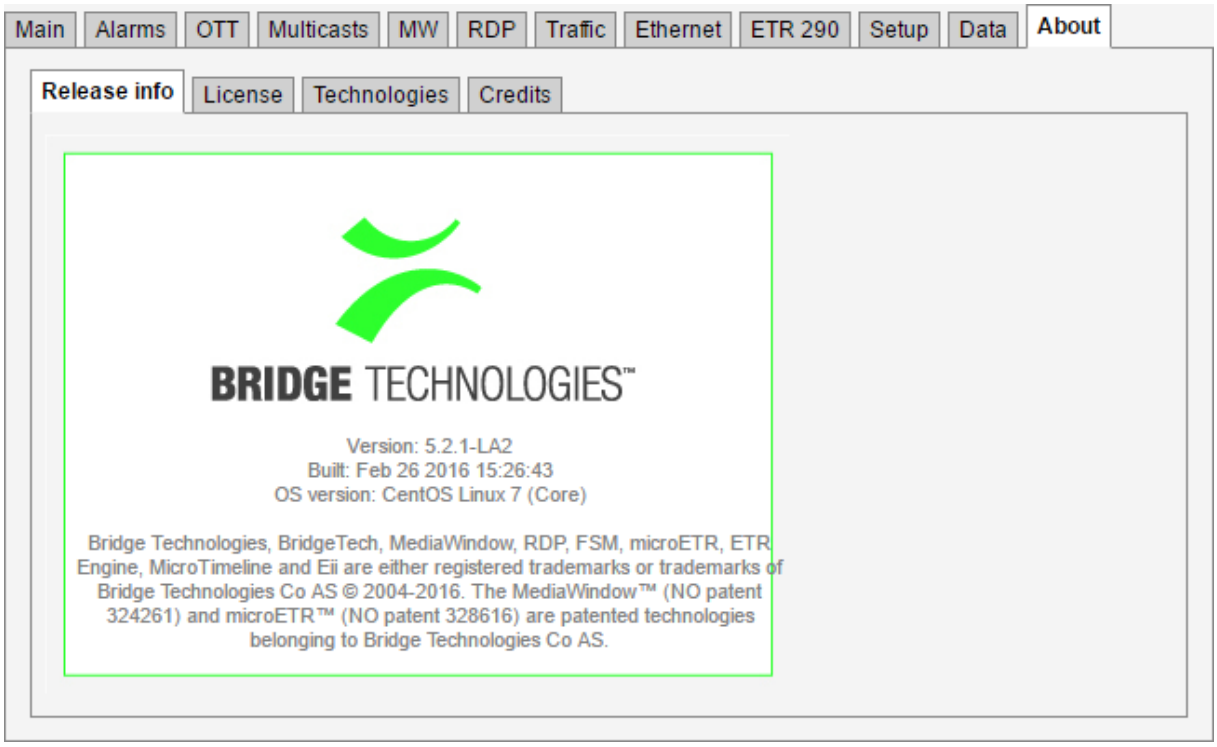


The **External integration interface** (Eii) allows inclusion of Bridge Technologies equipment into 3rd party NMS systems. In order to facilitate integration the **Data — Eii** view allows export of XML files containing the data typically being requested by an NMS system via the regular Eii interface.

Please refer to the document **Eii External Integration Interface** for detailed information about Eii.

5.12 About

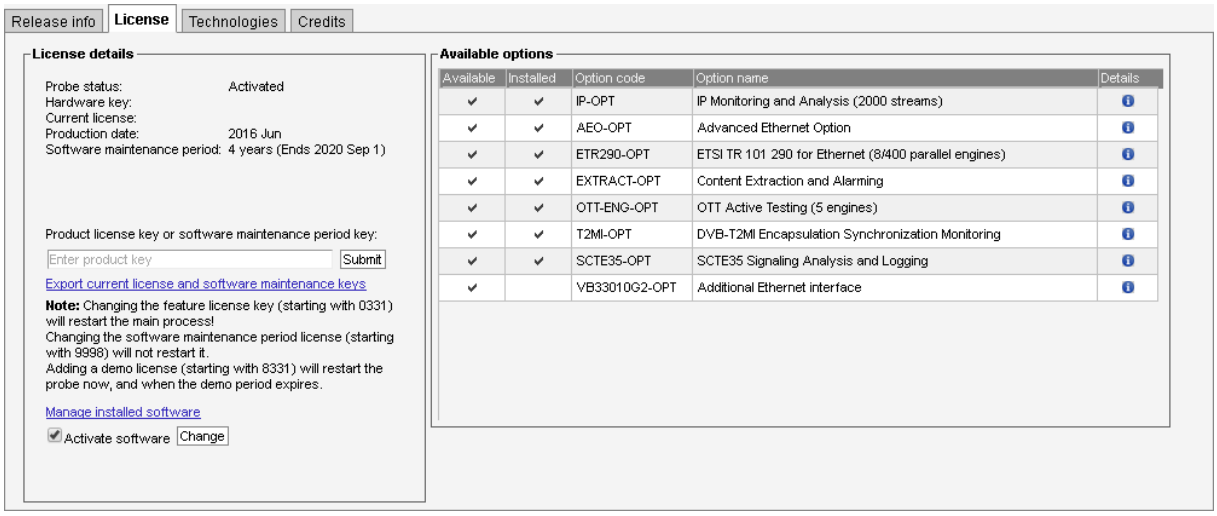
5.12.1 About — Release info



This view shows the software version, the software build date and the version of the underlying operating system for the 10G Software Probe.

In addition, if the system has been able to contact the license verification server, it will also display information on whether there is a newer version available for download, together with some information about this version. For more information on on-line license verification, see G Appendix: On-line License Verification.

5.12.2 About — License





The **License** view displays the currently active license. The license includes the available 10G Software Probe options and software maintenance details. By clicking the blue information icon associated with each option it is possible to view option details.

The 10G Software Probe supports two different licensing schemes, on-line licenses and classic licenses. When using a classic license, product and software maintenance license keys are tied to the hardware key, which is the shorter of the two keys presented, in a non-transferrable manner. The license is installed once, and can also be exported in XML format from this page. These keys can be imported using the **Data — Configuration** view, or from Software Activation.

When using an on-line license, the key is verified periodically towards a license server. The key is transferrable between systems running the same software, but only as long as on-line verification is supported. The longer system identifier is used to identify the system. The **Current license** field will display information on when the license key was last verified. Click the **Renew** button to immediately renew the license with the license server.

Click the **Release** button to remove the current license, making it available to another host. Please make sure you have the license key available before you do this, as you must enter it again on the system you wish to transfer the license to. If you have lost the license key, contact your dealer to retrieve it. Make sure you include all details from this page in your request.

Please refer to G Appendix: On-line License Verification for more information on how to use on-line licenses. This appendix also describes how to renew the license when the 10G Software Probe cannot connect to the Internet.

Please refer to H Appendix: Software Maintenance for more details on software maintenance licenses.

Click the **Manage installed software** link to access the Software Activation interface, see chapter 3.4 for more information.

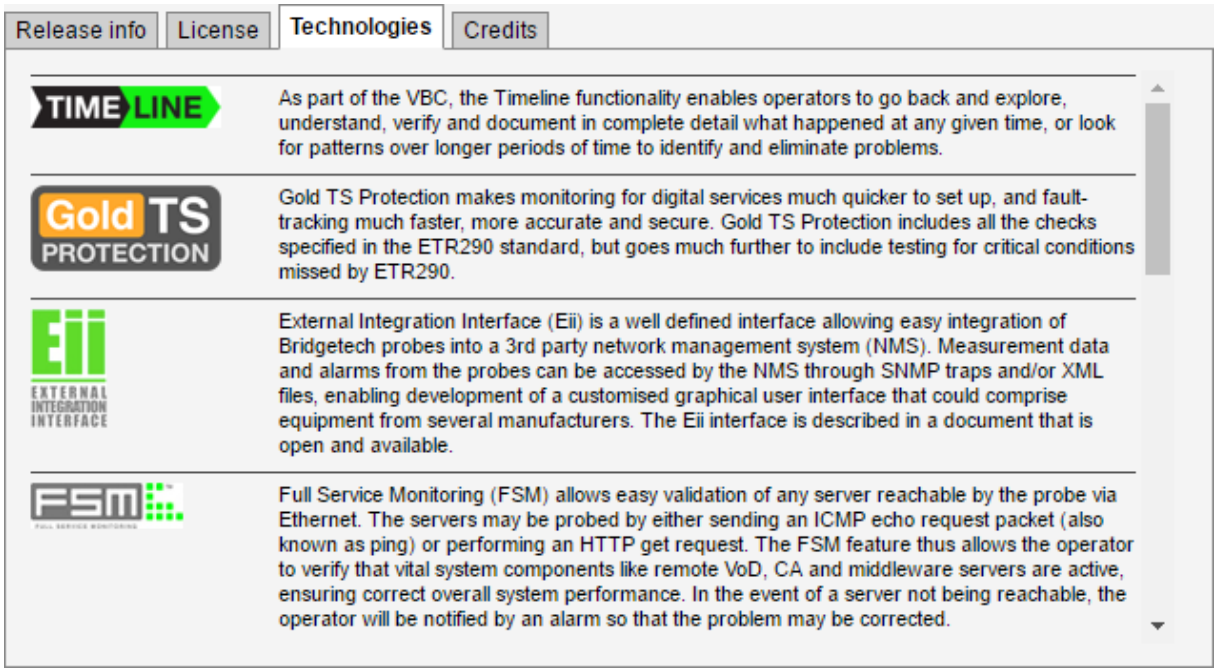
To disable the 10G Software Probe, uncheck the **Activate software** checkbox and click the **Change** button. You cannot do this if it has been set as the default software through the Software Activation interface (which is done by default the first time you activate the software), you will need to change the default back to **Software Activation** before disabling 10G Software Probe. See chapter 3.10 for more details.

Demo license

Entering a demo license key pair will start a trial period during which the features defined in the demo license are available. Once the trial period ends, the VB330-SW will revert back to the previous license. The time remaining is indicated in the **License details** page.

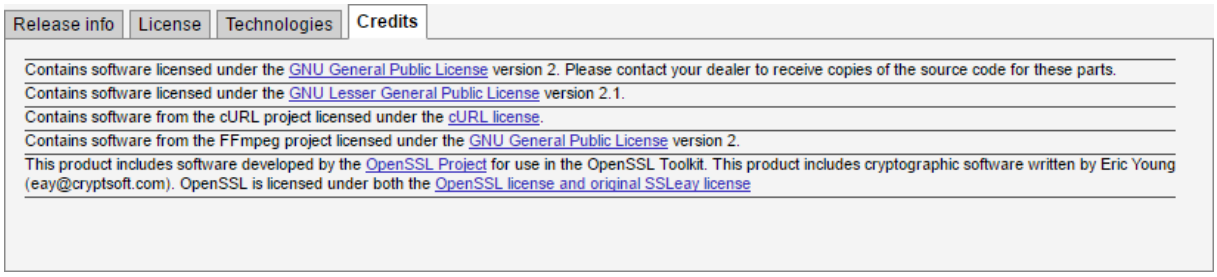
To end a trial period manually, enter a valid permanent license key.

5.12.3 About — Technologies



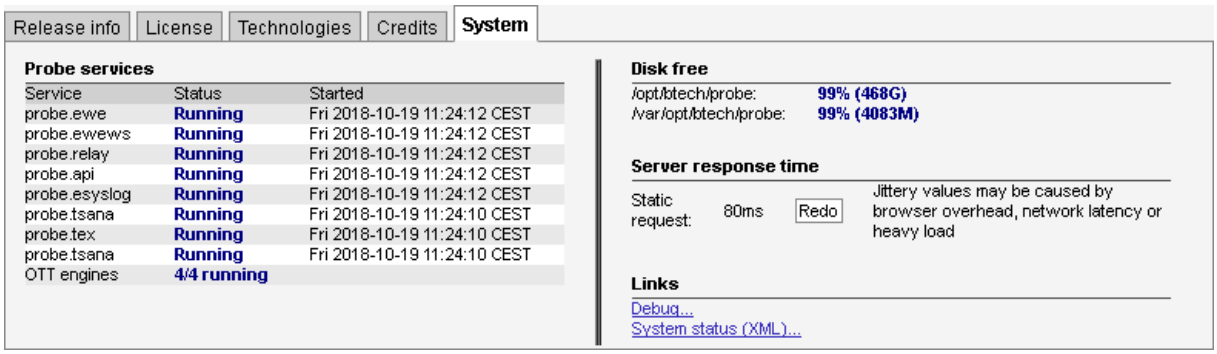
The **Technologies** view lists some of the technologies available in the Bridge Technologies product family.

5.12.4 About — Credits



This view shows information about the software included with the 10G Software Probe.

5.12.5 About — System



The **System** view displays a snapshot of the current status of the system, to ensure correct 10G Software Probe operation.



The **Probe services** overview displays the VB330-SW services that are required. All the VB330-SW services listed should have status *Running*.

Disk free displays free disk space to give the user some overview of disk resources available.

Server response time is determined upon entering the **System** view. When the **Redo** button is clicked, a new request is sent to the web server.

Clicking the **Debug...** link allows the user to generate a document containing debug information that may be useful if VB330-SW misbehavior is reported. This file should be sent along with a description of the misbehavior.

Clicking the **System status (XML)...** link generates an XML document with a short description of the system status.

A Appendix: VB330-SW Versus VBC Alarms

The VB330-SW 10G Software Probe alarms are independent of the VBC Controller alarms. The 10G Software Probe has been designed to yield instantaneous alarms based on the current measurements. This typically results in lots of short-lived alarms that would be “too much” for the VBC to report, as the VBC may control a large number of 10G Software Probes. The VBC therefore generates alarms based on error-second statistics gathered from 10G Software Probes during a selectable time period (default 60 minutes – sliding window).

Some the VBC alarms map to only one probe alarm type. Other the VBC alarms map to several probe or VB288 Objective QoE Content Extractor alarms. As an example, the VBC alarm ETR pri one error does alarming for the following probe alarms:

- TS sync
- Sync byte
- PAT
- Continuity
- PMT
- Missing PID

The VBC GUI has functionality for searching for all 10G Software Probe alarms that have corresponding VBC alarms. This makes it easier to find the cause of an VBC alarm.

Ethernet measurement data are sent from the VB330-SW 10G Software Probe together with Ethernet error-second threshold values (as set in the VB330-SW 10G Software Probe **Setup — VBC thresh.** view). The VBC monitors the error seconds for each parameter and will raise an alarm provided that the error-seconds figure exceeds the threshold value, as monitored during the windowing period.

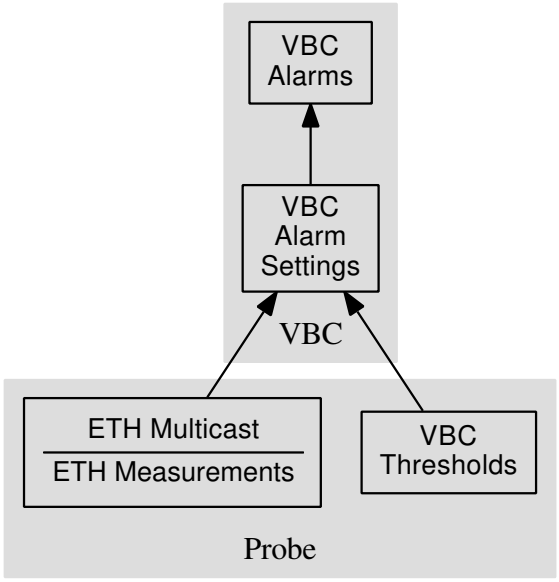


Figure A.1: VBC alarming based on 10G Software Probe measurements

B Appendix: Monitoring Practices

This Appendix summarizes a few useful monitoring practices.

B.1 RTP Monitoring

When running video inside an RTP wrapper it is possible to exactly deduce the number of dropped IP frames due to network issues. This is possible as a result of the 16-bit sequence counter inside the RTP header. When the protocol mapping is nTS/RTP the RTP parameters **RTPdrop**, **RTPdup**, **RTPooo** and **RTPlag** will be updated and the corresponding alarms **Packet drops:N**, **Duplicate packets:N** and **Out of order packets(lag:N)** are fired (if not switched off).

Note that the probe will perform out-of-order corrections before RTP packet loss analysis is performed.

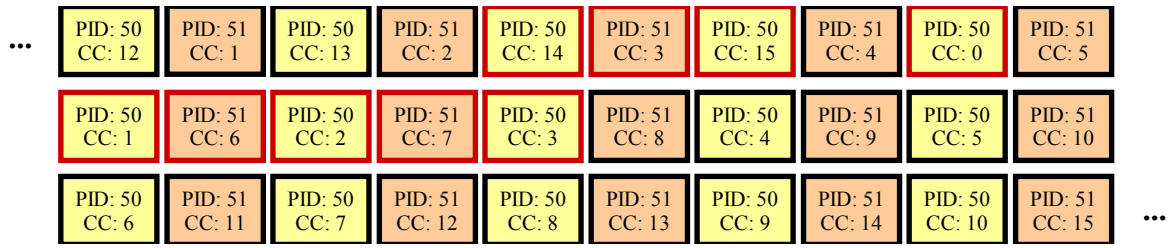
Example of RTP sequences and their effects on monitoring:

Sequence	Effect
..., 10, 11, 12, 13, 14, 17, 18, 19, ... 2 dropped packets (15-16)	Monitoring page: **RTPdrop:+2** Alarms & events: **RTP Packet drop: 2**
..., 10, 12, 13, 16, 17, 18, 19, ... 1 and 2 dropped packets (11, 14-15)	Monitoring page: **RTPdrop:+3** Alarms & events: **RTP Packet drop: 3**
..., 10, 11, 15, 12, 14, 16, 18, 19, ... 2 dropped packets (13, 17) 1 out of order packets of order 3 (15 → 12)	Monitoring page: **RTPdrop:+2** Monitoring page: **RTPooo:+1** Monitoring page: **RTPlag: 3** (at least) Alarms & events: **RTP Packet drops: 2** Alarms & events: **RTP out of order packets (lag:3)**

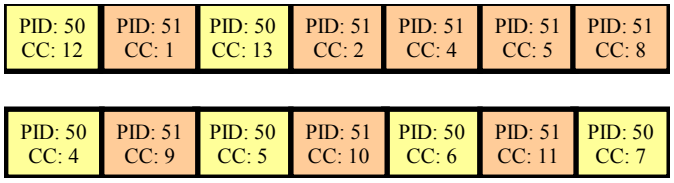
B.2 Default Multicast Monitoring

When the protocol mapping is nTS/UDP, meaning there is no RTP information in the multicast stream, there is no easy way to isolate and register network-induced errors. Assumptions can be done by performing continuity counter analysis for the content of each received UDP-frame on the fly. The probe will note CC-errors (**CCerr**) and generate corresponding alarms (**CC skips:N**).

Imagine the following MPEG-2 Transport Stream being generated by an encoder. The TS contains two PIDs (50 and 51) and the Continuity Counter (CC) values are continuous for each PID since there are no packets missing.



When the Transport Stream reaches our imaginary head-end some packets (those with red frame) have been lost (maybe due to a bad satellite connection). Our IP-Streamer packs 7 and 7 MPEG-2 TS packets into each UDP-frame (mapping is 7TS/UDP) and the resulting frames may look like:



...

The probe's response to this multicast is summarized in the following table:

Sequence	Effect
UDP packet #1 (7 MPEG2 TS packets): PID 50: 12, 13, 14, 15 PID 51: 1, 2, 4, 5, 8 PID 51 has 2 CC discontinuities of 2 (2→4) and 3 (5→8)	Monitoring page: **CCerr:+2**
UDP packet #2 (7 MPEG2 TS packets): PID 50: 4, 5, 6, 7 PID 51: 9, 10, 11 PID 50 has 1 CC discontinuity of 6 (13→4)	Monitoring page: **CCerr:+1**
If no more CC-errors for at least 1 second	Alarms & events: **CC skips:9 discontinuities:3** Depending on the thresholds you may also get: **MLR >= warning-threshold (9 >= 1)**

There were 9 TS packets missing (with red frame) and the alarm reflects this.

B.3 Strategy for MediaWindow Analysis

This section provides further insight into MediaWindow analysis and suggests how the Ethernet threshold settings can be configured to maximize the usefulness of the MediaWindow graphs and alarms.

The MLR value is always calculated using the continuity counter inside the transport stream packets. Since the continuity counter is expected to increase by one for each packet of the same PID it is possible to detect missing TS packets by noting gaps in the continuity counters. Knowing that there are usually 7 transport stream packets inside one UDP packet you expect a continuity counter error of 7 if one UDP packet goes missing. This corresponds to an MLR value of 7. The range of the continuity counter is 4 bits meaning that if you are unlucky and lose exactly 16 packets for the same PID you will not be able to detect the packet loss at all. Losing 16 or more packets of the same PID is very rare and will only happen in networks with plenty of obvious problems.

Not all PIDs carry continuity counters. The null packets (PID 8191) and PIDs carrying PCR (program clock reference) do not carry continuity counters. This is the reason why losing one UDP packet does not necessarily result in an MLR of 7 but maybe 6 or even 5 (assuming the mapping is 7TS/UDP).

Systems typically do not mix the mappings among their streams so there is seldom a need to remember the mapping for streams in order to interpret the exact impact of MLR values.

The range of the MediaWindow graphs can be configured by the user. Even when the graph is updated in "real-time" each bar in the graph will represent a large number of elementary measurements. For



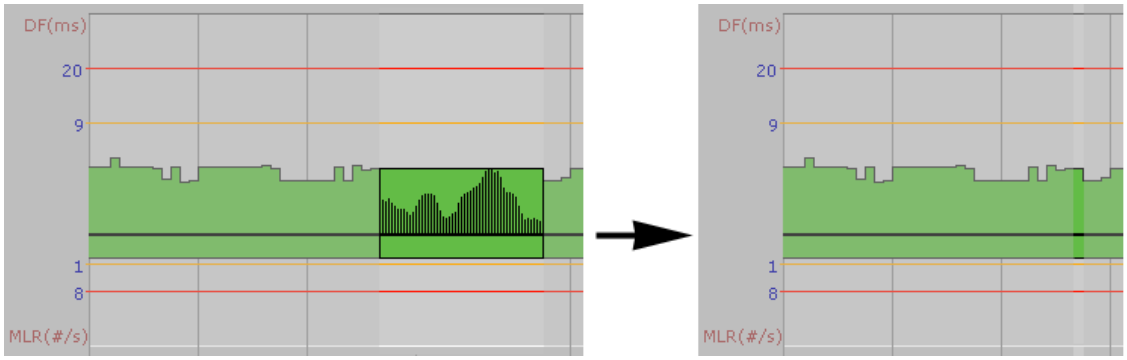
a 5Mbit/s stream there will be approximately 500 elementary measurements per second, assuming a mapping of 7 TS packets into each UDP-frame (i.e. there are approximately 500 UDP packets per second). An elementary measurement is generated for each interval between two neighboring UDP frames.

Within each update-interval only the extreme IAT and MLR values are displayed in the graph. For IAT the peak inter-arrival time over the measurement period represents the IAT for that period. For MLR the highest loss ratio within any second represents the MLR for that period.

When the range of the graph is set to larger intervals, even more elementary measurements are merged for each bar-interval.

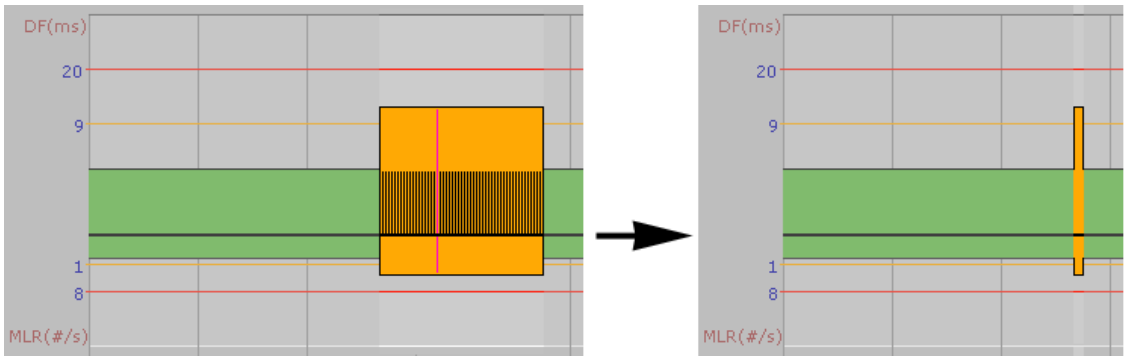
The rest of this discussion assumes the MediaWindow graph range is set to “running” since that lowers the probability that more packet losses occurred inside the same bar-interval.

The following figure shows how a large number of elementary measurements are represented by one bar in the graph.

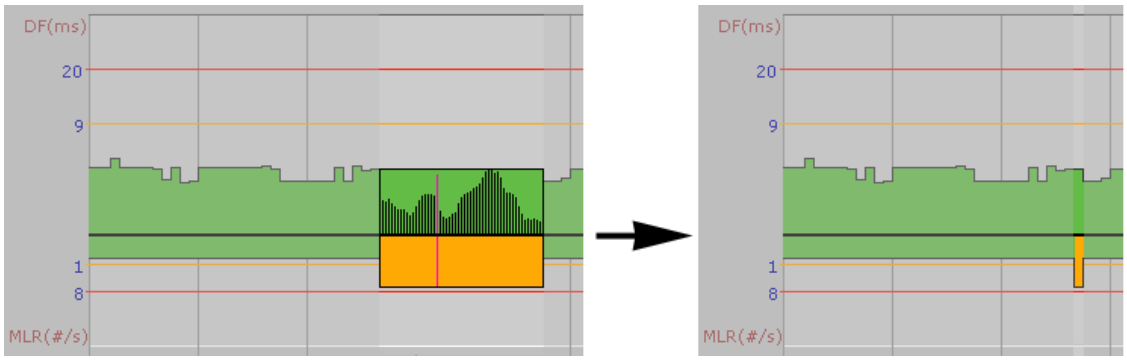


B.3.1 IAT Before and After Router

Packet-loss that occurs before or inside a router will usually not be visible since the queuing mechanism at the outgoing interface of the router will send out packets in an orderly fashion. If however the packet-loss did occur after the router (due to line noise for example) thus affect the timing between two neighboring packets – effectively doubling it – the packet loss will always affect the IAT component for CBR streams. For VBR streams, that are jittery by default, the extra time gap may have no effect since there may already be other larger gaps within the MediaWindow interval.



If a UDP packet goes missing after it has left the router it will visually affect both the IAT and MLR for CBR streams. The pink line represents one elementary measurement.

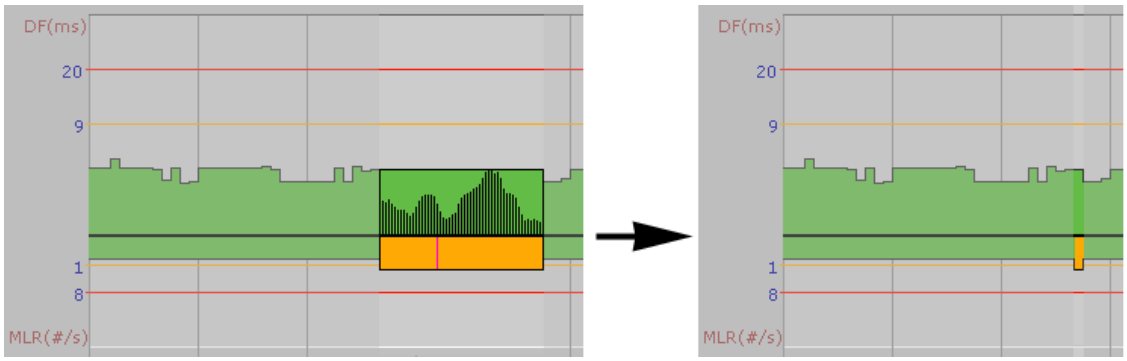


For VBR streams a similar packet-loss will not necessarily affect the IAT graph even if the time between two neighboring packets doubles. The pink line represents the IAT and MLR value measured for the missing packet.

B.3.2 Identifying UDP Packet Loss

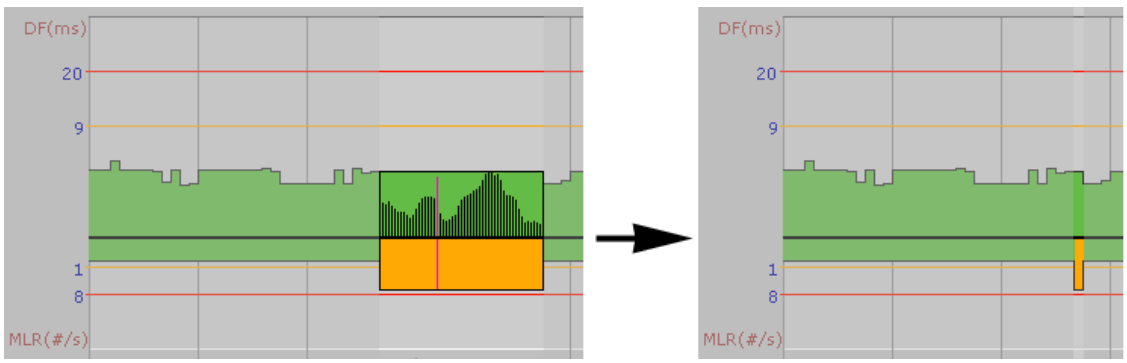
This discussion does not apply to streams with TS/RTP mapping since in that case identifying UDP packet loss is straight forward.

There is no fail-safe way to distinguish packet loss caused by dropping UDP packets from packet loss caused by dropping packets inside the TS layer. IP based networks will generally not introduce new errors in the TS layer. As soon as the TS layer is wrapped inside UDP packets all further processing operates on the UDP packets.



The pink line indicates a packet loss of 1-4 with no jitter component.

As a rule of thumb, the co-existence of small MLR readings (1-4) and no IAT readings can be assumed to have been caused by packet loss in the original TS data.



The pink line indicates a packet loss of 6 or 7 and a doubling of the jitter component.



A UDP packet-drop will usually show up in the MLR value as a multiple of the mapping value; for a mapping value of 7 TS packets into each UDP packet, the MLR component will be equal to 7, 14, 21 etc.

Slightly lower values such as 6, 13, and 20 can be expected if a missing UDP packet did contain one TS packet without continuity counter (i.e. a PCR packet with no payload).

As we have seen, there is no sure way to distinguish between UDP packet-loss and loss in the underlying TS packets. One way to deal with the situation is to have a probe doing zero readings close to the signal source before the network can introduce UDP packet loss.

B.4 Multicast Thresholds

It is useful to configure individual threshold settings for IAT for each stream unless they are fixed at the same bit-rate. Streams that are being monitored by several probes should have equal Ethernet thresholds configured on each probe to make it easy to compare measurements for a stream across several probes.

As a rule of thumb the IAT warning threshold could be set to 50% above the max IAT value observed over a considerable period of time, the last 24h or so. The IAT error threshold could be set a little below the maximum jitter the system can tolerate – usually limited by the STB jitter tolerance. STB manufacturers should be able to provide information about how much jitter they can handle. Setting the Ethernet warning-threshold too high results in a graph where almost all plots are close to the x-axis and it becomes less useful to visually compare MediaWindow graphs.

For streams with TS/UDP mapping the default MLR threshold is set so that errors are reported if the number of CC errors exceeds the number of TS packets in one UDP frame (assumed to be 7).

B.5 Dedicated interface for OTT

As a rule of thumb, you should never have OTT traffic on the same network as multicasts. This means that you should either use one 10G Software Probe for multicast and one for OTT, or you should use different and dedicated interfaces for each.

The interface used for OTT traffic is controlled using the **Setup — Routing** view.

B.6 OTT descrambling with Verimatrix

If you are using a Verimatrix VCAS 3.7 server to encrypt your OTT stream, you can get the 10G Software Probe to descramble the chunks. It will uses the same API to descramble the chunks, as the encoder or segmenter uses to encrypt the chunks. To achieve this, the 10G Software Probe need to be able to reach the VCAS server's private encoder interface.

Since the 10G Software Probe only uses a single interface for OTT, your network needs to be configured such as the 10G Software Probe can reach both the VCAS server and your origin server on the same interface.

B.7 OTT Bandwidth requirements

The recommended available bandwidth for full coverage OTT monitoring is equal to the sum of the profile bitrates monitored plus an estimated overhead of 20 % for manifests and IP, TCP and HTTP headers.

Note: The OTT engines will be using all available bandwidth on the interface in spikes while downloading the chunks, this is the main reason why it is not a good idea to mix multicasts on the same interface, as it can cause packet drops which multicasts cannot handle.

C Appendix: OTT Profile Health

C.1 OTT Profile Health Bar

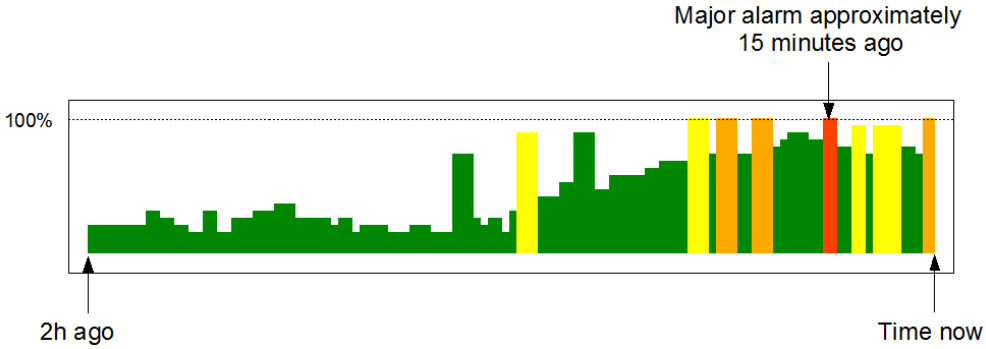


The profile health bar displayed at channel level shows an overview of current status for individual channel profiles. Different colors indicate status:

- Green: OK
- Yellow: Warning
- Orange: Error
- Red: Major
- Black: Fatal

All enabled alarms may affect the profile health bar, and alarm severities can be assigned to each alarm in the **Alarms — Alarm setup** view.

C.2 OTT Profile Health Timeline



The OTT profile health timeline shows information about channel bitrate and channel alarm status for the last two hours, with a time resolution of one minute. Green parts of the timeline indicate profile download time versus chunk length. The graph is scaled so that 100% indicates a chunk download time identical to chunk length (in seconds), chunk length being signaled in the profile manifest. Quick chunk download times therefore result in a 'low' green graph, as seen in the left hand part of the graph above. When download times exceed the user defined profile bitrate warning and error thresholds the graph is colored yellow and orange respectively.



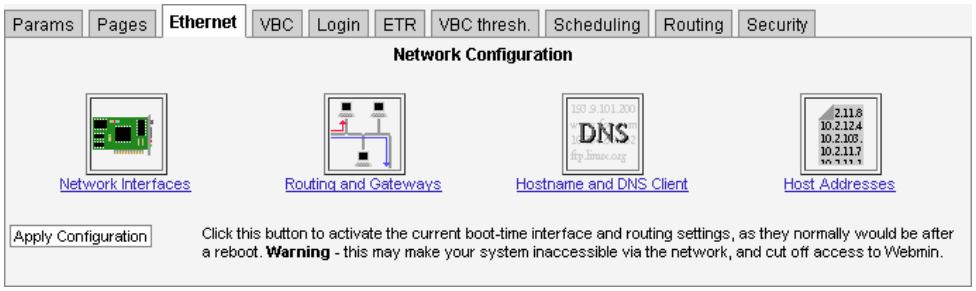
In addition to profile bitrate indication the graph displays profile status information related to non-bitrate alarms. Active profile alarms are represented in the graph as 100% bars, the color reflecting the severity of the alarm. If several alarms are active within a one minute period the graph color will reflect the most severe alarm. Historical alarms can be examined in more detail by viewing the OTT alarm list.

D Appendix: Network configuration

D.1 Web-based configuration

The system ships with a web-based network configuration module. If you are unable to access the system using the web interface, you will need to use the system console. Please see section D.2 for details on how to use the command-line based configuration tool from the console.

To access the web-based configuration module, open the **Setup — Ethernet** view.



The web-based network configuration tool is based on WebMin. Further documentation is available in the WebMin documentation[1].

Another alternative is to install the Cockpit web-based interface, which can be used to configure most aspects of the system, including the network settings. Packages for Cockpit are available in the base CentOS/Red Hat Enterprise Linux distribution. For more information on how to install and use Cockpit, please refer to Getting Started With Cockpit[2].

D.2 Command-line based configuration

Changes to network configuration, adding new interface devices and VLANs can be done with the **nmtui** tool. Simply type **nmtui** whilst logged into the server command shell as root[3]. Navigate the nmtui menus using the cursor (arrow) keys and Enter to select. More documentation on using **nmtui** can be found in the Networking Guide[4].

Editing Network interface configuration

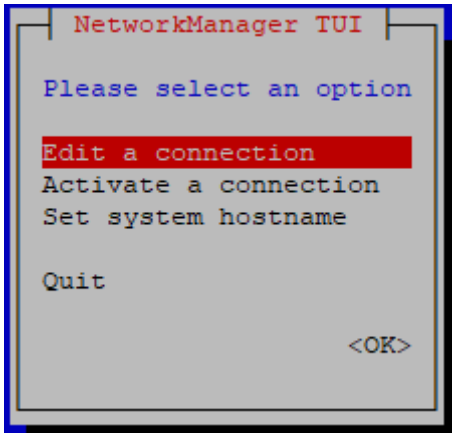
To edit a connection first select **Edit a connection** from the nmtui menu:

[1] `https://doxfer.webmin.com/Webmin/Network_Configuration`

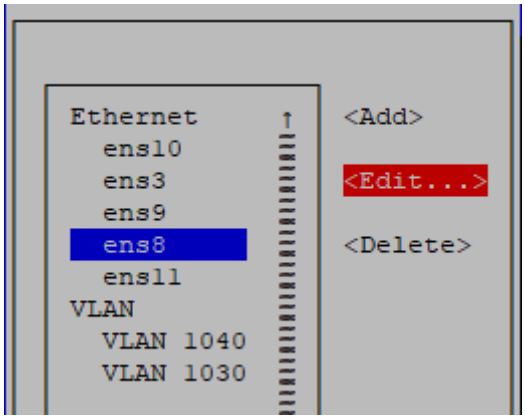
[2] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/getting_started_with_cockpit/`

[3] If the **nmtui** tool is not available on your system, you can install it by issuing the command **yum install NetworkManager-tui**

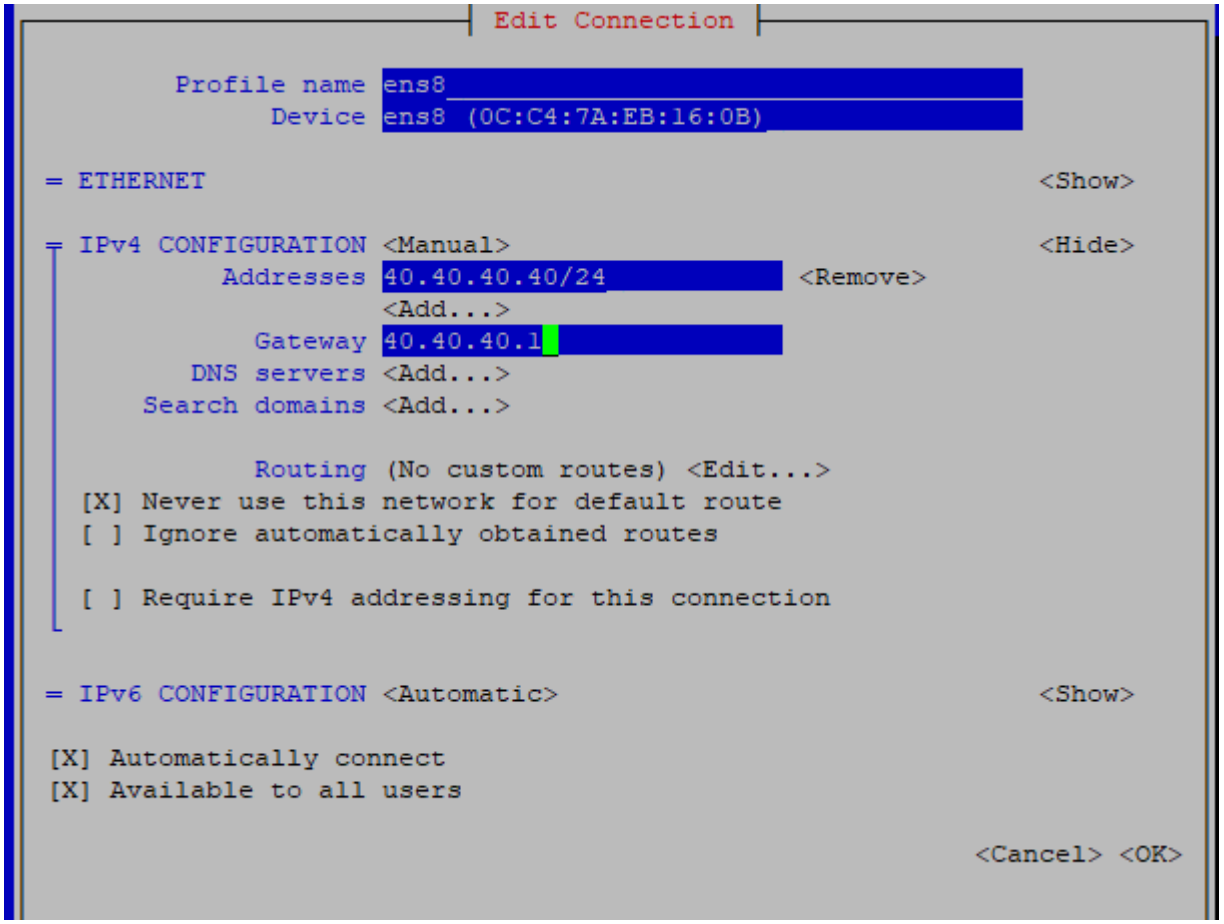
[4] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/sec-Networking_Config_Using_nmtui.html`



Select the interface to be edited and then select **Edit...** from the menu.



Make the necessary changes to IPv4 and IPv6 configuration.



Selecting **Automatically connect** will ensure the interface is connected next time the system boots.

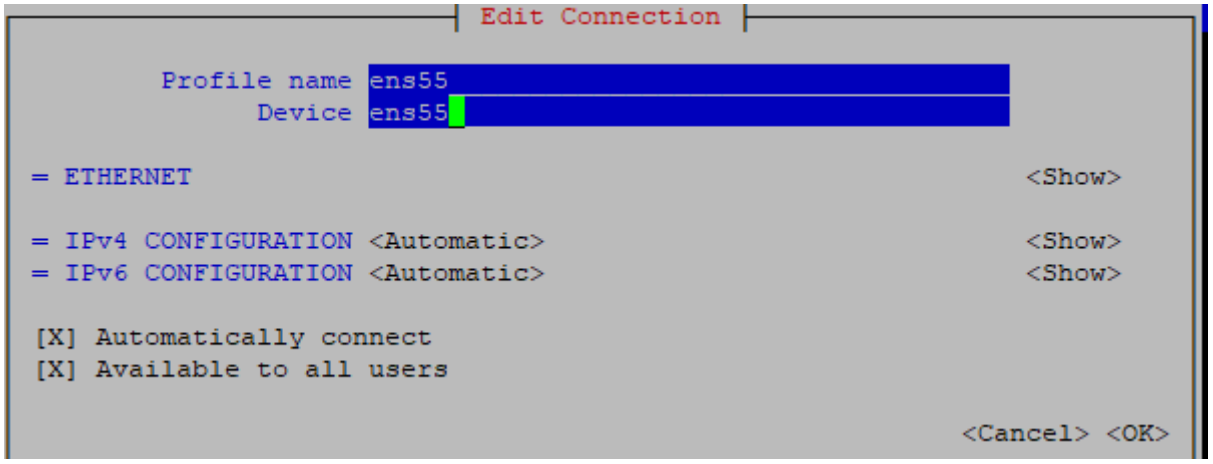
Sometimes it is desirable to select **Never use this interface for default route**, particularly if additional interfaces are only used for monitoring multicast traffic or when setting up a native interface for adding VLANs.

After making changes select **OK** to return the previous menu. Generally, network configuration changes will take effect the next time the interface is activated. This can be done by deactivating and reactivating the interface from the **Activate a connection** menu in nmtui or with the command line **ifdown ifname** followed by **ifup ifname**.

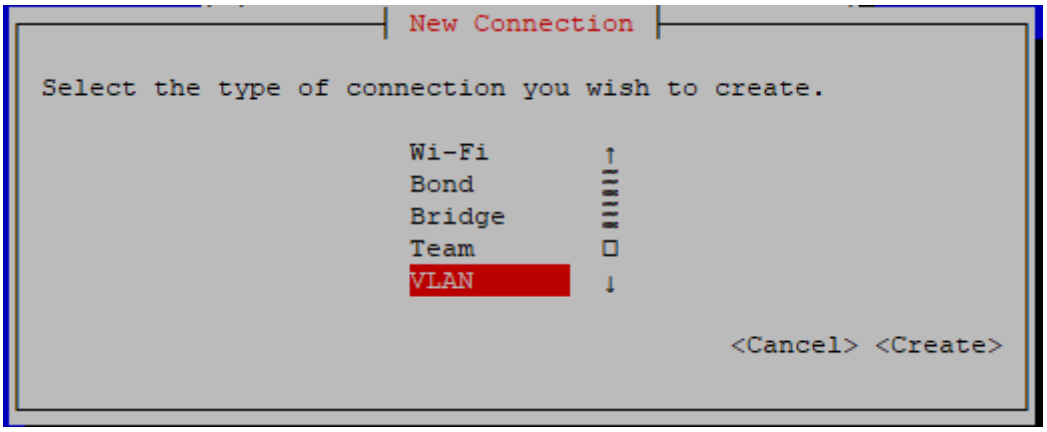
Adding new and VLAN interfaces

To add a new interface, in the nmtui main menu select **Edit a connection** followed by **Add** and select the interface type from the menu. Typically this is **Ethernet** but may also be used to create VLAN interfaces. Advanced configurations such as Bond and Bridge may be selected if they are required.

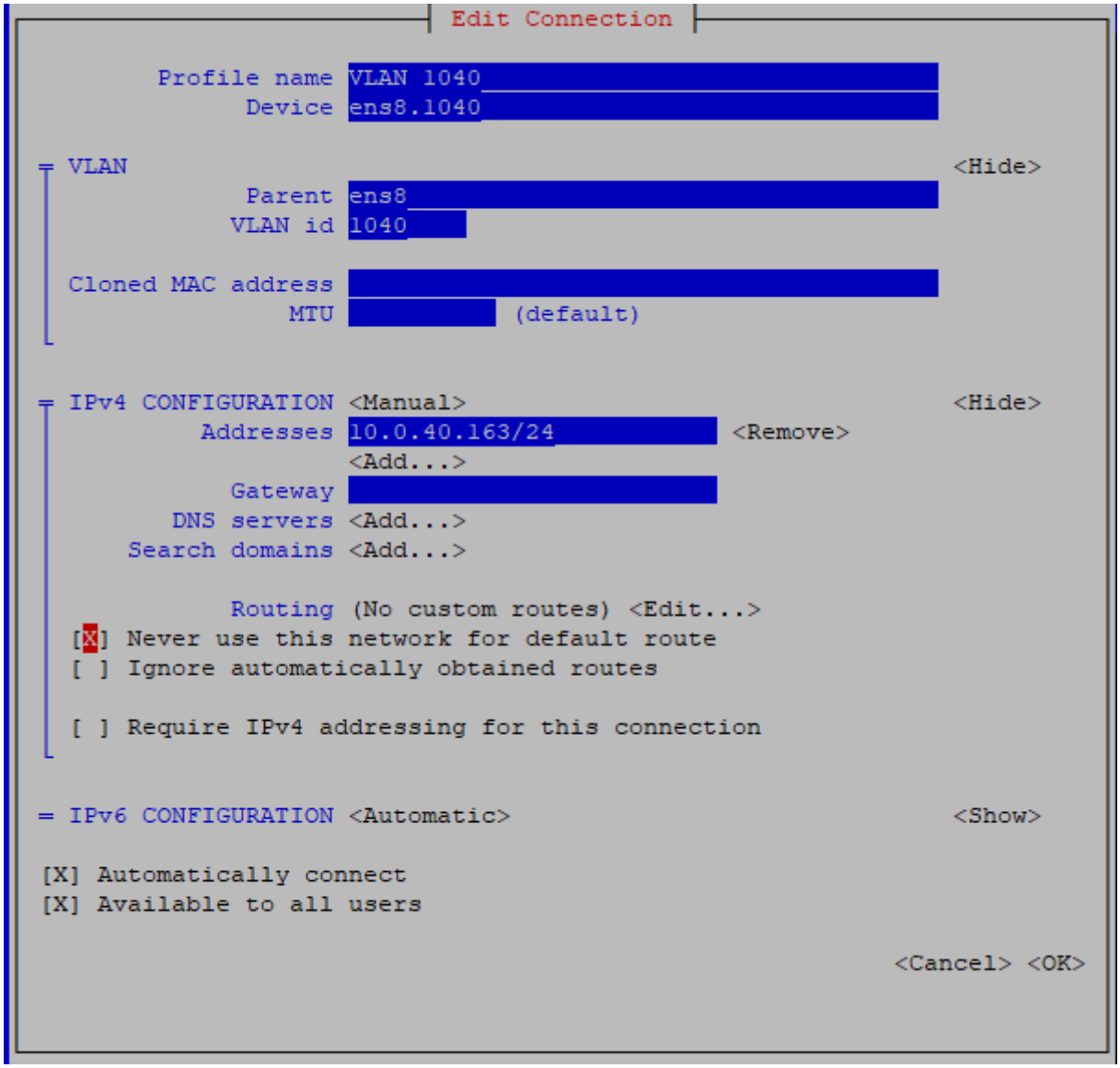
To find the system assigned name for a newly added hardware device use the command line **ifconfig** or search in the output of the **dmesg** tool. It can be helpful to keep the nmtui **Profile name** for the device the same as the device name itself, for example:



To add a VLAN interface from nmtui main menu select **Edit a connection** followed by **Add**. Scroll to the bottom of the list and select VLAN:



Edit the settings for the VLAN interface. The Device field should contain the name of the physical interface to be used for this VLAN and the VLAN number, for example `ens8.1040` means VLAN *1040* on interface *ens8*. The parent and VLAN ID fields should correspond to the values in the name field. In our example *ens8* is the parent and *1040* is the VLAN. Other settings are the same as for normal IPv4/6 interfaces.



After entering the configuration for the VLAN interface select **OK** to return the previous menu, then select **Back** and finally **Activate a connection** to activate the newly created VLAN interface.



E Appendix: Enabling HTTPS

By default, all web communication to and from the host running the 10G Software Probe is using unencrypted HTTP communication. To enable HTTPS, the installed Apache server software needs to be configured appropriately.

The guide below is based on the guide from the CentOS Wiki[1]. To install packages, generate keys and update the Apache configuration, you will need to be root so you can either **su** to root or use **sudo** in front of the commands below.

If the system is available on a publicly visible host name, you can use EFF's Certbot to deploy a Let's Encrypt certificate. Please see the section **Using Certbot with Let's Encrypt** below.

> Installing packages requires an active Internet connection. If you are using Red Hat Enterprise Linux, you will need an active subscription to install packages.

Getting the required software

To enable SSL on Apache, you will need to install the `mod_ssl` package, if not installed already. To install the package, issue the following command:

```
yum install mod_ssl
```

Generating a certificate

If you have an internal certificate authority, use that to create a certificate. Otherwise follow the steps below to generate a self-signed certificate. Please note that modern browsers display a warning message when connecting to a web server running a self-signed certificate. This message can usually be suppressed by installing the certificate in the browser.

First generate a private key, which we call **ca.key**:

```
openssl genrsa -out ca.key 2048
```

Second, create a certificate signing request (CSR) in **ca.csr**:

```
openssl req -new -key ca.key -out ca.csr
```

Third, we self-sign the key:

```
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

[1] `https://wiki.centos.org/HowTos/Https`



We now have the necessary files, but we need to copy them to the correct locations in the file system:

```
cp ca.crt /etc/pki/tls/certs
cp ca.key /etc/pki/tls/private/ca.key
cp ca.csr /etc/pki/tls/private/ca.csr
```

Configuring the web server

The Apache SSL configuration file, **/etc/httpd/conf.d/ssl.conf**, needs to be updated to make use of the generated certificate. Open it using a text editor, for example:

```
vi +/SSLCertificateFile /etc/httpd/conf.d/ssl.conf
```

Change the paths to match where the Key file (**ca.crt**) and Certificate Key (**ca.key**) are stored. If you've used the method above, the configuration should be:

```
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
```

We also need to forward the configuration from the HTTP host to the HTTPS host. This is done by adding the following line anywhere in the `VirtualHost` declaration in the **ssl.conf** file, you can for instance add this next to the lines above:

```
RewriteOptions Inherit
```

Quit and save the file and then restart Apache by issuing the command

```
systemctl restart httpd
```

All being well you should now be able to connect to the system using HTTPS. If there was an error, the command output should give you some hints on where to look.

Disabling HTTP access

To configure the server to redirect any access arriving over HTTP to the HTTPS server, the simplest way is to create the file `/etc/httpd/conf.d/001-http-to-https.conf`[2]:

```
cat <<'EOM' > /etc/httpd/conf.d/001-http-to-https.conf
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
EOM
```

[2] `https://wiki.apache.org/httpd/RewriteHTTPToHTTPS`



After creating the file, restart Apache by issuing the command

```
systemctl restart httpd
```

If this does not work, please consult the Apache documentation or the Apache Wiki[3]. It is also possible to completely disable the HTTP port, if it is not needed.

Using Certbot with Let's Encrypt

If the system is available on a publicly visible host name, you can use EFF's Certbot to deploy a Let's Encrypt certificate. Some preparations are needed before running Certbot.

To enable SSL on Apache, you will need to install the `mod_ssl` package, if not installed already. To install the package, issue the following command:

```
yum install mod_ssl
```

Next, we need to configure Apache *VirtualHost* configurations for HTTP and HTTPS. The HTTPS one is configured in the Apache SSL configuration file, **/etc/httpd/conf.d/ssl.conf**, and needs to be updated slightly:

Open it using a text editor, for example:

```
vi +/VirtualHost /etc/httpd/conf.d/ssl.conf
```

Add the following line after the `<VirtualHost _default_:443>` line:

```
RewriteOptions Inherit
```

Finally, we need to create a VirtualHost for the HTTP part, this one is kept simple and can be created by issuing the following command:

```
cat <<'EOM' > /etc/httpd/conf.d/002-http-virtualhost.conf
<VirtualHost _default_:80>
RewriteOptions Inherit
</VirtualHost>
EOM
```

Now the configuration should be ready for adding the Let's Encrypt certificate. Please follow the Certbot guide[4] for information on how to do that.

[3] `https://wiki.apache.org/httpd/RedirectSSL`
[4] `https://certbot.eff.org/lets-encrypt/centosrhel7-apache`

F Appendix: Enabling NTP time synchronization

It is strongly recommended that the server running the 10G Software Probe be synchronized against an external NTP server.

If not set up correctly, alarms may be displayed with incorrect timestamps and out out alignment with other monitoring devices in the system.

NTP synchronization against public servers on the Internet is usually enabled automatically if they were detected during the operating system installation. It is possible to change the servers to use, for instance to set it to use a local NTP server, by changing the configuration in the file `/etc/chrony.conf` manually.

Setting the VBC IP address in the **Setup — VBC** view will automatically add it as a time synchronization source.

For more details on configuring the date and time settings, please refer to the System Administrator's Guide, chapters *Configuring the Date and Time*[1] and *Using chrony*[2].

[1] `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/System_Administrators_Guide/chap-Configuring_the_Date_and_Time.html`

[2] `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/sect-using_chrony`



G Appendix: On-line License Verification

G.1 Introduction

The 10G Software Probe uses licenses which are verified and updated periodically over the Internet, without the need for human intervention. The license is only tied to the VB330-SW when it is used and is periodically renewed. To transfer the software to a new host, the license can simply be released from the software and applied to an instance running on a different server.

> Please make sure you have the license key available before you release the license, as you must enter it again on the system you wish to transfer the license to. The license key is *not* displayed in the VB330-SW user interface.
>
> If you have lost the license key, contact your dealer to retrieve it. Make sure you include all details from the **About — License** view in your request.

When the 10G Software Probe sends the on-license verification over the Internet, it includes some basic information to verify the 10G Software Probe. This includes a basic hardware footprint, as well as parts of the SNMP identification data configured in the **Setup — Params** view.

G.2 Requirements

The VB330-SW needs to be able to contact the license server either directly or via a proxy server, as described below. If proxy connectivity also is not available, an off-line verification procedure is available as well.

The VB330-SW must also be configured with a correct date and time. Please refer to F Appendix: Enabling NTP time synchronization for more information on configuring time synchronization.

Direct access to verification server

To verify the license on-line directly, the VB330-SW needs to be configured with a valid DNS server address (see D Appendix: Network configuration) which is able to look up the host name `license.microanalytics.org`. The VB330-SW needs to be able to contact the host this name resolves to using HTTPS on port 443 (outgoing only).

Using the VBC server as a proxy

When installing the VBC software to a server, an instance of the Tinyproxy[1] software is automatically installed and configured to allow its connected blades to connect to (and only to) the licensing system as described in the previous section.

When the VB330-SW has been configured with the address to the VBC server in the **Setup — VBC** view, the VB330-SW will automatically attempt to use this proxy if a direct connection fails.

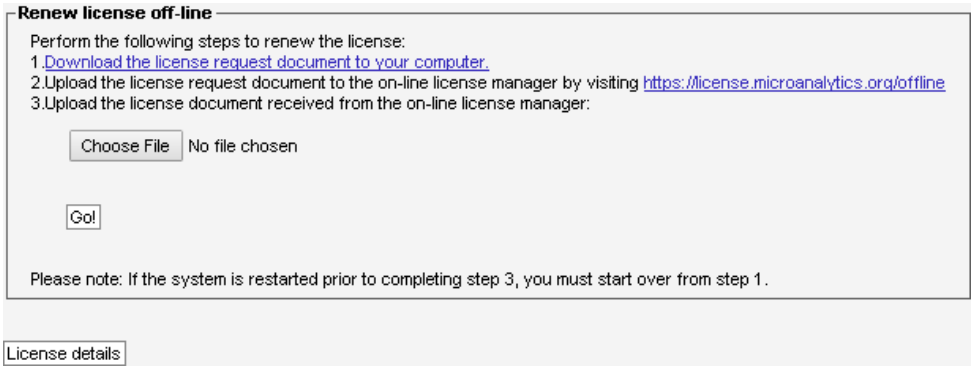
[1] `https://tinyproxy.github.io/`

Using an arbitrary proxy server

The 10G Software Probe can be configured to use an arbitrary proxy server to connect to the licensing server. By adding the URL to a proxy server in the **Setup — Routing** view, the VB330-SW will automatically attempt to use this proxy if a direct connection fails.

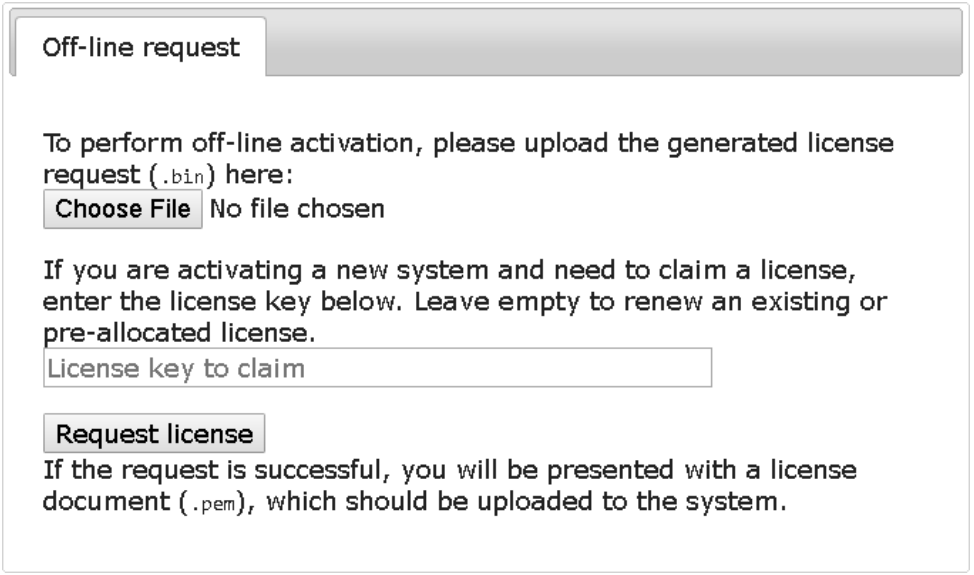
Off-line verification procedure

If the VB330-SW network is completely disconnected from the Internet, it is still possible to verify the license using the off-line verification procedure. When using this, the license will be tied to the system and will not be transferable to another server. Click the **Renew license off-line** button to start the off-line verification procedure. This procedure has to be repeated yearly.



Follow the steps described in the dialog to renew or activate the license. To abort the procedure, click the **License details** button to return to the previous screen.

First, download the license request document from the 10G Software Probe to the computer you are browsing from. Once the file has been downloaded, connect the computer to the Internet if not already connected, and open the link to the off-line license manager[2].



[2] https://license.microanalytics.org/offline



Select the `.bin` file that was downloaded in the first step, and optionally add a license key if the system you are activating did not already have a license attached. Once done, click the **Request license** button and save the license document file to the computer.

If needed, re-connect to the VB330-SW network, return to the **Renew license off-line** view, select the `.pem` file that was generated by the license manager and press **Go!**

The license should now be added to the system. If this is a new or different license, the software will restart. Use the **License details** view to verify that the license was applied correctly.

H Appendix: Software Maintenance

Purchasing yearly software maintenance enables future feature protection and guarantees access to the latest software for the 10G Software Probe. The latest version of the VB330-SW software can be found in the End User area at `https://www.bridgetech.tv/`.

The software maintenance can be purchased for a three or five year period, typically initially purchased together with the system itself, during which new major releases can be installed.

The current software maintenance period is displayed in the **About — License** view, see chapter 5.12.2 for more details. For an overview of software maintenance periods for multiple units, please refer to the **Equipment** view on the VBC Controller server.

For renewals, contact the local partner the system have been purchased from or Bridge Technologies directly at: `sales@bridgetech.tv`, with the title "**se-maintenance**".

Use the **Data — Software** view to update the VB330-SW software, please refer to chapter 5.11.2.



I Appendix: Software Upload

The process of performing a software upload to the probe involves the following steps:

1. Obtain the software image.
2. Export and save the probe configuration.
3. Transfer the image to the probe using the software upload functionality in the **Data — Software** view, the Software Activation interface or by using ssh, and save the new software image on the system.
4. Wait while the software is being saved.
5. Verify the new image.

I.1 Obtain the software image

The image will have a **.tea** extension and is distributed in a compressed ZIP archive together with the readme file detailing changes for this patch release.

Please study the **readme** file to be aware of any important information related to your current software patch. Subsequent patch details may indicate that significant bugs were identified and resolved after your current version and indicate where special care is recommended.

You can find the current version number under **About — Release**.

When upgrading to a new major version, please also study the release notes and **readme** files for all versions between your currently installed major version and the one you are upgrading to, as there might be important changes that you need to be aware of.

If you require any assistance understanding the release notes or readme files please contact your first line support service.

If you would rather re-install the system from scratch instead of using the upgrade procedure, please refer to chapter 3.

I.2 Export and save the probe configuration

Software upgrade should not alter the probe configuration, however for safety is is a good idea to export the probe configuration (from the **Data — Configuration** view) and save it to a file. Please refer to chapter 5.11.1.

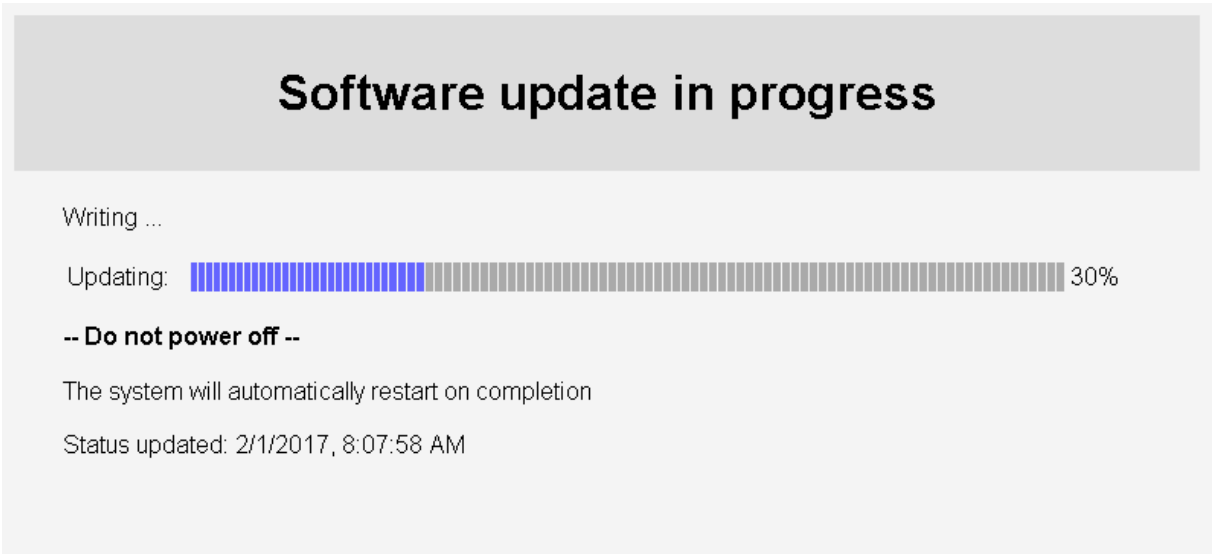
I.3 Transfer the image to the probe and save

Using the software upload functionality in the Data view

From the **Data — Software** view select the software image file to be uploaded and click the **Go!** button. When the software has been successfully transferred to the probe click the **Update software** button and confirm.



Progress bars are displayed to show the software update status.



Note that the probe will restart when the new software has been installed, and the probe's user interface will be unresponsive until restart has completed.

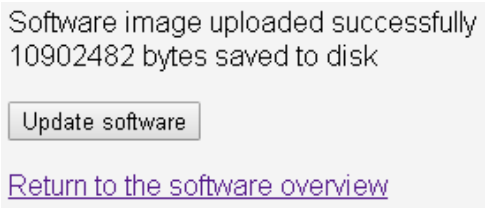
Using the software upload functionality in Software Activation

It is also possible to upload the software image using the Software Activation interface. Access Software Activation and expand the **More options** heading. Under the heading **Update software**, select the software image file to be uploaded and click the **Update** button.





When the software has been transferred to the probe, click the **Update software** button to initiate the update.



If the software was already activated, you will be transferred to the progress bar displaying the update status as described above.

If the software was not activated, the upgrade will run in the background and you will be forwarded to the product page inside the Software Activation interface. Depending on how long the update takes, you may need to reload the product page again to verify that the software has been updated.

Using scp/sftp and ssh

Using a Secure Shell (ssh) client, such as PuTTY[1], first transfer (scp/sftp) the software image to the system.

Next, log in to the system as the **root** user to get a command prompt. If you copied the file as the root user, the file should be in the directory you just logged in to. If not, navigate to the directory you uploaded to using the **cd** command.

Copy the downloaded file to the `/var/opt/btech/probe` directory and issue the command `/opt/btech/probe/bin/vprobe_upgrade` to begin the upgrade procedure.

```
cd /path/to/download
cp filename.tea /var/opt/btech/probe
/opt/btech/probe/bin/vprobe_upgrade
```

I.4 Wait while the software is being saved

This will take a few minutes. The probe software will then restart automatically. The probe should state that the software image has been saved successfully.

When using the alternate method do not disconnect the ssh session before the software upgrade is completed.

I.5 Verify the new image

Connect a browser towards the probe and verify the version and build time in the **About — Release info** view.

If you upgrade a product that has not been activated using the Software Activation interface, open the product page in the Software Activation interface to verify the version number.

[1] `https://www.chiark.greenend.org.uk/~sgtatham/putty/`

I.6 Software upload troubleshooting

If the upgrade is rejected, verify that the software version you are trying to upload is covered by software maintenance. Refer to H Appendix: Software Maintenance for more details.

If the web interface does not appear to work correctly straight after upgrading the probe it may be because the web browser is using files that are cached. Files may be cached for up to one hour in the web browser. To fix the issue, clear the cache manually:

Google Chrome: Settings — Advanced — Clear browsing data — Cached images and files

Mozilla Firefox: Options — Privacy & Security — Cached Web Content — Clear Now

Microsoft Edge: Settings — Clear browsing data — Choose what to clear — Cached data and files

Microsoft Internet Explorer: Tools — Internet options — General — Browsing history — Delete... — Temporary Internet files and website files

Note that the probe configuration may be lost when downgrading to an older software version. In this case the saved configuration file may be useful.

A log file from the last upgrade process is included in the debug data, which can be downloaded from the **Data — Configuration** view. If you are unable to access the GUI after the upgrade, you can inspect the log file manually by logging in to the system and opening the file `/opt/btech/probe/log/upgrade.log` manually.