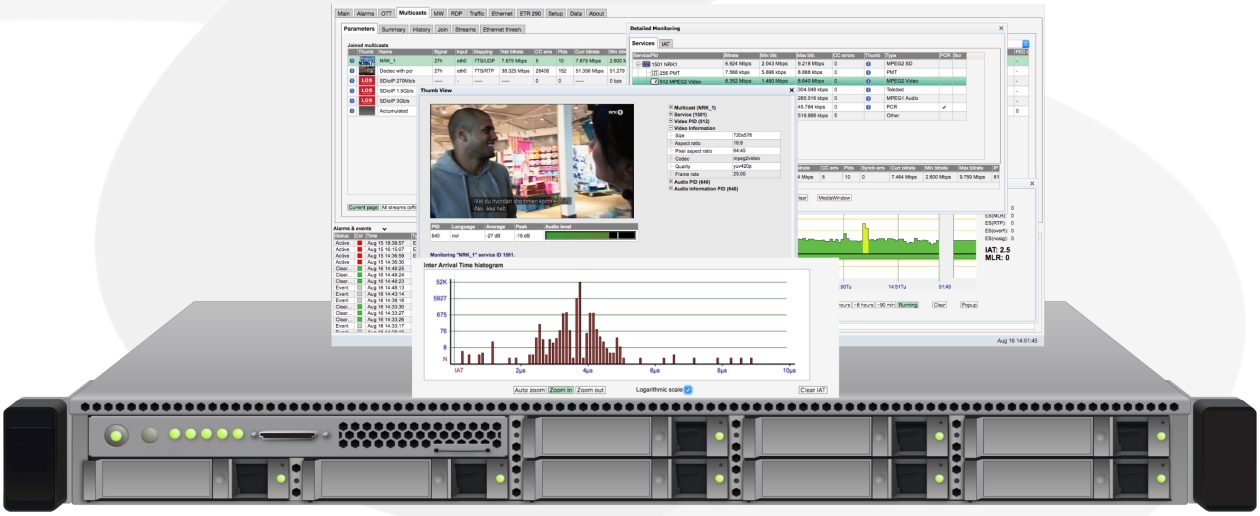


VB330-SW 10G Software Probe

Applies to software release v6.5

Form 8160J • February 2025

VB330-SW 10G Software Probe User's Manual
Revision 9f077faf (2025-02-05)

3200 Sencore Drive, Sioux Falls, SD USA
www.sencore.com

About Sencore
Sencore is an engineering leader in the development of high-quality signal transmission solutions for the broadcast, cable, satellite, IPTV, and telecommunications markets. The company's world-class portfolio includes video delivery products, system monitoring and analysis solutions, and test and measurement equipment, all designed to support system interoperability and backed by best-in-class customer support. Sencore products meet the rapidly changing needs of modern media by ensuring the efficient delivery of high-quality video from the source to the home. More information about Sencore is available at the company's website, www.sencore.com.

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

Contents

Document Revision History

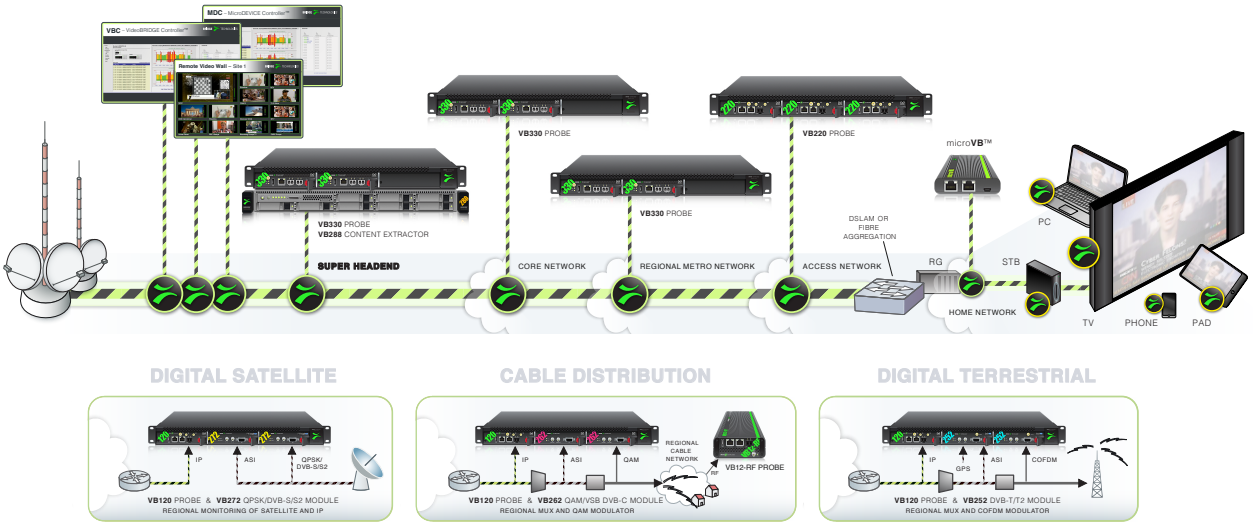
Date	*Version*	*Description*
February 2025	6.5	Updated manual to reflect changes in v6.5 software
August 2024	6.4	Updated manual to reflect changes in v6.4 software
March 2024	6.3	Updated manual to reflect changes in v6.3 software
June 2023	6.2	Updated manual to reflect changes in v6.2 software
February 2022	6.1	Updated manual to reflect changes in v6.1 software
November 2020	6.0	Updated manual to reflect changes in v6.0 software
February 2020	5.6	Updated manual to reflect changes in v5.6 software
February 2019	5.5	Updated manual to reflect changes in v5.5 software
February 2018	5.4	Updated manual to reflect changes in v5.4 software
February 2017	5.3	Updated manual to reflect changes in v5.3 software
March 2016	5.2	Updated manual to reflect changes in v5.2 software
February 2015	5.1	Updated manual to reflect changes in v5.1 software
January 2014	5.0	Updated manual to reflect changes in v5.0 software

1 INTRODUCTION

1.1 About the Software Probe

1.1.1 VB330-SW – Overview

With support for up to 100 Gbit/s Ethernet connectivity and a massive multiprocessor architecture the VB330 can deliver monitoring and analytics of thousands of streams and a multitude of technologies in real-time and in parallel. The VB330 is deployed either on dedicated embedded hardware, as a pre-configured and pre-installed appliance or as a software-only solution. This gives the operator greater flexibility when it comes to tailoring the monitoring solution towards the underlying system architecture in the best possible manner. Feature parity is ensured across the various deployment options, varying only in factors such as scalability, power consumption and longevity. The web-based user experience and feature availability stays the same across all the deployment alternatives.



The OTT software option is available on the VB330-SW and enables monitoring of up to 1000 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 Software Probe can also be managed via the VideoBRIDGE Controller. The VideoBRIDGE Controller will add management features like alarm aggregation and report functionality.

The Software Probe is a server appliance, that can be installed onto any server that meets the minimum requirements specified in chapter 3 or delivered as a pre-configured and pre-installed appliance server.

1.1.2 VB330-SW – Platform alternatives

The VB330, VB330-SW and VB330-SW probes supports common functionality for all the available deployment alternatives, varying mostly only in factors such as storage size and stream count. This is in contrast to the VB120 and VB220 embedded hardware probes which support add-on interface cards to support different RF and ASI standards. These include VB242 and VB246 for ASI, VB252 for DVB-T/T2, VB262 for QAM, VB256 for ISDB-T, VB258 for DVB-T, DVB-T2, DVB-C, QAM-B, ISDB-T, ATSC 1.0 and ATSC 3.0 and VB272 for satellite.

VB330 Embedded Hardware	*VB330/VB380 Appliance Server*	*VB330 Software Image*
Custom electronics developed by Sencore	Pre-selected server hardware with pre-loaded software	Software image for installation on Ubuntu
Low power consumption. Each VB330 draws approx. 35 W	Server power consumption	Suitable for 3rd party server installation
Dual 10 Gbit/s SFP+ network interface	Dual QSFP28 10/25/40/50/100 Gbit/s network interface	Suitable for cloud-based infrastructure
1RU 40 cm depth rack solution with space for 2 VB330 modules	1RU 50 cm depth rack solution	Suitable for architectures where virtualization technology is utilized
Dual 10 Gbit/s network connectivity per VB330	Delivered as working system out of the box	Warranty depends on underlying system
Capacity: 12 Gbit/s per VB330 with second input option enabled	Capacity: Up to 50 Gbit/s	Capacity: Will depend on underlying drivers and architecture
24 month standard warranty	24 month standard warranty	
Designed for long lifetime and long product availability	Powerful and future-proof server based platform	License manager / floating licenses

Note that the VB330 software image and VB330 Appliance can be licensed to run any bitrate from 1 Gbit/s to 50 Gbit/s, limited by the underlying network interface cards and server performance.

1.1.3 Software Probe – Functionality

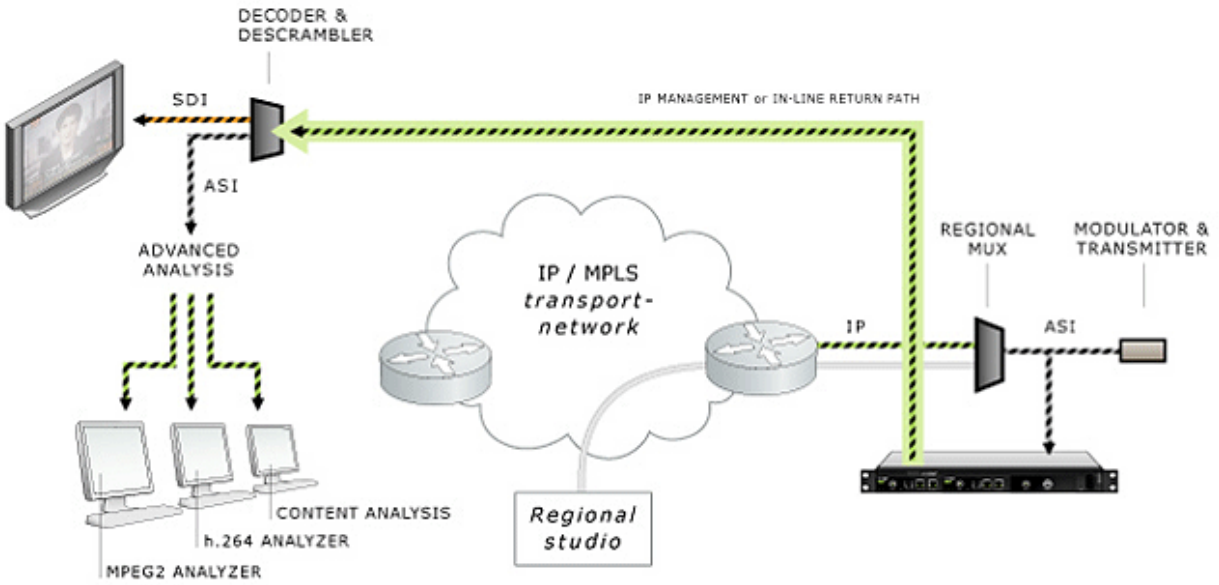
An IP-based network is fully transparent with respect to signal contents quality, provided that the IP packets arrive, and provided that they arrive in time. The Software Probe therefore uses the patented MediaWindow to allow monitoring at-a-glance of packet loss and errors in inter-packet arrival time. 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 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 Software Probe a real-time sniffer capability.

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

The 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.

The Content Extraction and Analysis option adds QoE monitoring, including freeze-frame, MOS and VMAF scoring, closed caption and audio level monitoring, thumbnail and metadata extraction,

as well as Encoder Boundary Point monitoring. The Timeline view includes an analysis capability for an enormously data analysis technology that allows users to play through recorded data in an NLE-style Timeline display to observe correlations and patterns of errors occurring over any time period.

1.2 How to Use This Manual

This User's Manual is valid for software version 6.5 of the VB330-SW 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 stream received as a uni- or multicast or over an SRT connection. When the term multicast is used in this manual, it explicitly refers to a stream arriving over the network as a multicast or unicast, including unicasts that use the SRT protocol.

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 Software Probe once the initial setup has been performed.

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

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

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

F **Appendix: SRT Streams** provides a quick introduction to SRT (Secure Reliable Transport).

G **Appendix: On-line License Activation** outlines the on-line license activation 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 Software Probe.

Note that current version of the User's Manual can be obtained from Sencore ProCare support by emailing procare@sencore.com.

2 PRINCIPLE OF OPERATION

The VB330-SW 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 Software Probe is configured in the operating system web server setup[1].

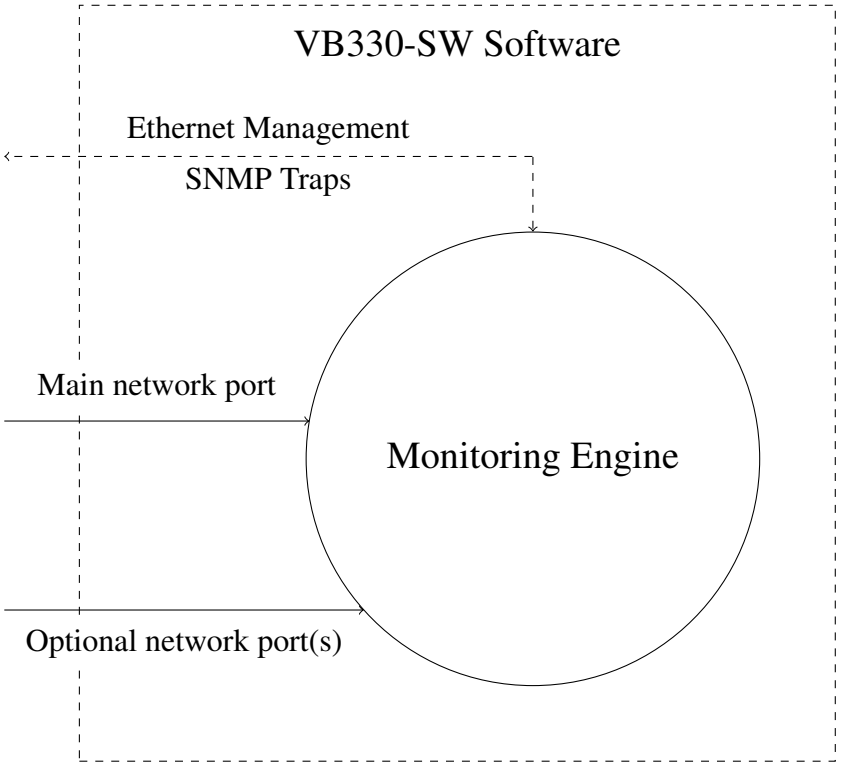


Figure 2.1: The VB330-SW Software – Principle of Operation

A simplified diagram of the alarm handling mechanisms of the 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 Software Probe alarm list and sent as SNMP traps to an external management system.

[1] https://ubuntu.com/server/docs/how-to-configure-nginx

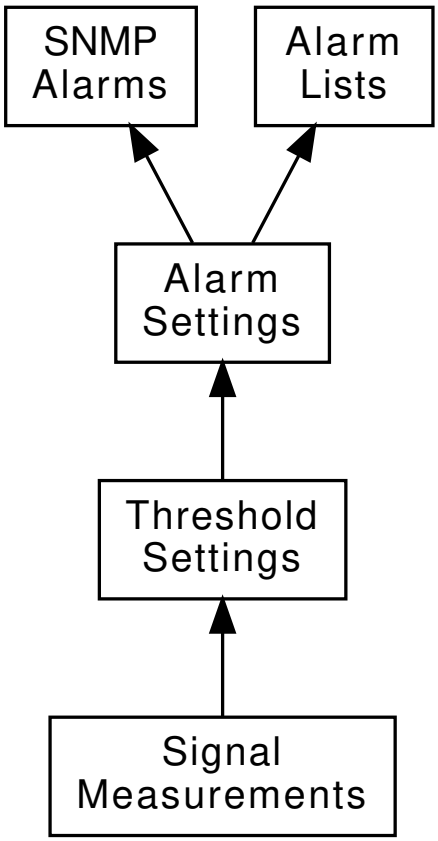


Figure 2.2: Simplified Diagram of the Alarm Handling in the Software Probe

3 INSTALLATION AND INITIAL SETUP

These instructions apply when installing the Software Image. The Appliance Server comes with the software pre-installed, please skip directly to chapter 3.4.

3.1 System Requirements

Please refer to the web site at `https://www.sencore.com/` for the currently recommended hardware. 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.

Supported platforms:

- Ubuntu 24.04 LTS for x86_64

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 or virtual environment matches the requirements and then follow the procedure outlined below.

The VB330 Appliance comes with the software already installed, and you can continue directly to chapter 3.3.

This manual details installation on Ubuntu Server 24.04 LTS. For more details, please refer to the Ubuntu Server installation guide[1].

3.2.1 Obtaining and preparing the installation media

Obtain the latest installation ISO image from Sencore. The same installation media is used for Ubuntu Server and Ubuntu Server Pro installations. If you have an Ubuntu Pro subscription, you can enter the subscription details during the installation procedure.

To install from a USB mass storage device, transfer the downloaded image to the device using a tool such as **dd** (macOS, Unix, Linux), **Rufus**[2] (Windows) or **Etcher**[3] (macOS, Windows, Linux).

[1] `https://ubuntu.com/server/docs/how-to`
[2] `https://rufus.ie/`
[3] `https://etcher.io/`

The Ubuntu documentation[4] has a step-by-step guide on how to create a bootable USB stick, just remember to use the ISO file you just downloaded and not the one linked from the guide.

Once the USB device is prepared, please continue to chapter 3.2.4. For installation in a virtualized environment, please continue to chapter 3.2.2.

3.2.2 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. To reduce the chance of performance-related issues if you nevertheless need to use a virtual network interface, make sure each Software Probe has its own data interface(s).

If using the Software Probe with the multi-stream recording feature, we recommend creating a separate virtual disk and allocating this for recorded data. Mount the disk at `/opt/btech/probe/storage/recordings` and verify that it is identified as *Mounted filesystem* in the **Record – Dashboard** view.

If using the Software Probe with the Timeline feature, you may also want to create a virtual disk for Timeline data using `/opt/btech/probe/storage/database` as the mount point.

To install the software in the virtualized environment, please attach the downloaded ISO image to a virtual DVD-ROM unit and follow the steps in chapter 3.2.4. We recommended **disabling** any 'Easy install', 'Unattended 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.

3.2.3 Obtaining and installing pre-built virtual images

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 below, 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 to chapter 3.3.

[4] `https://ubuntu.com/tutorials/create-a-usb-stick-on-ubuntu`

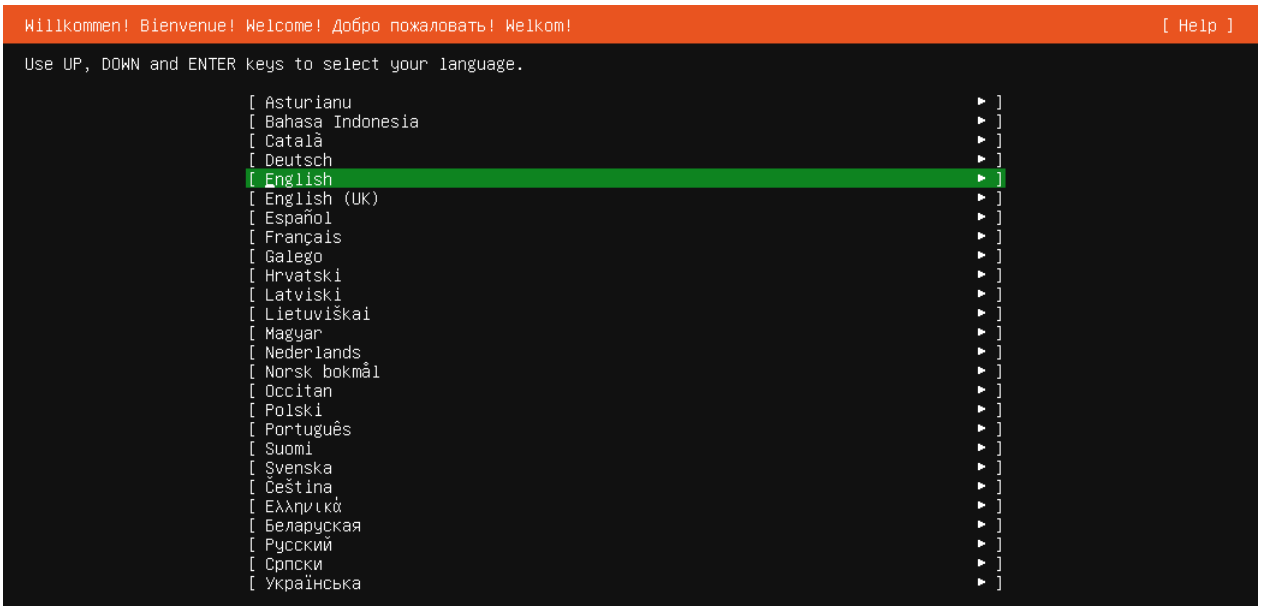


Figure 3.1: Welcoming screen

3.2.4 Installing from provided installation media

The installation media will install Ubuntu Linux Server 24.04 LTS 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.

1. Boot the server and make sure that the primary boot device is set appropriately.

   The installer will run, showing a screen similar to the one depicted in figure 3.1. Some of the steps described in the Ubuntu Server installation guide will be skipped over, with the appropriate settings applied. Please follow the on-screen prompts to install the system:

2. First select the language in which to run the installer, and then which keyboard layout to use to navigate the installer, selecting ‘Done’ to continue.

   Please note that all screenshots and descriptions in this installation manual describe the English user interface, but all settings should be available independent of the language selected.

3. Configure your network devices as needed to reach the internet, see figure 3.2.

   If a proxy is required on your network to reach the internet, provide the address in the next step. The connection will be tested and once ready, select ‘Done’ to continue.

   The installer will be able to run without an internet connection, in this case select ‘Continue without network’.

   Post-installation network configuration can be performed using the **nmtui** utility, please refer to D Appendix: Network configuration for details.

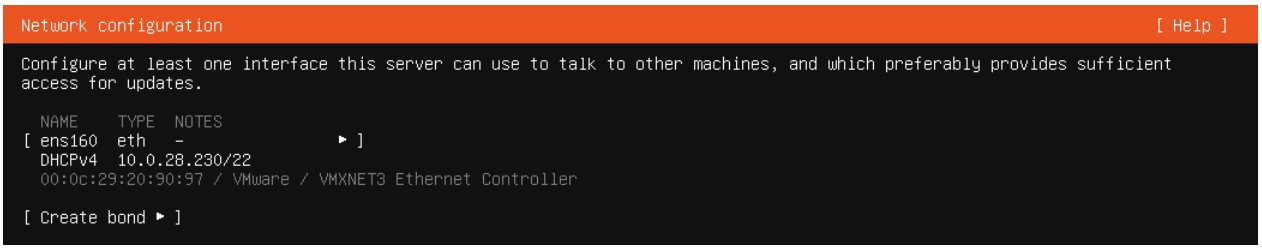


Figure 3.2: Network configuration

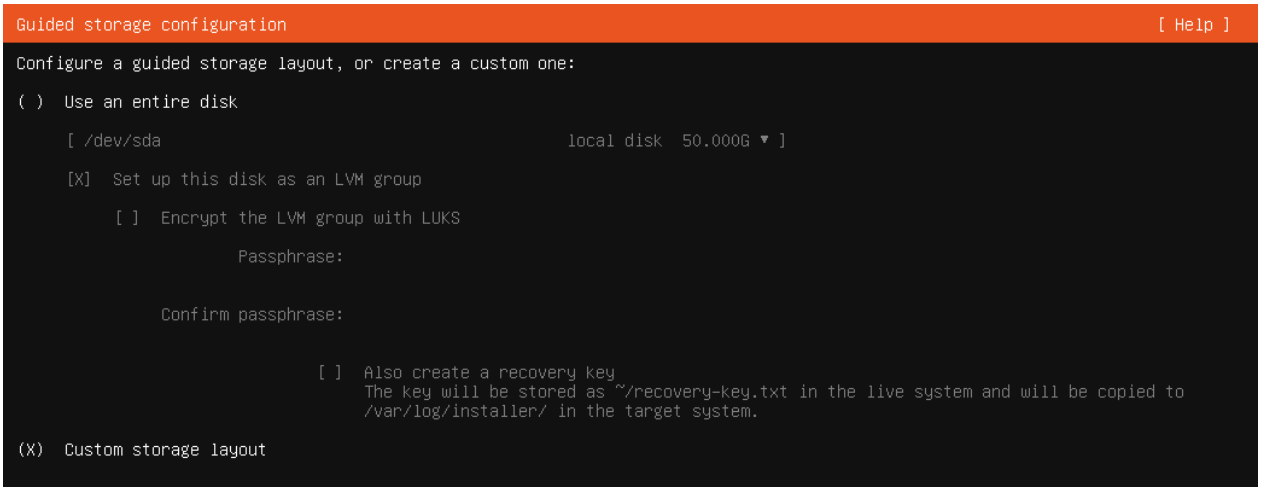


Figure 3.3: Select ‘Custom storage layout’

4. Next, configure the partitioning. We recommend selecting ‘Custom storage layout’ (figure 3.3) and configuring the partitioning manually, as the automatic partitioning often leaves parts of the hard disk unused.

   We recommend not using a swap partition when using the Software Probe, as this can interfere with the real-time operation of the software.

   If you are installing on a system with pre-existing partitions, volumes and/or RAID devices, you will need to select ‘Delete’ on each of these in turn to remove them before continuing. If you are unable to remove specific partitions, highlight the disk itself and select ‘Reformat’ to clear all partitions on the disk. When installing from USB, the USB device will be displayed in this list. It will be marked as ‘in use’ and cannot be deleted.

   - For the drive intended for the OS, select ‘Use As Boot Device’. Compare figure 3.4.
   - Select ‘free space’ on the same device. In the pop-up menu, select ‘Add GPT Partition’ and create a partition of 1G, formatted as xfs at mount point `/boot`. Select ‘Create’ to create the partition, see figure 3.5.
   - Again, select ‘free space’, open the pop-up menu and select ‘Add GPT partition’. Leave the Size field blank (to assign the maximum available), set format to ‘Leave unformatted’ and select ‘Create’ to create the partition, see figure 3.6.

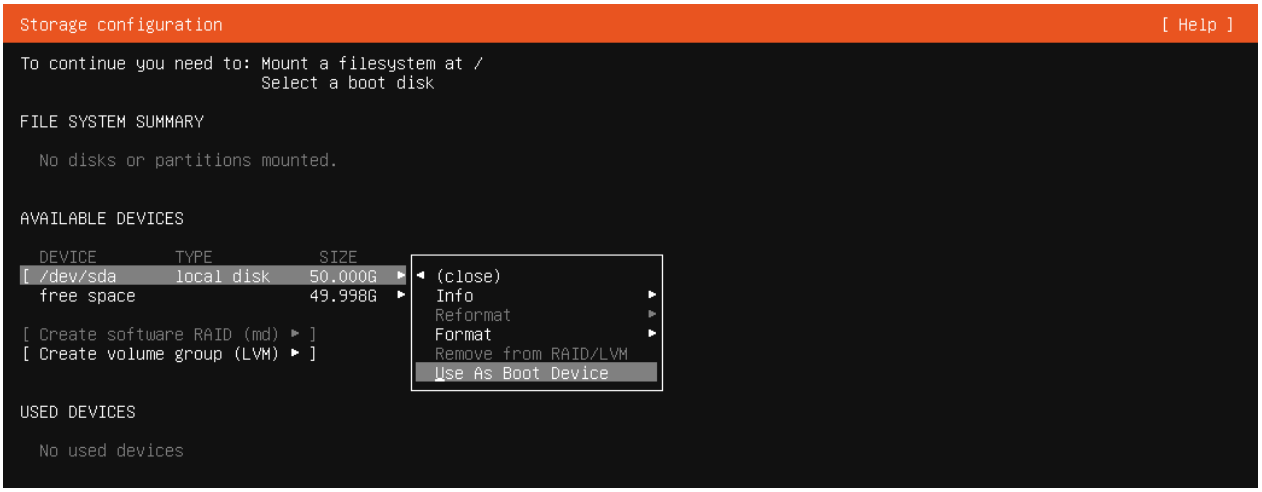


Figure 3.4: Select boot device

Figure 3.5: Create boot partition

Figure 3.6: Create space for volume group

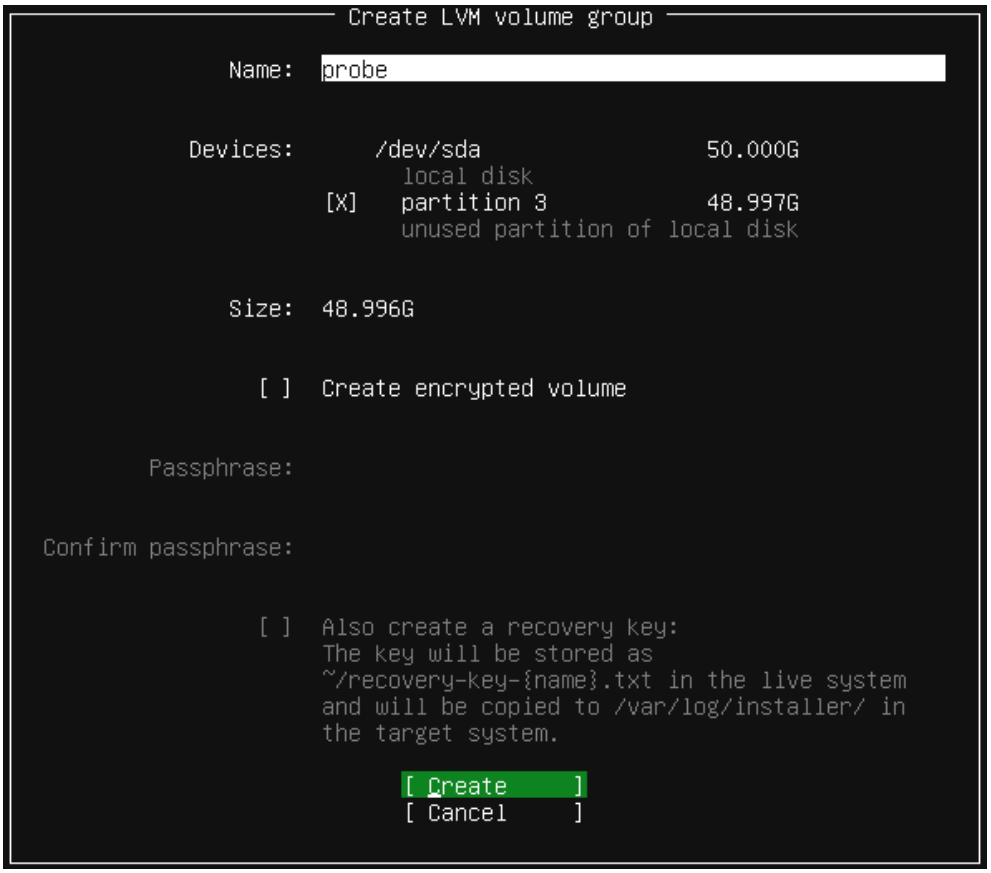


Figure 3.7: Create volume group

- Select ‘Create volume group (LVM)’, selecting the partition created in the previous step. Select ‘Create’ to create the LVM volume group, see figure 3.7.
- Next, determine the amount of storage to set aside for the multi-stream recording feature, and possibly also the Timeline feature, if licensed.

  To create a Timeline storage volume on a pair of disks using RAID mirroring, only set up the multi-stream recording partition now, and instead use the ‘Disk Manager’ option in the administrative interface after finishing the installation.

  Unless using dedicated disks, as a rule of thumb, we can assign half the disk to the system and half to the multi-stream recording feature, or one-third each to the system, multi-stream recording feature and Timeline feature.

  By creating the volumes using logical volumes, they can easily be extended later by adding additional storage space.
- To create the volumes for the multi-stream recording and Timeline features, select ‘free space’ under the ‘NN (new)‘ device (where *NN* is the name you gave it in the previous step) or select the second attached drive as described in 3.2.2. Select ‘Create Logical Volume’, naming it ‘recordings’ for multi-stream recording and ‘database‘ for Timeline.

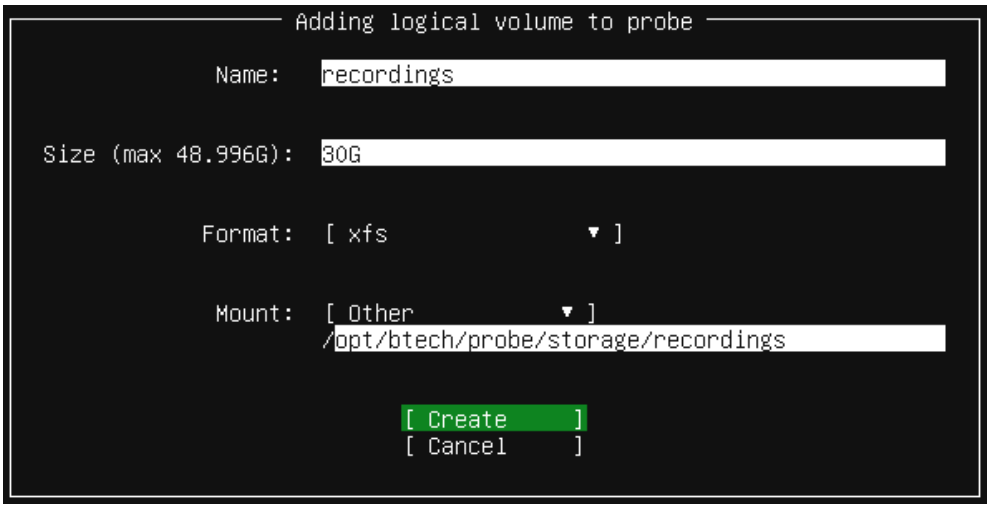


Figure 3.8: Create multi-stream recording volume

Assign the determined available space for the partition if creating a logical volume on the shared disk, or leave the size field blank to assign all available space if creating the volume on the second attached drive.

Set the format to 'xfs' and set the mount point by choosing 'Other' and selecting `/opt/btech/probe/storage/recordings` for multi-stream recording and `/opt/btech/probe/storage/database` for Timeline. The configuration should look similar to figure 3.8. Select 'Create' to create the logical volume.

- Select 'free space' under the 'NN (new)' device (where *NN* is the name you gave it in the previous step). Select 'Create Logical Volume'. Name it 'root', leaving the size field blank (to assign the maximum available), and setting format to 'xfs'.

  The configuration should look similar to figure 3.9. Select 'Create' to create the logical volume.

- The storage configuration should look similar to figure 3.10. Accept it by selecting 'Done'.

  Confirm that you want to apply the changes by selecting 'Continue'.

5. Next, create the administrative user and password, see figure 3.11. This is used later to log in to the administrative interface.

6. If you have an Ubuntu Pro subscription, enter it here, as seen in figure 3.12. Otherwise, select 'Skip for now'.

   To attach an Ubuntu Pro subscription later, enter `pro attach` at the command line and follow the on-screen prompts.

7. To be able to log in remotely to the system, select 'Install OpenSSH server' in the SSH configuration screen depicted in figure 3.13.

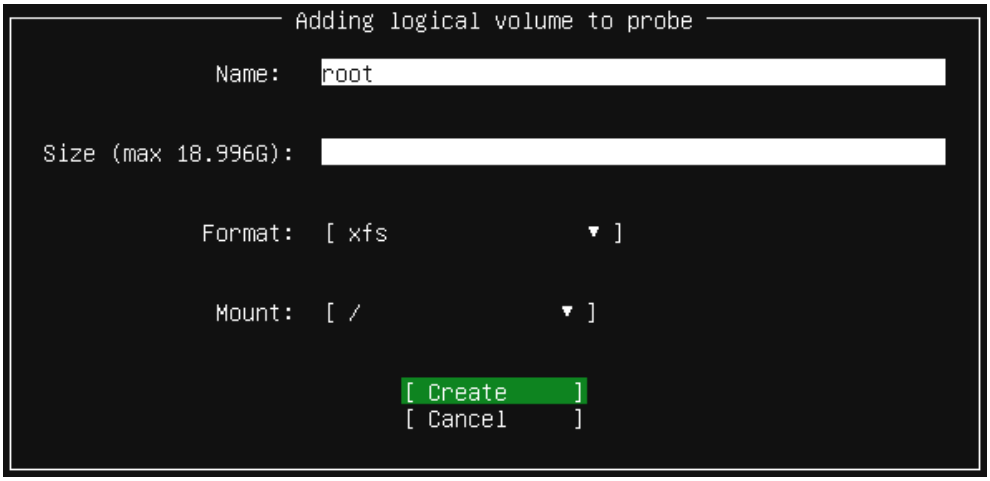


Figure 3.9: Create root volume

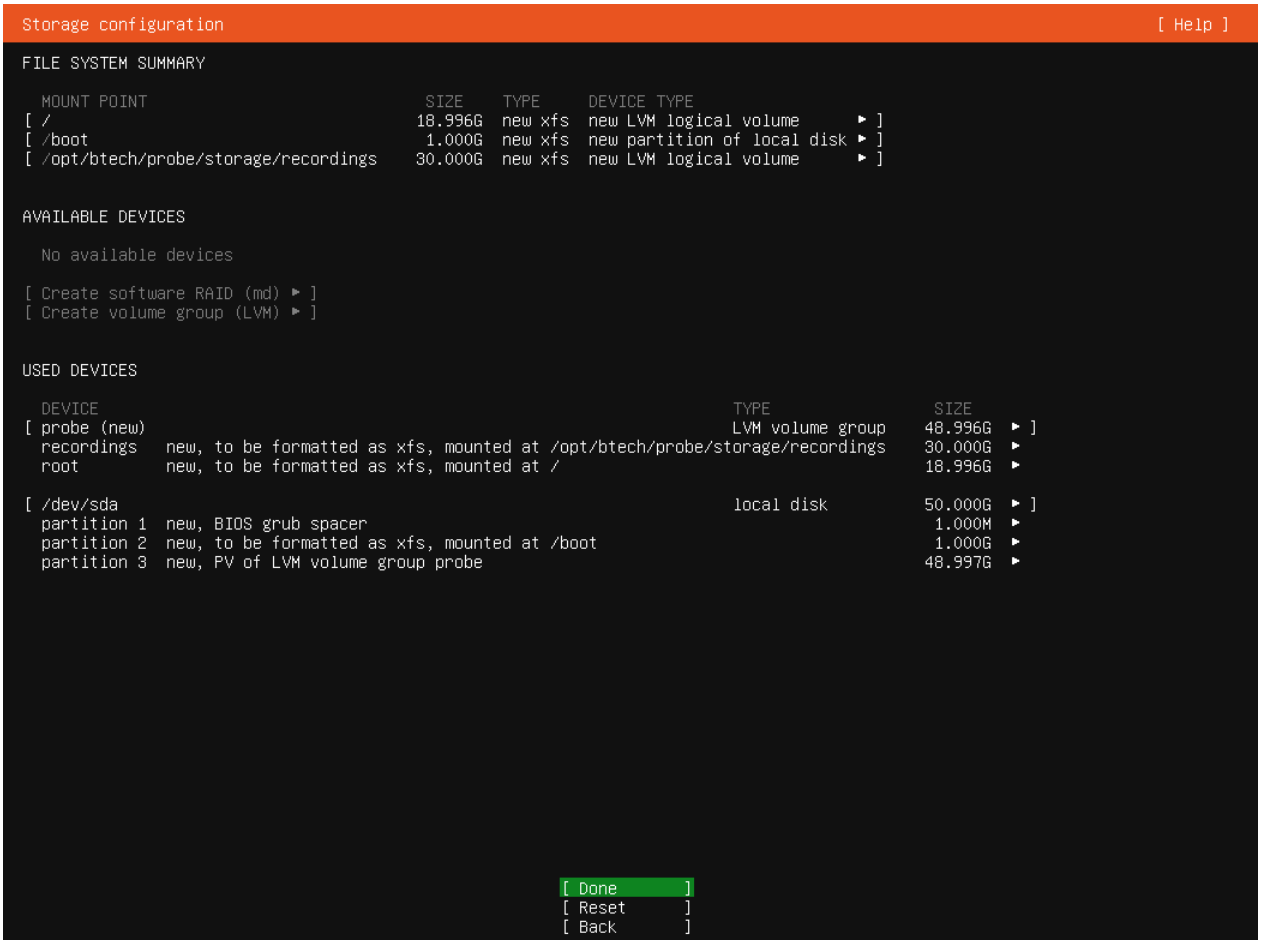


Figure 3.10: Finishing partitioning setup

Figure 3.11: Create a log-in profile

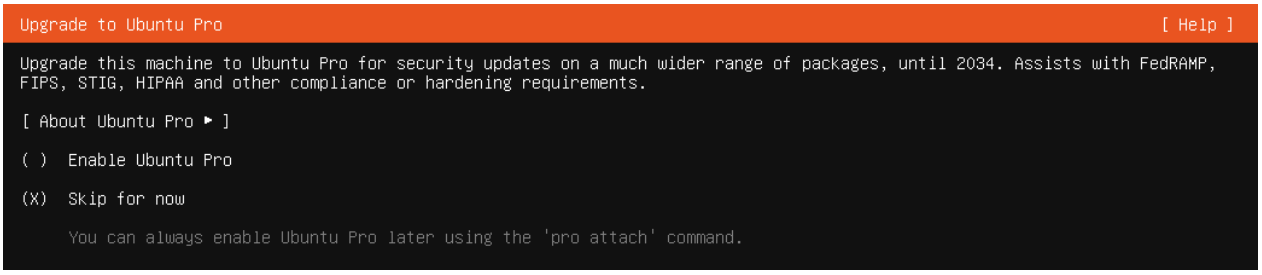


Figure 3.12: Enable Ubuntu Pro

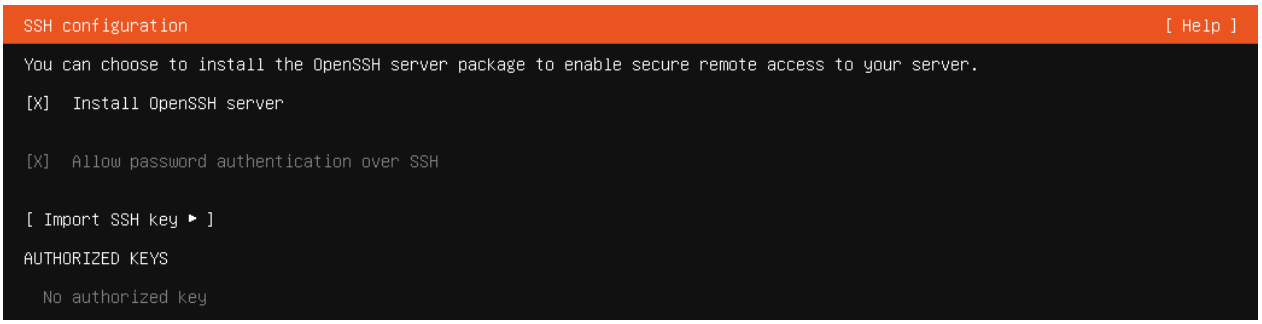


Figure 3.13: SSH configuration

You can import SSH keys to enable password-less installation using the ‘Import SSH key’ feature if the system has internet connectivity and you have an account with any of the supported services. Please note that you will still need to have set a password to use the Cockpit administrative interface.

8. The installation will now start. Once finished, there will be a button at the bottom of the screen saying ‘Reboot Now’. Remove the installation media and ensure that the system boots up properly.

   The default installation does not provide any graphical user interface environment, and only a minimal set of command-line tools. Please refer to the Ubuntu Server documentation about how to unminimize it if necessary.

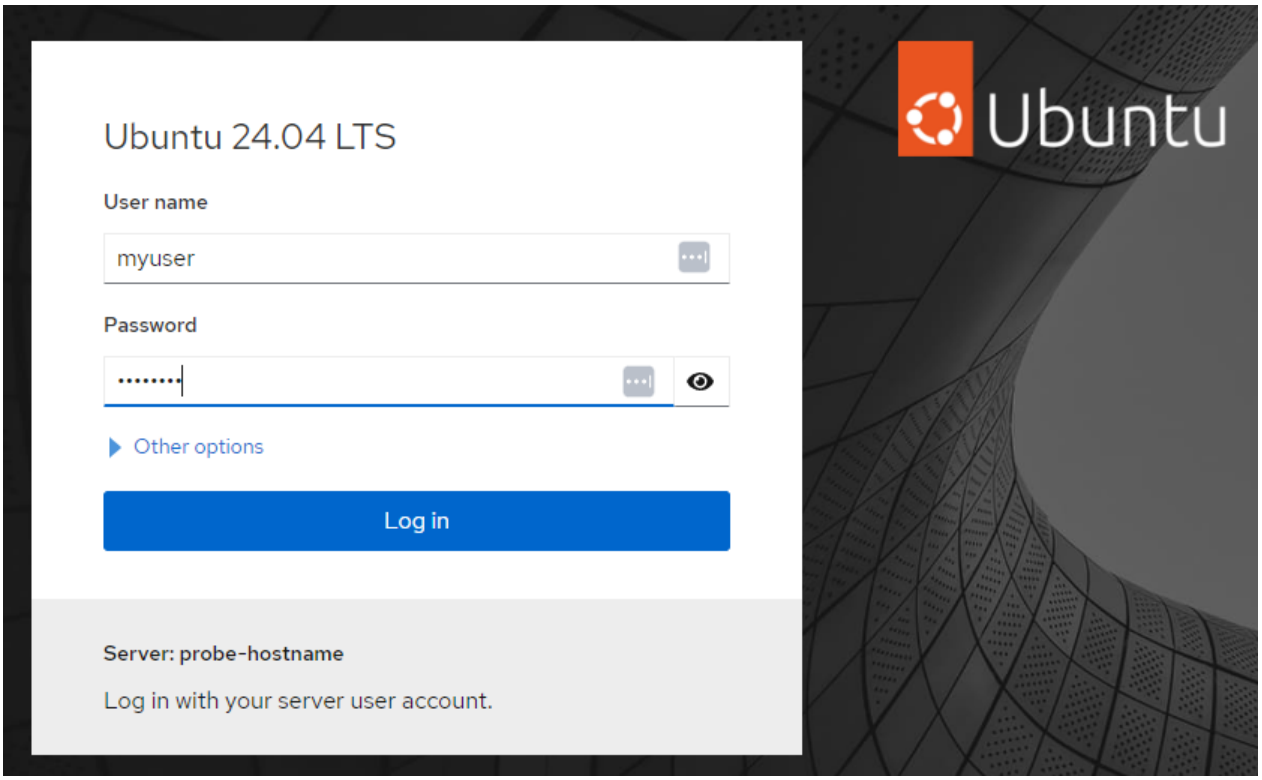


Figure 3.14: Cockpit administrative interface

We do not recommend running a graphical user interface environment on a system running the Software Probe.

3.3 Maintaining the underlying Operating System

The software installed on the system is using Ubuntu Linux Server as its base system. For information on how to maintain the operating system, including how to update it to install security patches, please refer to the Ubuntu Server system documentation.

An overview of Ubuntu Server documentation can be found at `https://ubuntu.com/server/docs/how-to`

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.

When logging in to the pre-built images and the VB330 Appliance, the default password for the **admin** user is **elvis**. The same password is used for logging in remotely using Secure Shell (ssh) and the Cockpit administrative interface.

1. Launch a web browser application on the management system. One of the following browsers are recommended:

   - Google Chrome
   - Mozilla Firefox
   - Microsoft Edge
   - Apple Safari

2. 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.

   If you get a HTTPS certificate warning, just accept it.

   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 Cockpit administrative interface should be displayed inside the browser. Cockpit is password-protected and uses the system accounts for logging in. The page displayed should look similar to figure 3.14.

4. Most operations require that you obtain administrative access by clicking the button at the top of the screen after having logged in. When using the command shell (terminal), use the **sudo** command to run programs with administrative access.

   If you have enabled the root account by setting a password for it, it will automatically have administrative access.

5. If this is a new server, and you need to obtain license keys for the purchased products, please contact your sales representative.

6. The Software Probe is not enabled by default on the newly installed server. To enable it, click the icon next to its name. This will open a detailed view with display details of the installed software, such as the installed version. 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** and wait for it to finish. An activation message will be shown upon completion. If successful, the 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.

To return to the Cockpit administrative interface to make changes, open the **About — License** tab in the Software Probe user interface and click the link labeled **Manage server**.

It is **strongly recommended** that the system time is configured to be synchronized against an external NTP server. Please refer to E 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 Software Probe web based management interface, verify the following:

- Verify that the client machine and the 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 Software Probe.
- Make sure that the IP address of the gateway and the network interface are not the same.
- Verify that the appropriate Ethernet link indicators of the PC and the 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 nginx
  ```

  on the server's command line. If it is not running properly, check the system logs for hints by typing

  ```
  journalctl -u nginx
  ```

- If you can reach the Cockpit administrative interface, but the 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 using the Cockpit administrative interface.

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.

3.6.1 Upgrading by Re-Installing the System

Sometimes it is necessary to upgrade the system by doing a full reinstall, for instance when upgrading to a new major operating system release. Please follow these steps to perform a full re-install:

1. Backup the system configuration (**Data — Configuration — Full configuration**).
2. If using a classic license key, you can export it using **About — License — Export current license and software maintenance keys**.

   If using an on-line activated license and installing on the same server, the license will be transferred automatically. If transferring to a new server, you should release the license using **About — License — Manage license activation** before deactivating the old system.
3. Possibly back up the system network configuration by logging in to the machine and copying any files matching the wildcard `/etc/netplan/*.yaml` (Ubuntu 24.04), `/etc/NetworkManager/system-connections/*.nmconnection` (Rocky Linux 9 and Red Hat Enterprise Linux 9) or `/etc/sysconfig/network-scripts/ifcfg-*` (CentOS 7 or Red Hat Enterprise Linux 7) to a safe location (off the system).
4. Back up any storage data needed (see below).
5. Re-install the system as described above.
6. Activate the software and import or re-enter the license key, using the **Data — Configuration** and **About — License** views, respectively.
7. Import the configuration from **Data — Configuration — Import configuration XML**.
8. Import any network configuration if backed up as described above. Netplan on Ubuntu will not read network configuration files created by Red Hat Enterprise Linux, Rocky Linux or CentOS Linux.

Please note that classic license keys are no longer supported. Please see section 5.15.2 About — License on how to obtain the current hardware key and contact your sales representative to obtain a new license key before moving to a newer operating system.

Keeping Timeline Data and Recordings

If you are using the **Timeline** or **Record** features with permanent disks and you wish to keep the stored data, you must take care to avoid overwriting or clearing the associated storage if installing the new operating system on the same server.

Timeline data is stored in the `/opt/btech/probe/storage/data` (CentOS, Rocky and Red Hat systems) or `/opt/btech/probe/storage/database` (Ubuntu systems). Recordings are stored in `/opt/btech/probe/storage/recordings`.

If these directories are located on one or more separate disks or partitions, make a note of where they are mounted and make sure to keep these partitions intact when creating the new operating system partitions. Mount the partitions in the same locations on the new system to keep the associated data. The Software Probe will automatically detect the old data and make it available.

If any of the directories are located on the root file system, you will need to back the data up and restore it after re-installing. If you are moving the system to a new server, you must make provisions for copying or moving the data to the new server.

Copying the **Timeline** data from a system running CentOS Linux 7, Rocky Linux 9 or Red Hat Enterprise Linux 7 or 9 to a system using Ubuntu 24.04 is *not* supported at this time.

3.6.2 Upgrading From Version 6.4.0 or later

Please refer to chapter 5.14.2 and I Appendix: Software Upload for details on how to install the upgrade image.

3.6.3 Upgrading From Version 6.3.0 or earlier

Software Probe release 6.5 no longer supports the operating system used for these releases. Please see chapter 3.6.1 for details on how to re-install the system.

3.7 Upgrading To a Maintenance Release

Please refer to chapter 5.14.2 and I Appendix: Software Upload for details on how to upgrade to maintenance releases.

If the system has access to software updates over the internet, the Software Probe software will be upgraded along with the Ubuntu OS software. On-line upgrades will always install from the same major software release (i.e. 6.5), upgrades to a new major software release must be installed manually.

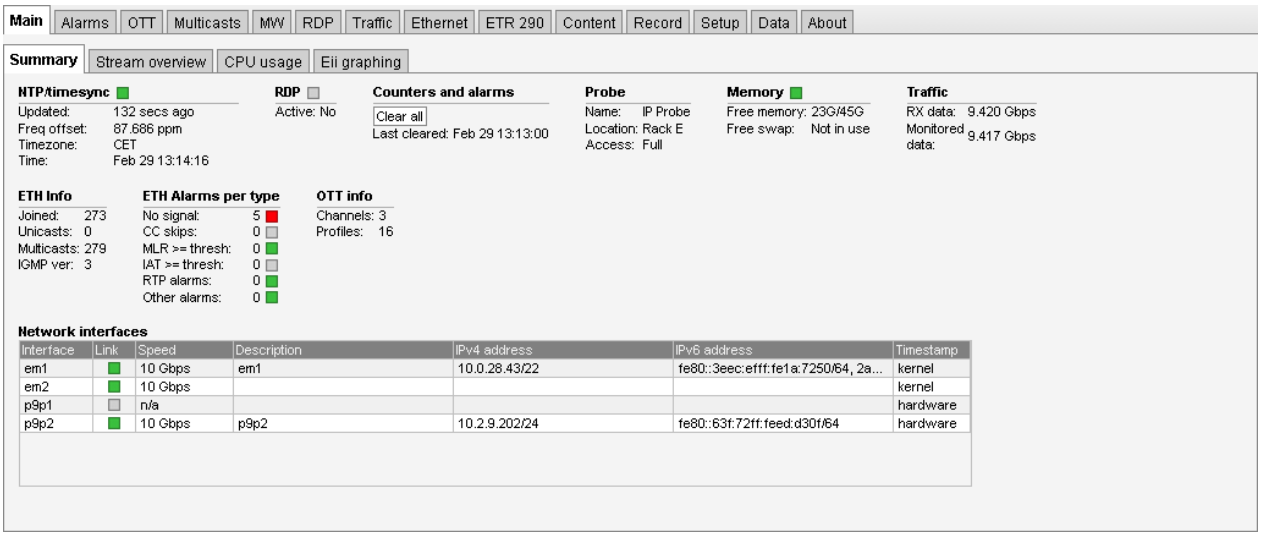


Figure 3.15: The VB330-SW Graphical User Interface

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
- Apple Safari

The default management view should look similar to figure 3.15. If you have problems accessing the user interface, refer to chapter 3.5 for troubleshooting.

3.9 Accessing the administrative interface

To return to the administrative interface after activating the Software Probe, you can either navigate to the **About — License** view and follow the **Manage sever** link, or navigate your web browser to the address `https://<IP>/admin`, where `<IP>` is the IP address (or host name, if using DNS) of the server.

3.10 Deactivating

To deactivate Software Probe, you must first access the administrative interface (see the previous section) and make sure that it is not set to the default. Expand the product details heading and click the **Remove as default** button.

Once this is done, access the 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 E Appendix: Enabling NTP time synchronization for further details on how to configure the date and time.
3. If access control is required, first log in as the **admin** user using the **Setup — Login** view, and then define users and password in the **Setup — Security** view.

   Note: it is important to read the instructions in the associated section of this manual, see chapters 5.13.4 and 5.13.9.

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

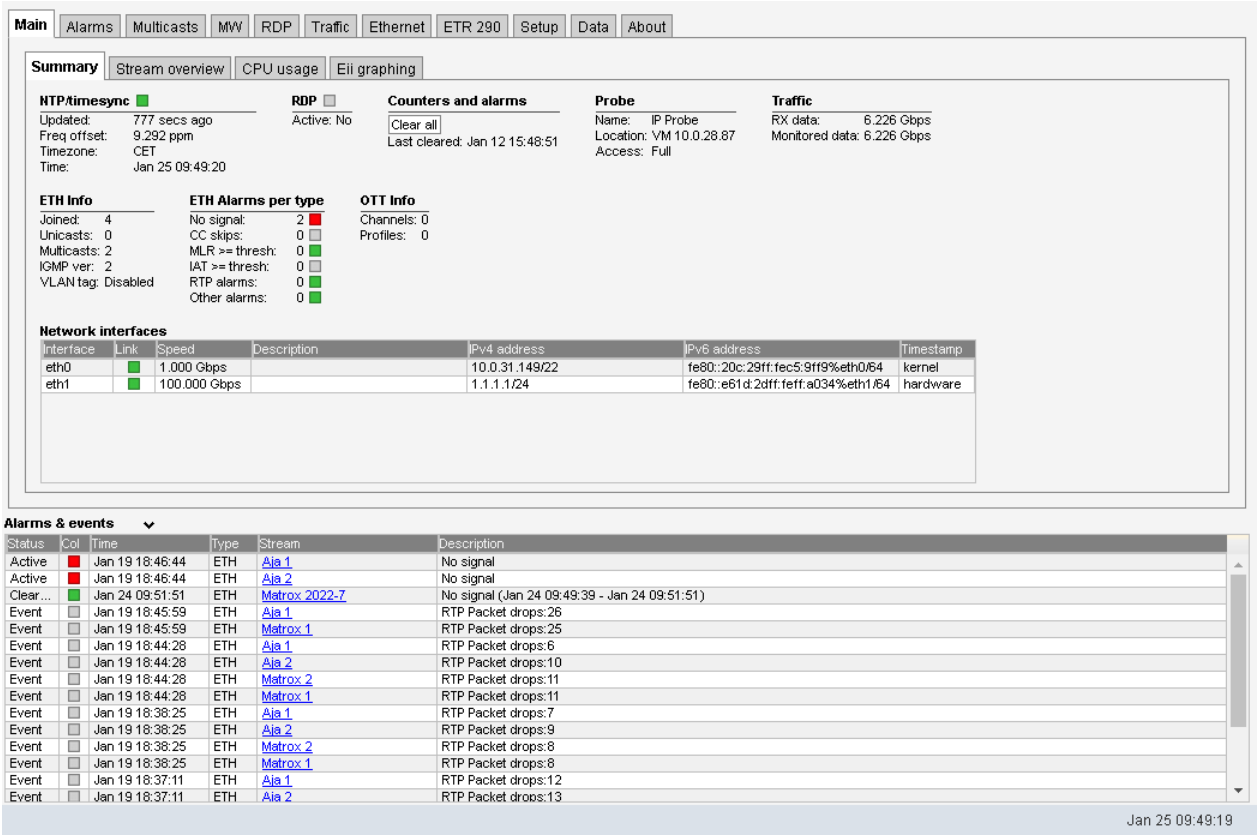
By default the streams configured in the probe will be set up to use the ETR 290 threshold named **Default**. This has the most important alarms enabled but have been adjusted to match real world systems and only alarm on more severe problems. The threshold named **ETSI TR 101 290** is based on the ETSI 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 SOFTWARE PROBE GRAPHICAL USER INTERFACE



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

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- 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 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 is by default hidden, and can be displayed and hidden again by clicking the **Toggle** link, which is displayed as an arrow head.

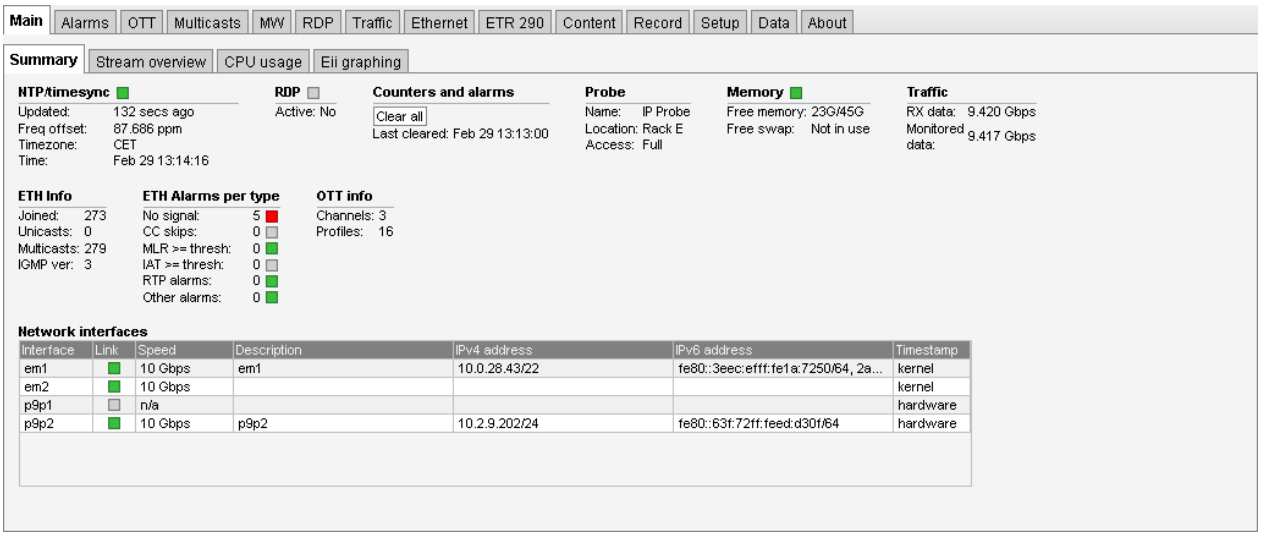
The web interface has been designed to be resizable in both vertical and horizontal directions with a minimum screen resolution of 1280×800 pixels.

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, and to use Chrony as the network time client. 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.

[1] `https://ubuntu.com/server/docs/how-to`

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	
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 — Security** view.

Memory	
Free memory:	The available free memory.
Free swap:	The available free swap memory. We recommend not using a swap partition when using the Software Probe, as this can interfere with the real-time operation of the software. If swap is disabled “Not in use” is displayed here.

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 enabled IGMPv3 in the **Setup — Params** view.

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

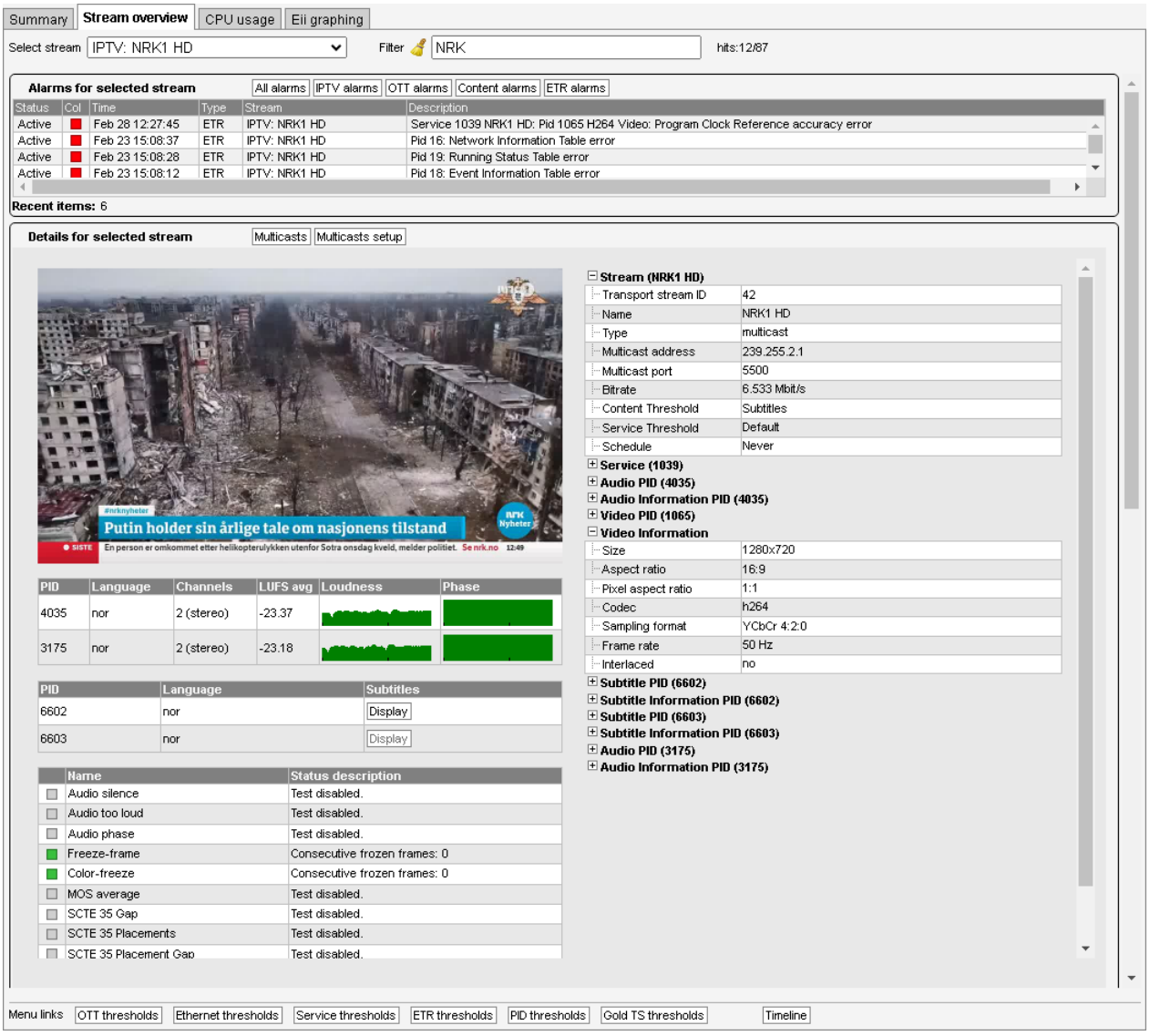
OTT info	
Channels:	The number of enabled OTT channels.
Profiles:	The total number of profiles in the enabled OTT channels.

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.
Speed:	Shows the current bitrate for the interface.
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.

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

5.1.2 Main — Stream overview

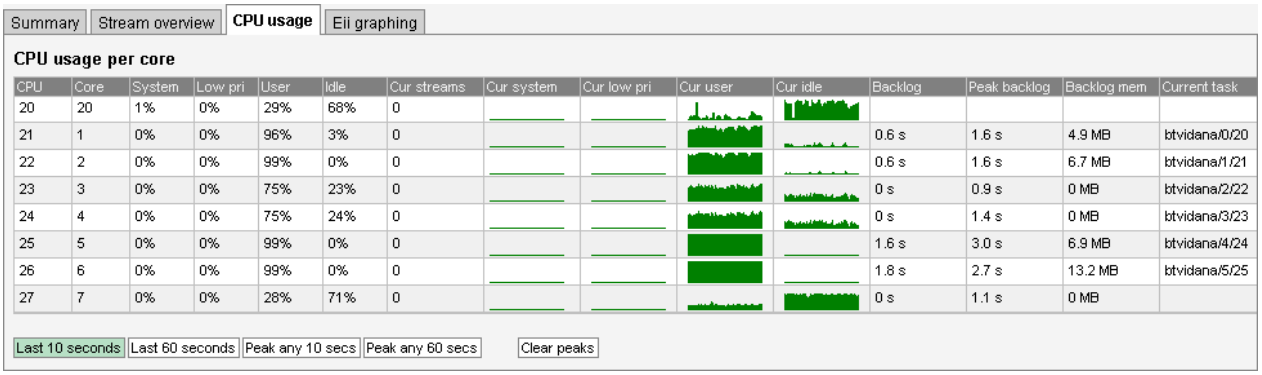


The **Stream overview** offers an easy way to get an overview of the status of a single channel by collecting the relevant information views from various parts of the probe and displaying them all in one place. This page is opened when clicking a channel alarm in any of the alarm list. When using the probe in conjunction with a the VideoBRIDGE Controller, this page is also displayed when clicking on a stream mentioned in the VBC user interface.

Use the **Select stream** drop-down to select a stream to display. By entering a stream name in the **Filter** box, only streams matching this filter will be show in the drop-down.

The list of active alarms for the selected channel is displayed on top, followed by different information depending on the kind of the stream selected. Please refer to the **Multicasts**, **ETR 290** and **OTT** chapters for detailed documentation on the various information views.

5.1.3 Main — CPU usage



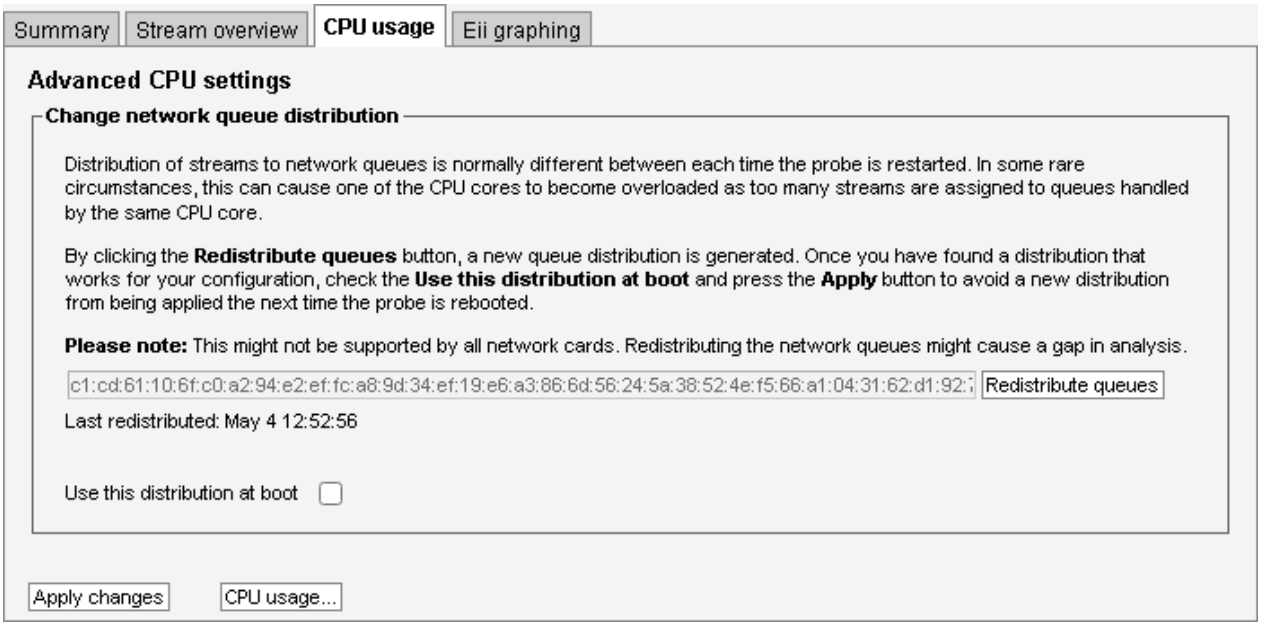
The **CPU usage** view is meant for troubleshooting performance issues in case of excessively high traffic load.

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 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. Click the **Advanced** button to open the **Advanced CPU settings** view.

The length of the queues for multicast video analysis are displayed in the **Backlog** column, with the highest recorded value in the **Peak backlog** column. If these values keep growing, the probe is not able to keep up with the amount of data it has been set to monitor, and will eventually start dropping data to catch up again. Please refer to appendix B.5 for more details. Additionally, the currently running process (at the time of update) on each CPU core is displayed in the **Current task** column.

5.1.3.1 Advanced CPU settings



The **Advanced CPU settings** view can be opened by clicking the **Advanced** button in the **Main — CPU usage** view, and is meant for manually overriding the automatic CPU allocation settings.

During normal operation, incoming network streams are allocated automatically to different CPU cores. The RSS (Receiving Side Scaling) hash key is randomized by the operating system at boot, and in some rare circumstances, this can cause one or more of the CPU cores to have too many streams assigned to the queues handled by these CPU cores.

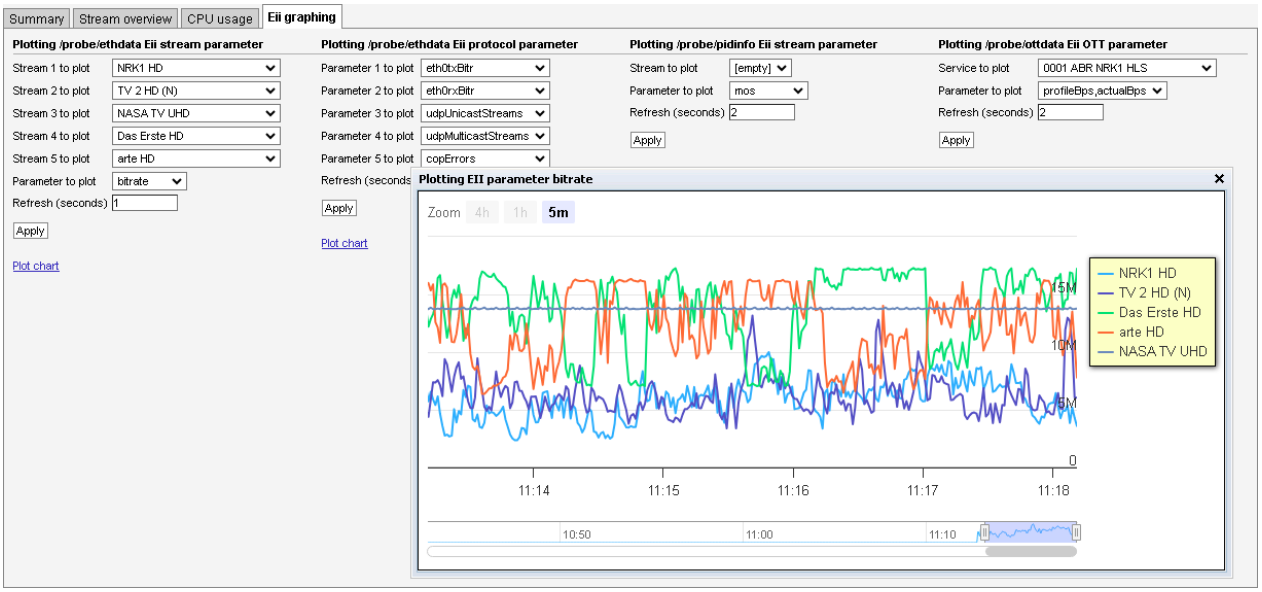
By clicking the **Redistribute queues** button, a new random RSS hash key is generated and streams are redistributed accordingly. Once you have found a hash key that works for your current configuration, you can check **Use this distribution at boot** and click **Apply changes** to configure the Software Probe to use this RSS hash key on start.

Some network card drivers do not support changing this value.

Changing the RSS hash key may cause gaps in the analysis.

Click the **CPU usage** button to return to the **Main — CPU usage** 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** drop-down.

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.

Pidinfo Eii stream parameter

Using the **Pidinfo Eii stream parameter** plot, it is possible to plot content analysis results for any streams that have QoE monitoring enabled. Select the channel in the **Stream to plot** drop-down and the parameter in the **Parameter to plot** drop-down.

Only streams which have QoE enabled are listed in the Stream drop-down.

Pidinfo Eii parameters	
mos	Composite MOS value, on the scale 1–5
blocking	Detected picture blockiness, scaled 0–1, where 1 is the best (no blocking).
blurriness	Detected picture blurriness, scaled 0–1, where 1 is the best (no blurring).
noisiness	Detected picture noisiness, scaled 0–1, where 1 is the best (no noise).
brightness	Detected picture brightness, scaled 0–1, where 0 is dark and 1 is bright.
contrast	Detected picture contrast, scaled 0–1.

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** drop-down.

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 segment (bits per second)
chunkDur:	Last segment length (seconds)
firstByte:	Time to first byte (milliseconds)
downloadDur:	Time to download segment (seconds)
chunkSize:	Size of downloaded segment (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 for further details.

5.2 Alarms

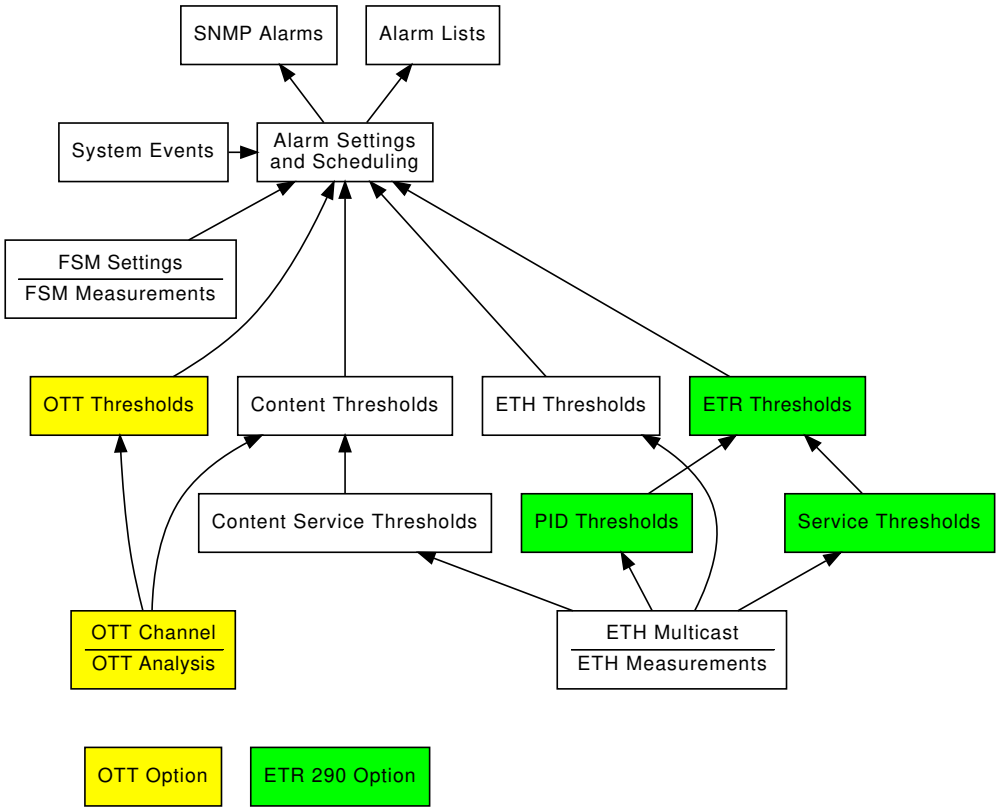


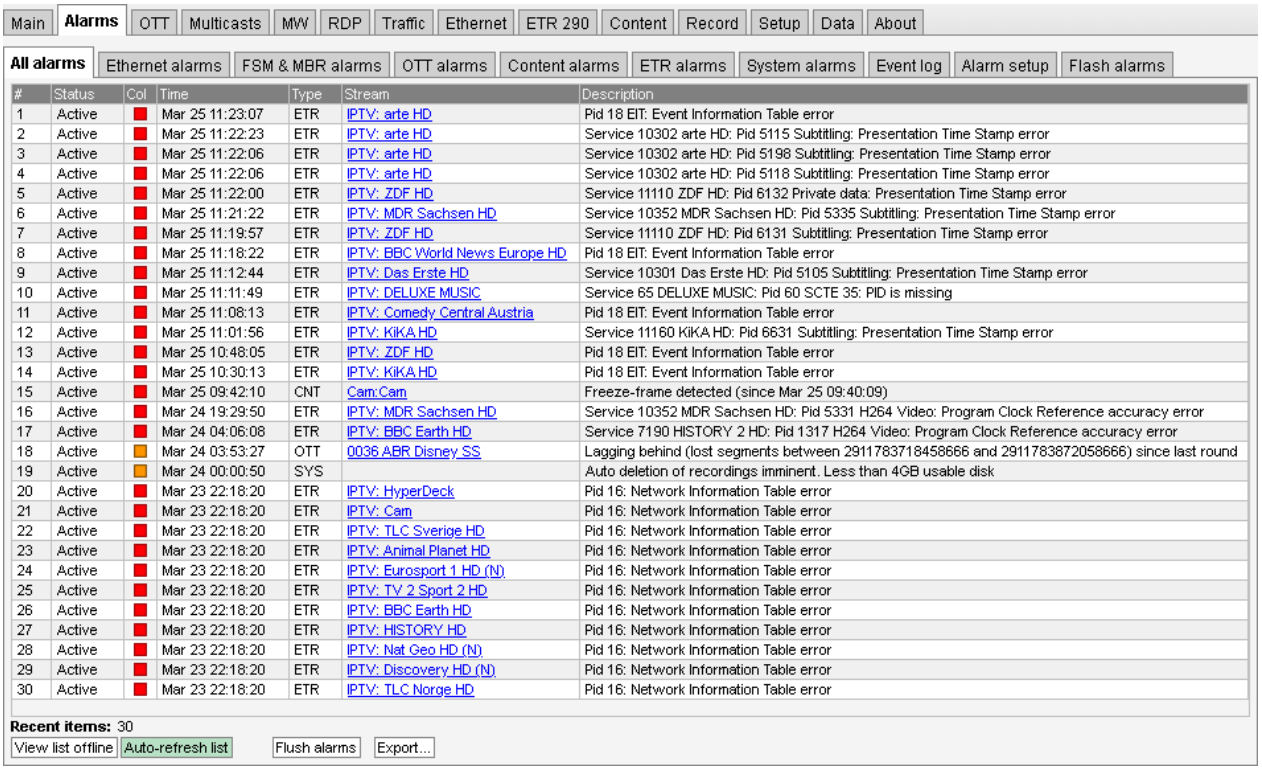
Figure 5.1: Alarm handling in the Software Probe.

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

The 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. If configured to do so, 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 VideoBRIDGE Controller.

The 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)	10000 alarms
Full Service Monitoring and Microbitrate (FSM)	100 alarms
Over The Top Television (OTT)	2500 alarms
ETSI TR 101 290 Analysis (ETR)	10000 alarms
Content (CNT)	2500 alarms
System alarms (SYS)	2500 alarms
Event log (LOG)	2500 events

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.

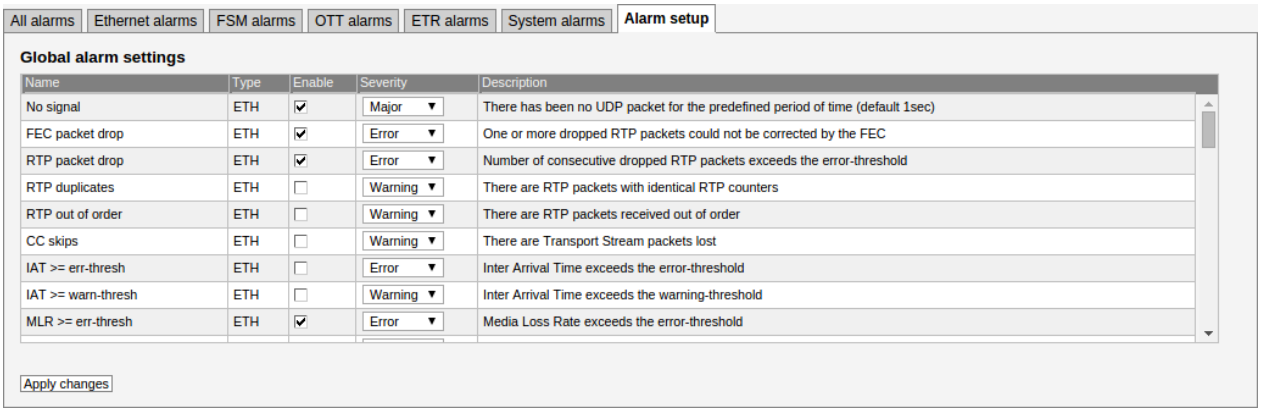
Clicking the **View list offline** button gives the user the opportunity to view the complete alarms and events list. By clicking one of the blue information icons leftmost in the offline list, a detailed alarm description can be viewed. The search field in the upper right corner of the view allows the 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.

Clicking the blue link text of any alarm in the alarm list opens the **Main — Stream overview** for the channel in the alarm. 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. 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 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 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
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 (Full service monitoring & Microbitrate) alarms		
Full service monitoring:	No reply was obtained within timeout period for the configured FSM service	Default: Enabled, severity Major
Microbitrate bursting:	Raised if the bitrate of the user-interval exceeds the **Burst threshold** setting	Default: Enabled, severity Warning
Microbitrate excessive ES bursting:	Raised whenever the bitrate of the user-interval exceeds the **Burst threshold** for **ES threshold** number of seconds during the last **ES Alarm window** seconds	Default: Enabled, severity Error
Full service monitoring:	No reply was obtained within timeout period for the configured FSM service	Default: Enabled, severity Major

LOG (Event log)		
[Log config events]:	Log configuration related events, such as config uploads	Default: Enabled, severity OK
[Log startup events]:	Log startup related events (currently not used)	Default: Enabled, severity OK
[Log stream events]:	Log stream related events, such as manual resets of monitoring for ETR	Default: Enabled, severity OK
[Log other events]:	Log other events (currently not used)	Default: Enabled, severity OK

CNT (Content) alarms		
Freeze-frame detected:	The service has frozen frames	Default: Enabled, severity Major
Color-freeze detected:	The service has frozen in one color	Default: Enabled, severity Major
SCTE 35 event gap:	The service has not received SCTE 35 or SCTE 104 data for longer than the threshold	Default: Enabled, severity Error

Too few SCTE 35 placement opportunities:	The service has not had enough placement opportunities signaled in SCTE 35 or SCTE 104 for the previous clock hour	Default: Enabled, severity Error
SCTE 35 placement gap:	The service has not had SCTE 35 or SCTE 104 placement opportunities for longer than the threshold	Default: Enabled, severity Error
SCTE 35 end event without start:	A SCTE 35 or SCTE 104 end segmentation descriptor message was received in a Time signal event, without the corresponding start segmentation descriptor message having been received.	Default: Enabled, severity Error
SCTE 35 start event without end:	A SCTE 35 or SCTE 104 start segmentation descriptor message was received in a Time signal event, without the corresponding end segmentation descriptor message being received within the defined timeout.	Default: Enabled, severity Error
SCTE 35 minimum pre-roll time:	A SCTE 35 event is received too close to the splice time.	Default: Enabled, severity Error
SCTE 35 maximum pre-roll time:	A SCTE 35 event is received too far from the splice time.	Default: Enabled, severity Error
Audio silence detected:	The service has silent audio tracks	Default: Enabled, severity Major
Audio too loud detected:	The service has too loud audio tracks	Default: Enabled, severity Major
Audio out of phase detected:	The service has audio tracks that are out of phase	Default: Enabled, severity Major
EBP PTS gap:	The PTS gap between two subsequent EBPs is outside of the min and max thresholds	Default: Enabled, severity Major
EBP group PTS skew:	The PTS skew between the stream's and the group reference's EBP is outside of the threshold	Default: Enabled, severity Major
IDR PTS gap:	The PTS gap between two subsequent IDR frames is outside of the min and max thresholds	Default: Enabled, severity Major

IDR group PTS skew:	The PTS skew between the stream's and the group reference's IDR frames is outside of the threshold	Default: Enabled, severity Major
EBP and IDR PTS unaligned:	The difference between the IDR frame and EBP PTSs is outside of the threshold	Default: Enabled, severity Major
MOS below threshold:	The average MOS for the service is below the configured threshold	Default: Enabled, severity Major
Wrong DAR:	The stream has wrong Display Aspect Ratio	Default: Enabled, severity Major
Wrong PAR:	The stream has wrong Pixel Aspect Ratio	Default: Enabled, severity Major
Caption service missing:	The service has less caption services than specified in the threshold	Default: Enabled, severity Major
Bad caption quality:	The received caption data was corrupt	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
Missing 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
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
Modulation:	Unexpected modulation parameter:	Default: Enabled, severity Major

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

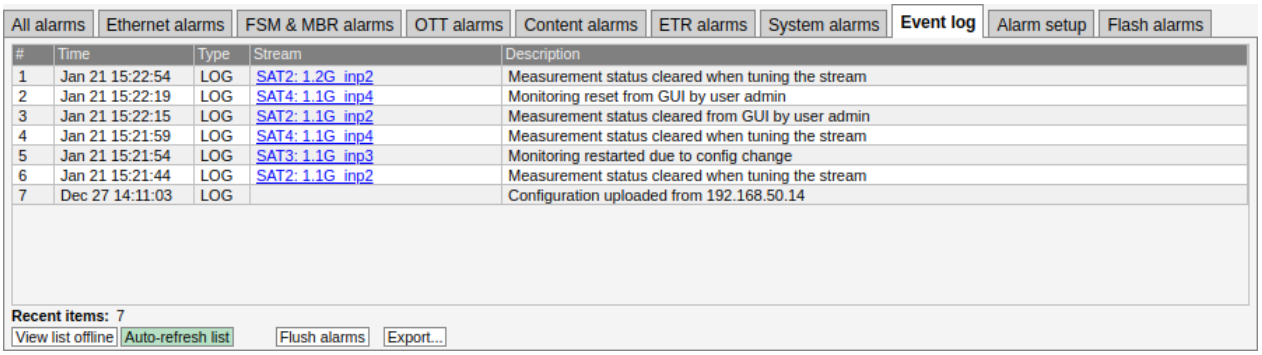
There is a multitude of system alarms which are reported under the above headings and the configuration applies to them as a group. See section 5.2.5 for a partial list of possible system alarms.

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
Wrong profile type	The channel has profiles of a different type 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 segment 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 segment 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
Mis-alignment detected:	One or more profiles are out of visual alignment	Default: Enabled, severity Major
Manifest parse error:	Failed to parse manifest file. Invalid format	Default: Enabled, severity Major
Segment error:	Expected segment missing from manifest	Default: Enabled, severity Major
Unknown manifest:	Cannot recognize manifest XML format	Default: Enabled, severity Fatal

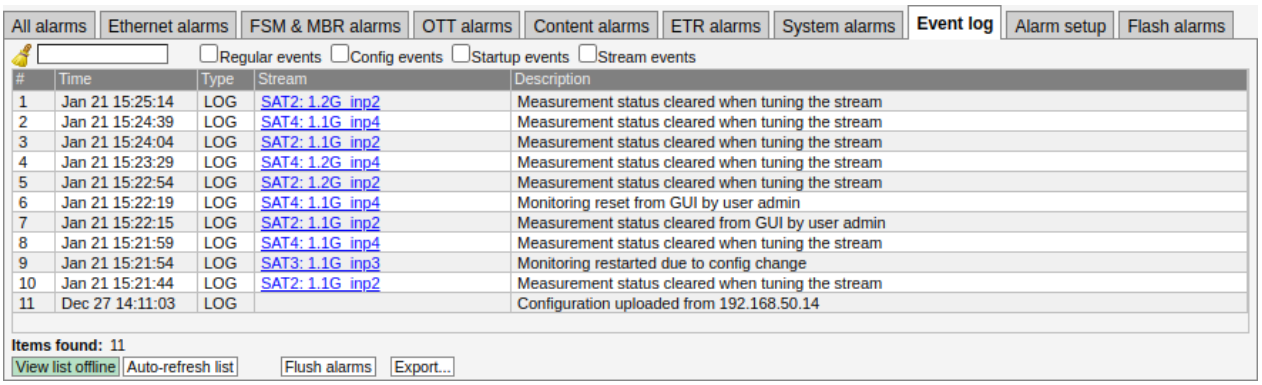
5.2.3 Alarms — Event log



The Event log displays the events logged by the probe. These are events that happen which are not errors in any way, such as configuration uploads or logging of monitoring resets for ETR streams.

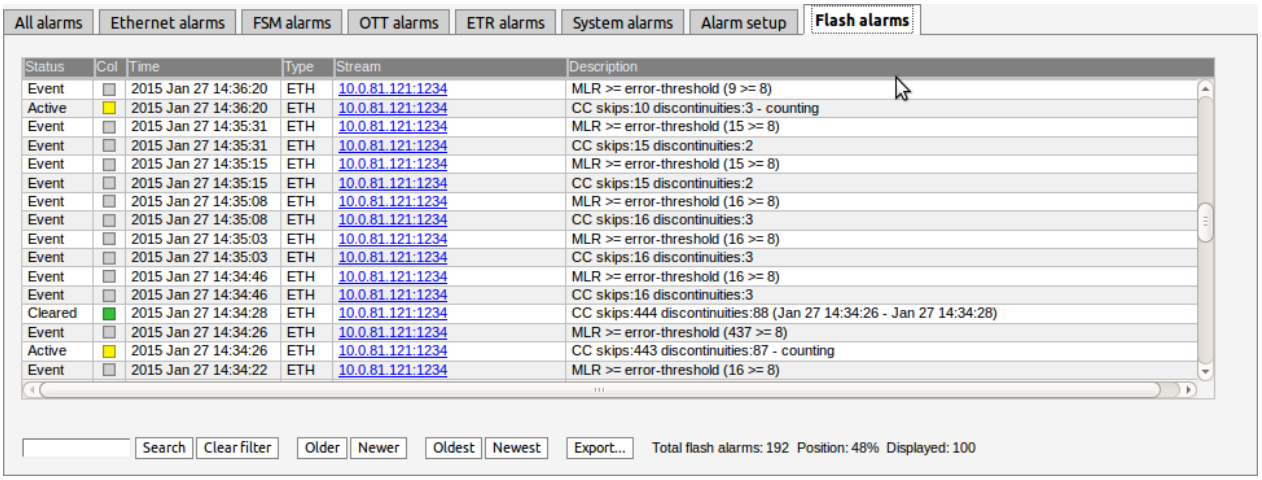
When **View list offline** is enabled filter buttons will be shown on the top of list. These allows filtering of the events based on their type:

- Regular events
- Config events
- Startup events
- Stream events



To enable/disable logging of ETR stream events go to the **Setup — ETR** view.

5.2.4 Alarms — Flash Alarms (requires DATA-LOG-OPT)



The DATA-LOG option enables the **Flash alarms** tab. This alarm list contains the last 20,000 alarms and keeps them on the hard disk so that they survive reboots and power-outages. This opens up a lot of possibilities for probes that cannot be reached while doing measurements and for probes that need to be powered down and consulted elsewhere. It also severely increases the size of the alarm list allowing browsing of older alarms.

5.2.5 System alarms

This section contains a partial list of system alarms that may be raised by the Software Probe.

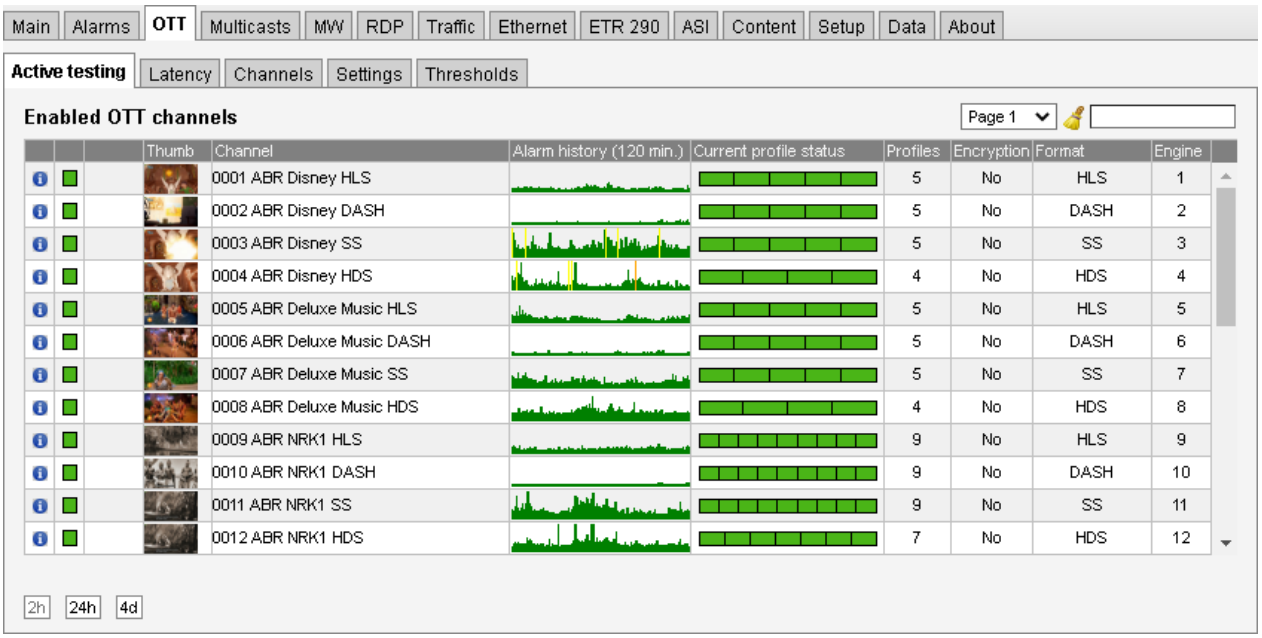
System alarms	
System time is wrong	The system time does not agree with the time stamp of the license activation. Please refer to G Appendix: On-line License Activation for more details.

License expires in N hours	The current license activation is about to expire and the system is not able to connect to the internet to refresh it automatically. Please refer to G Appendix: On-line License Activation for more details.
Stopped processes	One or more of the required system processes have stopped. This can be due to an intermittent software failure (bug), in which case the alarm should go away after a little while. If the problem persists, this might indicate that the system is overloaded; try reducing load to see if the problem clears. This alarm is sometimes raised during system start-up if one of the processes is slow to start. As long as the alarm goes away in a few minutes, this is only an indication that the system might be running slow due to high load.
Packet Errors on interface	The VB330-SW has detected problems with the attached Ethernet connection. Verify cables and connectors.
Timeline storage capacity below critical level	The file system mounted for Timeline does not have enough free space to continue storing data. Free up space by changing the settings in the **Content — Setup** view.
NN% disk free for Timeline storage	The file system mounted for Timeline has fallen below the configured warning threshold. Free up space by changing the settings in the **Content — Setup** view.
Auto deletion of recordings imminent. Less than NN GB usable disk.	The amount of free space on the file system mounted for Recordings is getting close to the configured minimum level. Free up space or change the settings int the **Record — Setup** view. You can protect important recordings from being removed automatically, in the **Record — Recordings** view. Please refer to chapter 5.11.7 for more details.
Recordings stopped due to disk usage	The file system mounted for Recordings does not have enough free space to continue storing data, and the VB330-SW is not able to remove previous recordings to make more space available. Free up space or change the settings in the **Record — Setup** view.
Recordings stopped due to limited free memory	The system does not have enough memory to keep buffering the streams configured for triggered recordings. Free up memory by changing the buffer sizes in the **Record — Thresholds** view.
No disk free	The internal disk is full, please clear contents to ensure correct operation.

RAID system reports error	The system has a supported RAID installed, and the controller reports an error. Please refer to the RAID documentation in the OS and system documentation for more information.
Write error saving config file	The VB330-SW configuration file could not be saved. If the problem persists, you should export a full configuration using the **Data — Configuration** to avoid loss of data.
Trap queue is full	The VB330-SW is creating so many simultaneous alarms that it is unable to forward them as traps over SNMP. If the problem persists, try to reduce the load or disable unimportant alarms, or use the Eii to fetch alarm information.
Content analysis overloaded	The content analysis engine is overloaded. Please refer to B.5 Content Thresholds for more details.
Data queue overflow	The named data queue is receiving more data than the VB330-SW is able to process. This usually means that this part of the system is overloaded. Try reducing load to see if the problem goes away.

5.3 OTT (Option)

5.3.1 OTT — Active testing



The OTT option enables monitoring of up to 1000 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 Software Probe will parse a channel's manifest file, and for a live channel one of the latest segments in each OTT profile's segment 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 segments in the VoD file, one in each round-robin loop.

If manifest file parsing or segment 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, Smooth Streaming and RTMP channels, as well as AES128 and SAMPLE-AES encrypted HLS channels, and fixed key CENC encrypted DASH.

The page to display can be selected from a drop-down menu.

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.

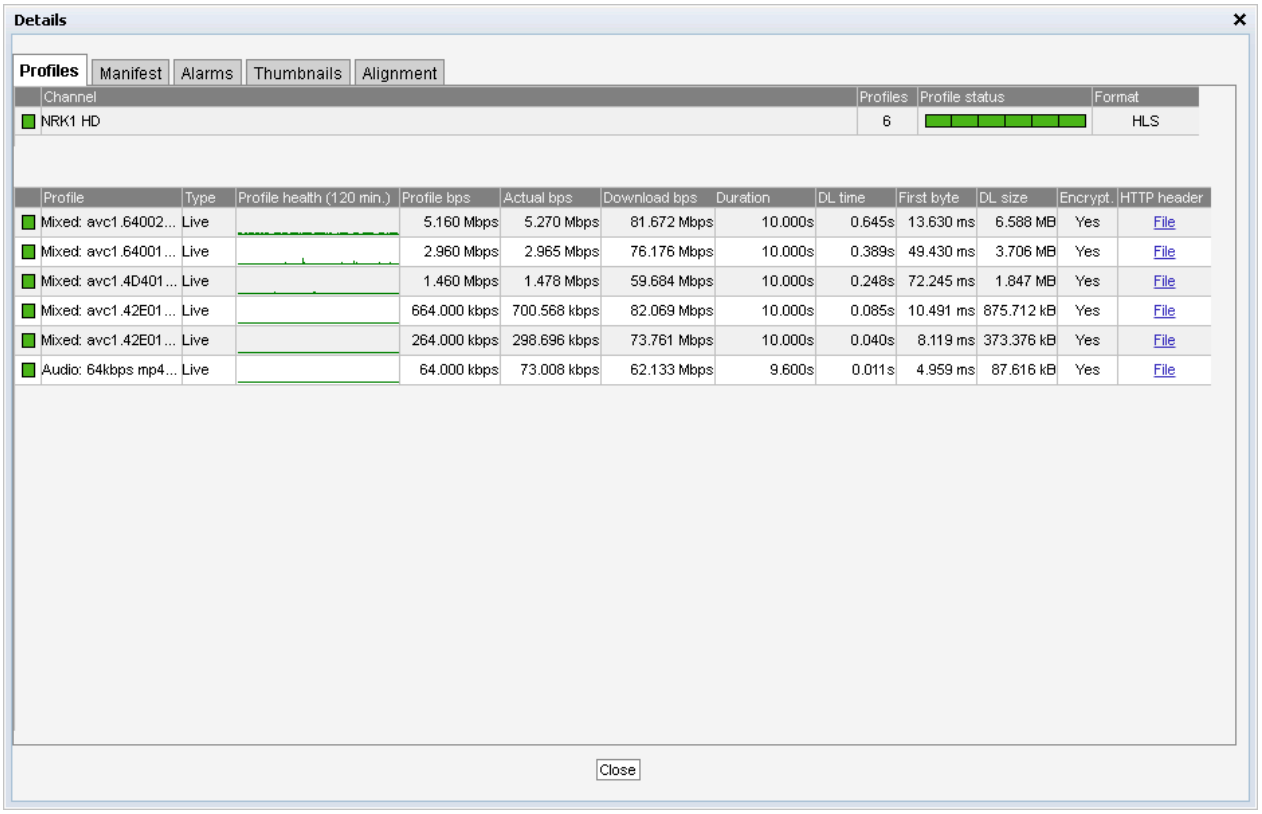
Thumb:	If thumbnail extraction has been enabled, a thumbnail is displayed for the channel if supported. Thumbnail decoding is a process asynchronous of the channel analysis and therefore should not be expected to be updated at the same time. The main purpose of the thumbnails is to provide brief information about the channel contents. If thumbnail extraction has not been enabled, or if the thumbnail extraction fails, an icon indicating the stream type will be displayed instead.
Channel:	The channel name defined by the user and linked to a URL in the **OTT — Channels** view.
Alarm history:	A timeline graph display of a combined bitrate and alarm representation for the channel. This shows the most severe alarm or download speed for all monitored profiles. The individual profiles graphs can be found in the **OTT — Details — Profiles** view. The timeline can display 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*.
Format:	The channel format is resolved from the manifest files, and is shown here (Apple **HLS**, Microsoft **Smooth Streaming**, Adobe **HDS**, **MPEG DASH**, **SHOUTcast** or **RTMP**).
Engine:	Indicates which OTT engine is assigned to what channel. The Software Probe can be licensed with anywhere from 1 up to 50 OTT engines. Each engine is capable of handling any number of channels.

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 **Content — Thumbnails** view, see chapter 5.10.1 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:

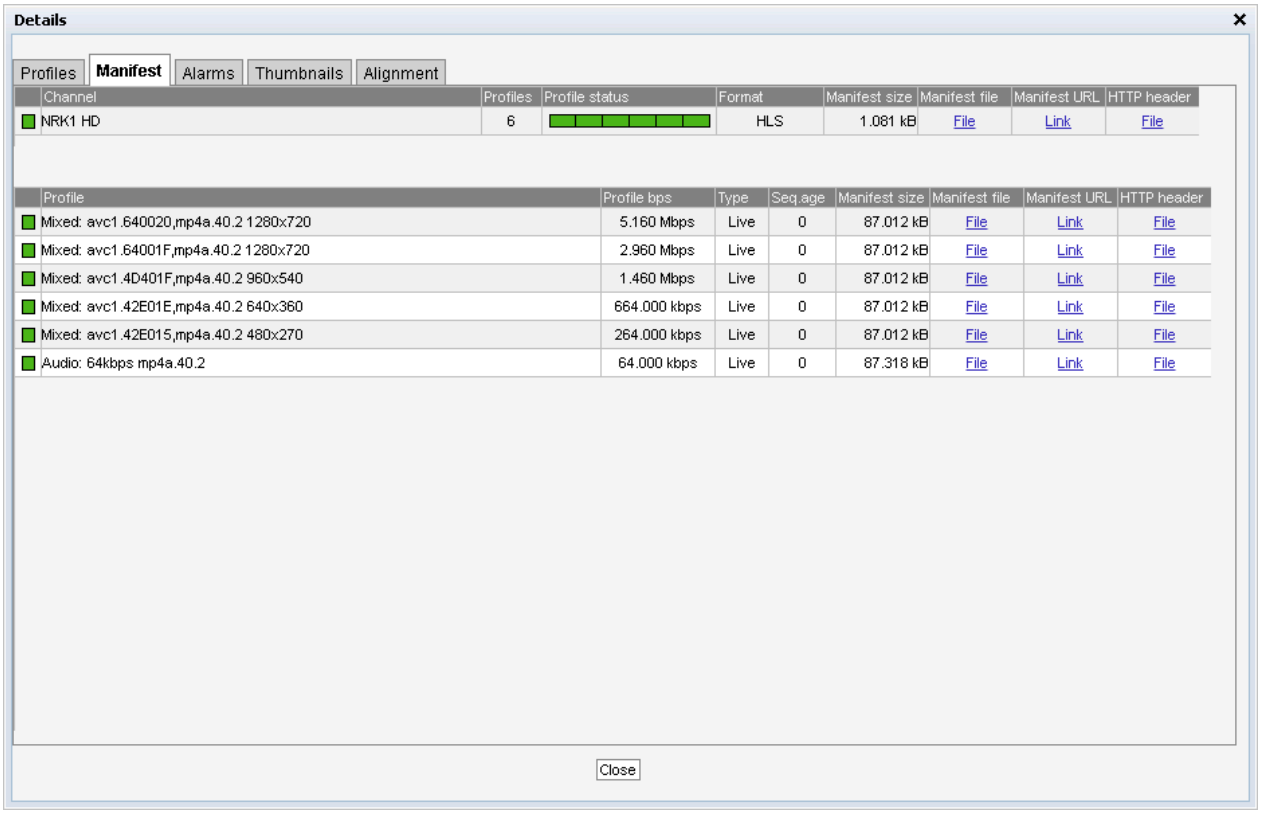
Channel	
Channel:	The channel name defined by the user and linked to a URL in the **OTT — Channels** view. A bulb indicates the current status of the channel, i.e. the most severe profile status.
Profiles:	The number of profiles associated with a channel.

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
Format:	The channel format is shown here (Apple **HLS**, Microsoft **Smooth Streaming**, Adobe **HDS**, **MPEG DASH**, **SHOUTcast** or **RTMP**).

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 can display the last 120 minutes, 24 hours or four days, and the graph resolution is one minute for the two hour graph, twelve minutes for the 24 hour graph or 48 minutes for the four day graph.
Profile bps:	The profile nominal bandwidth as flagged in the manifest files.
Actual bps:	The actual profile bitrate, i.e. the segment size (megabits) divided by the segment 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 segment size (megabits) divided by the download time (seconds).
Duration:	The profile segment duration (seconds) specified in the manifest file.
Download time:	The actual profile segment download time (seconds).
First byte:	The time (in seconds) before the first payload data byte was received.
Download size:	The actual profile segment 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 segment downloaded for that profile.

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 for the formats were such are available.

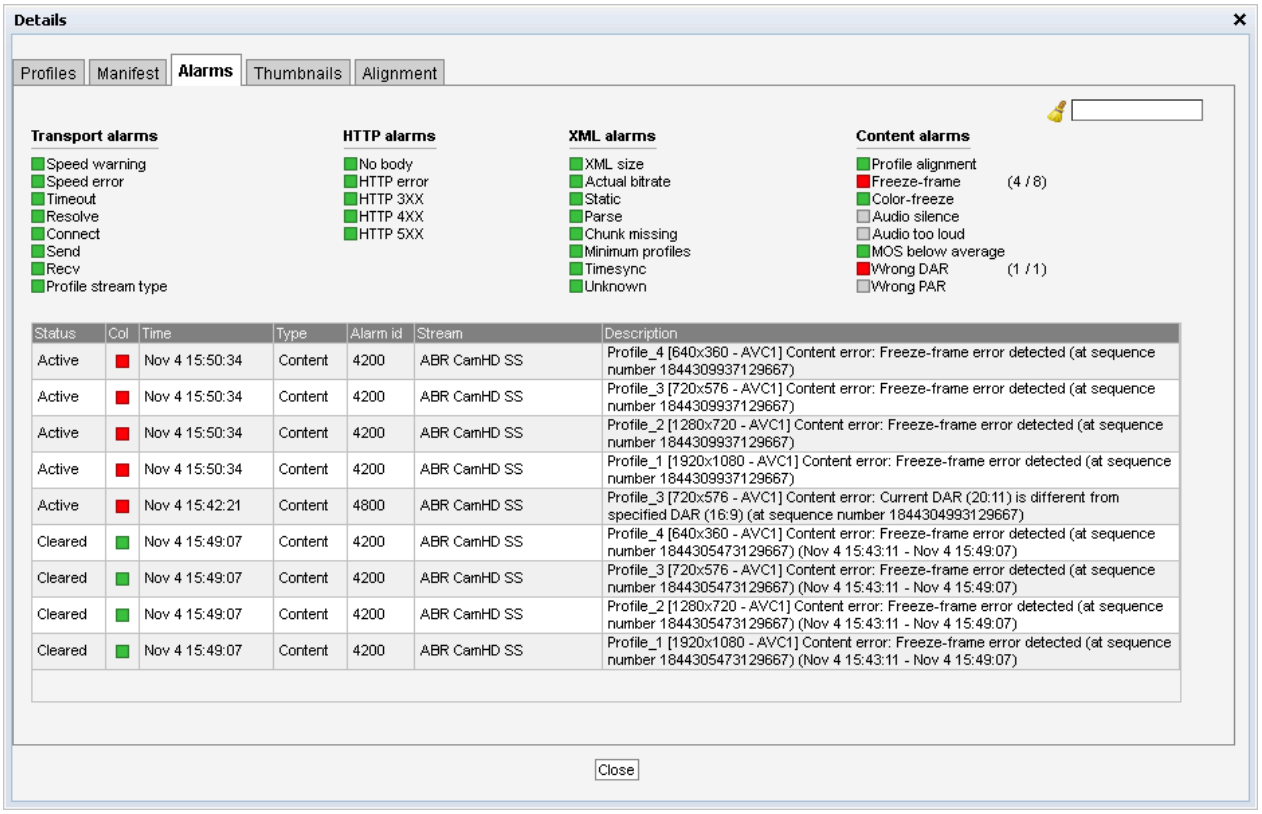
Channel	
Channel:	The channel name defined by the user and linked to a URL in the **OTT — Channels** view. A bulb indicates the current status of the channel, i.e. the most severe profile status.
Profiles:	The number of profiles associated with a channel.
Profile status:	The channel health bar displays 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
Format:	The channel format is shown here (Apple **HLS**, Microsoft **Smooth Streaming**, Adobe **HDS**, **MPEG DASH**, **SHOUTcast** or **RTMP**).

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. The profile sequence age is only reported for **Live** profiles.
Manifest size:	The size in bytes of the manifest file for a particular profile, for formats where such a file is available.
Manifest file:	Clickable URL for displaying the manifest file as text for this particular profile, or “N/A” for formats where such a file is not available.
Manifest URL:	Clickable URL to the profile manifest file, for formats where such a file is available.
HTTP header:	URL to HTTP header in text form for a particular profile manifest file, or “N/A” for formats where such a file is not available.

5.3.2.3 OTT — Details — Alarms

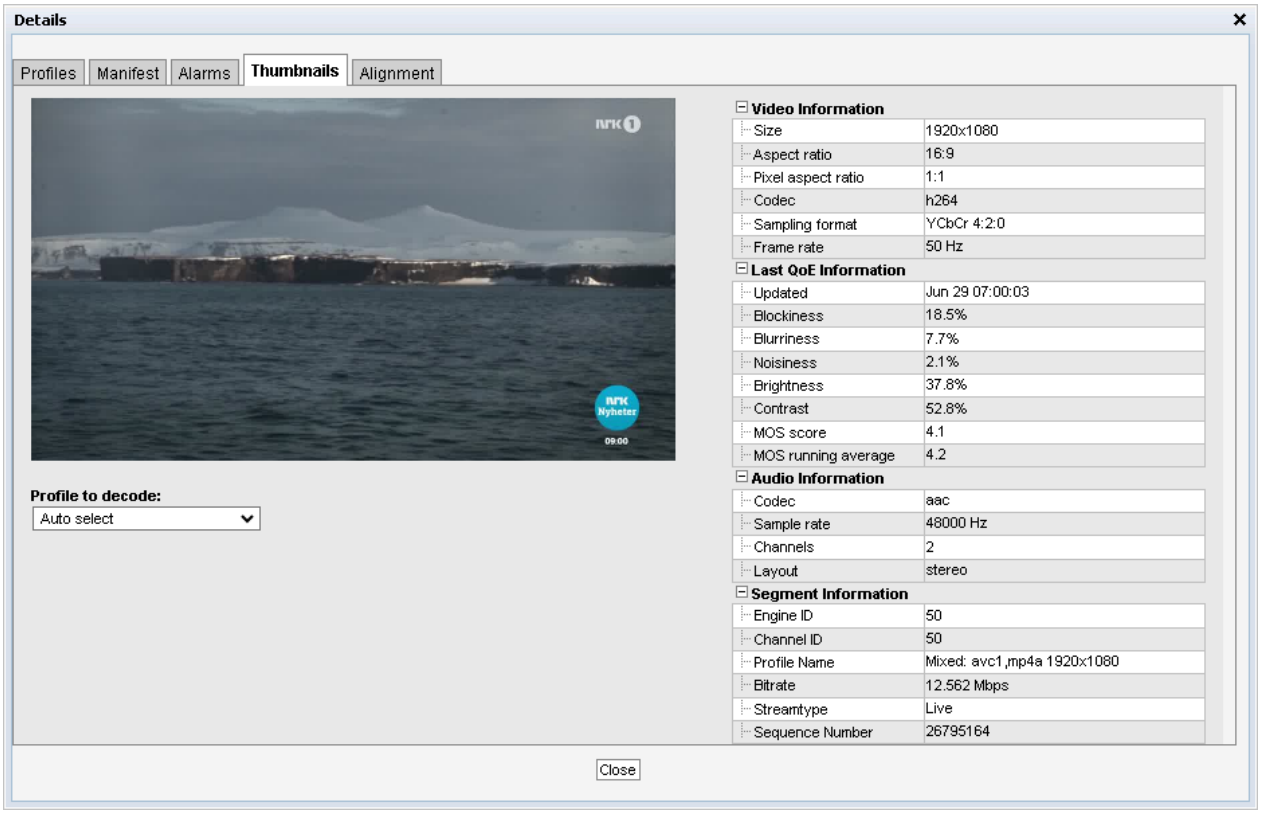


The **Details — Alarms** view gives an at-a-glance overview of any active OTT alarms for the selected channel. An alarm log for the selected channel is also provided here.

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** view 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 segment 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.

Video 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
Sampling format:	The video sampling format of the selected profile
Frame rate:	The video frame rate of the selected profile (Hz)

Last QoE information (Displayed if QoE scoring is enabled)	
Updated:	Indicates the time when QoE scores were last generated.
Blockiness:	Detected picture blockiness, in percent.
Blurriness:	Detected picture blurriness, in percent.
Noisiness:	Detected picture noisiness, in percent.
Brightness:	Detected picture brightness, in percent.
Contrast:	Detected picture contrast, in percent.
MOS score:	Calculated picture quality score, on a scale from 1.0 to 5.0, where 5.0 is best.
MOS running average:	If MOS average alarming has been enabled, the current MOS running average is displayed here
MOS average window:	If MOS average alarming has been enabled, the averaging window is displayed here

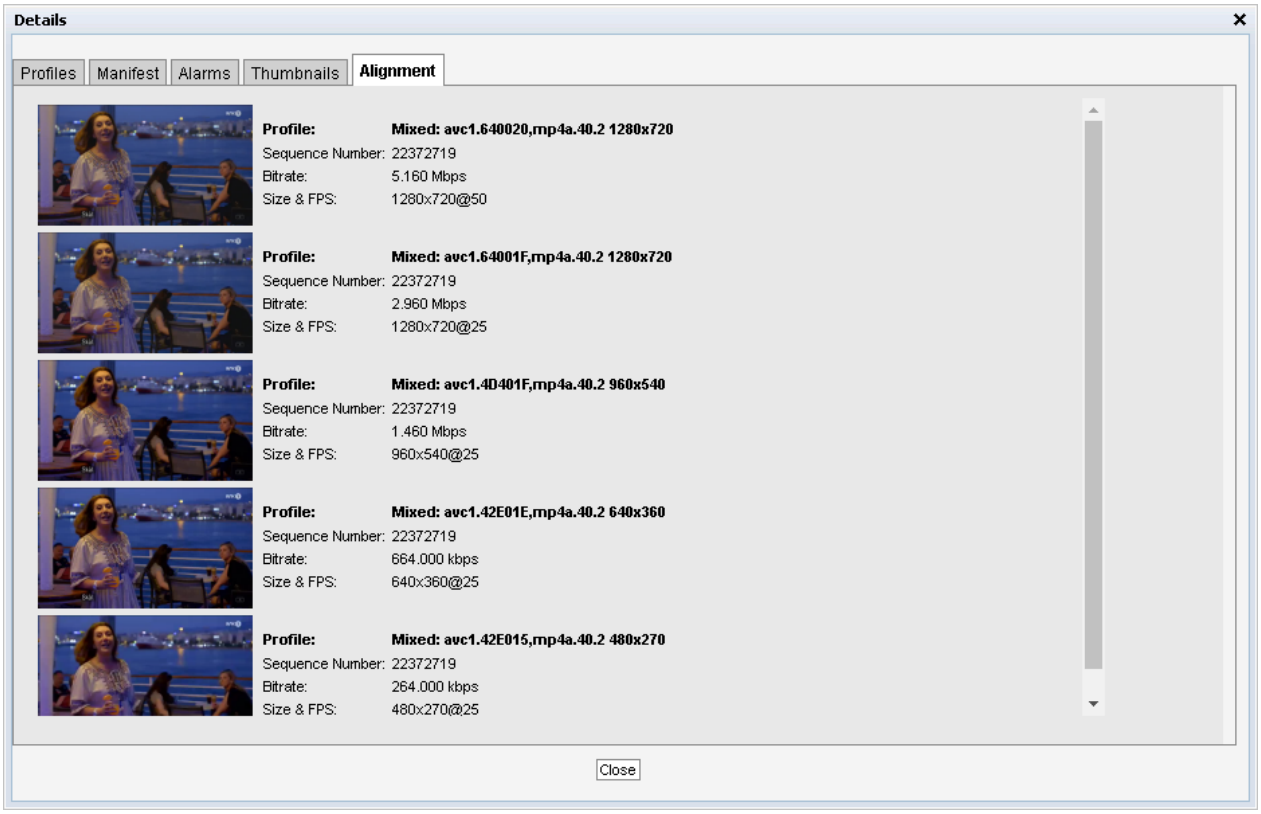
The QoE scores are only calculated for the profile with the highest bitrate. To measure the quality loss between profiles, enable VMAF scoring and use the measurements displayed in the **Alignment** view.

Audio Information	
Codec:	The audio encoding format
Sample rate:	The audio sample rate
Channels:	The number of audio channels represented by the audio PID
Layout:	The audio channel layout

Audio information is only displayed if audio monitoring has been enabled in the content thresholds for the channel.

Segment 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 Name:	The name of the OTT profile as flagged in the manifest files.
Bitrate:	Bitrate rate of the a segment.
Streamtype:	The type of the stream detected; live or video on demand.
Sequence Number:	The current sequence number being analyzed. This is either signaled in the channel manifest (HLS, HDS, DASH, Smooth Streaming), or generated by the VB330-SW(RTMP, SHOUTcast).

5.3.2.5 OTT — Details — Alignment



The **Alignment** view shows the user all the profiles for a selected channel with thumbnails and corresponding data.

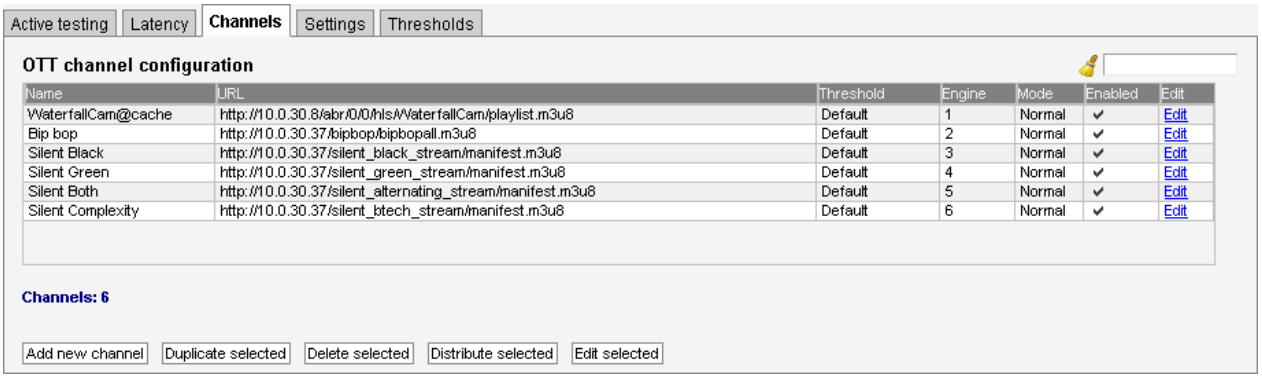
Profile Alignment Information	
Profile:	The name of the OTT profile as flagged in the manifest files. The first profile listed is always the one with the highest signaled bitrate.
Sequence Number:	The segment or sequence number for the current thumbnail. This is either signaled in the channel manifest (HLS, HDS, DASH, Smooth Streaming), or generated by the VB330-SW(RTMP, SHOUTcast). If the sequence numbers are highlighted in yellow, the thumbnails are not generated from the same segment for all profiles, and may therefor appear to be out of synchronization. Please note that VMAF scoring and alignment testing is only performed when the profiles sequence numbers inside each adaptation set are in alignment.
Bitrate:	The signaled bitrate for this profile (bits/s).
Size & FPS:	Indicates the original video size (pixels) and the frame-rate (Hz).

VMAF score:	If enabled in the OTT thresholds, a VMAF score is calculated for each of the profiles, with the highest-bitrate profile used as the reference.
Audio:	Indicates the audio channel layout.

The current version of the VMAF algorithm and model (denoted as VMAF 2.3.1), released as part of the VMAF Development Kit open source software, uses the following elementary metrics fused by Support Vector Machine (SVM) regression: **Visual Information Fidelity (VIF)**, **ADM (previously known as Detail Loss Metric)**, **Motion**

Software Probe release 6.5 utilizes metrics described above for its QoE scoring.

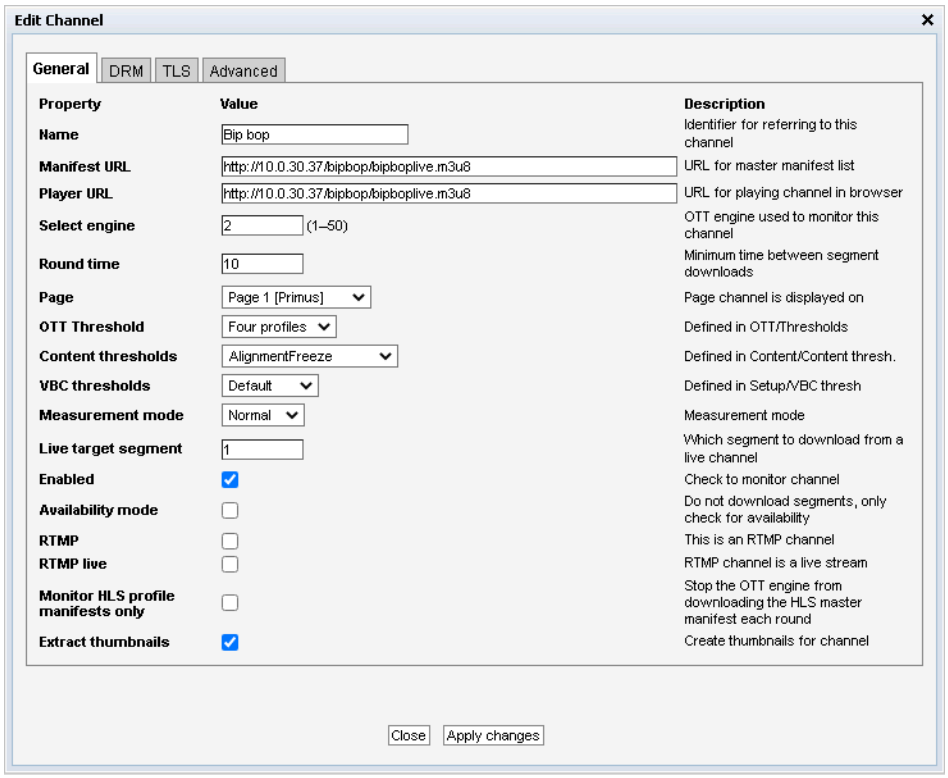
5.3.3 OTT — Channels



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

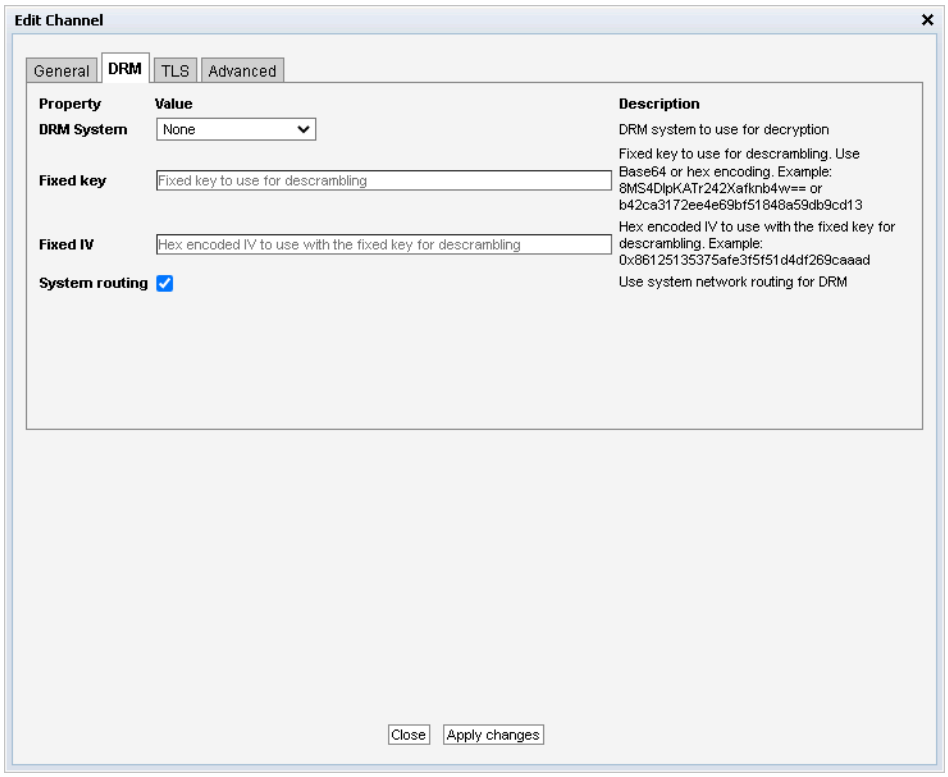
To add a channel to the list click the **Add new channel** button. This will open the **Edit channel** pop-up view, allowing the user to define channel parameters. A channel entry can be selected by clicking the channel; the list entry will be highlighted. Several list entries can be selected by using 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	
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 **Active testing** view, which will open the selected URL in a new browser tab.
Select engine:	A number between 1 and 50, depending on license activated, indicating which OTT engine the channel uses.
Round time:	Sets the minimum round time of this OTT channel, in seconds (default: 15 seconds). If processing all the profiles of a single channel takes 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. The round time setting does not apply to channels for which real-time audio analysis have been enabled. Note: The round time may not be set to a value less than 2 seconds.
Page:	Choose which Active Testing page this channel should be displayed on. Having too many channels on the same page can cause the page reloading to stutter.

OTT 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.
Content thresholds:	The Content thresholds specify content alarming options. Selectable Content thresholds templates are defined in the **Content — Content thresh.** view.
Content schedule:	The scheduling scheme that should be assigned to the content monitoring for the OTT channel. Scheduling schemes that have been defined in the **Setup — Scheduling** view are available for selection from the drop-down menu. Scheduling allows masking content alarms at predefined time periods.
VBC thresholds:	The alarm threshold template used to configure when alarms are generated towards the VBC server.
Live target segment:	This specifies which segment, counted from the bottom of the list, the VB330-SW should download when doing active testing on a live channel.
Enabled:	Check the 'Enabled' check box to start monitoring the OTT service.
Availability mode:	If this option is enabled, the engine will only check for segment 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.
Monitor HLS profile manifests only:	This option makes the OTT engine only download the master manifest once. After the initial download, it will only re-download it if one of the profiles gets an error or the connection reset timeout occurs. This option can be used if the server hosting the manifest is generating an unique session for each download of the master manifest, for instance by changing the profile playlist URLs between each download.
Extract thumbnails:	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. If the Content Extraction and Alarming option is licensed, alignment checking is enabled in the Content threshold and this setting is not visible.

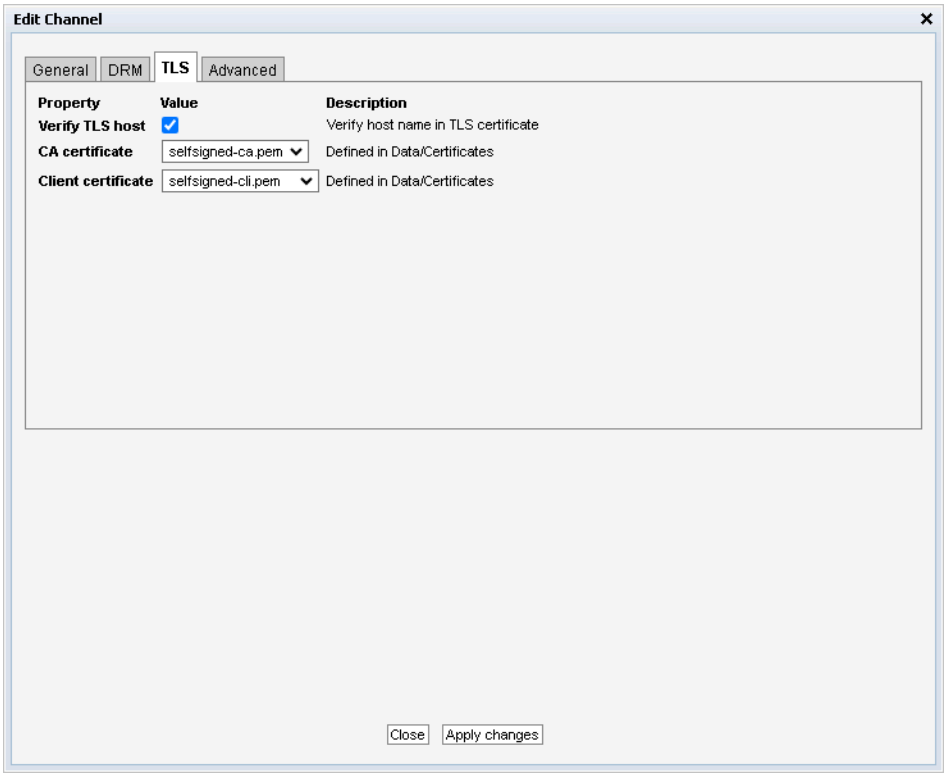


DRM	
DRM system:	If this channel is encrypted using a Verimatrix VCAS server, selecting the **Verimatrix VCAS 3.7** or **Verimatrix VCAS 4.3** option and entering the IP address or hostname of the VCAS server's encoder interface in the **DRM hostname** field will allow descrambling of the encrypted segments. See **OTT descrambling with Verimatrix** for more info. If this channel is encrypted using an Irdeto server, select the **Irdeto** option and configuring access to the Irdeto server will allow descrambling of the encrypted segments. Select **None** option for streams that are not encrypted, or where you have a fixed key or IV available.

Fixed key:	The key that will be used to descramble the segments for this channel. Using this field will override any key found during manifest parsing.
	For HLS, use a Base64 encoded string, like this:
	`8MS4DlpKATr242Xafknb4w==`
	For DASH, use a hex encoded string, like this:
	`b42ca3172ee4e69bf51848a59db9cd13`

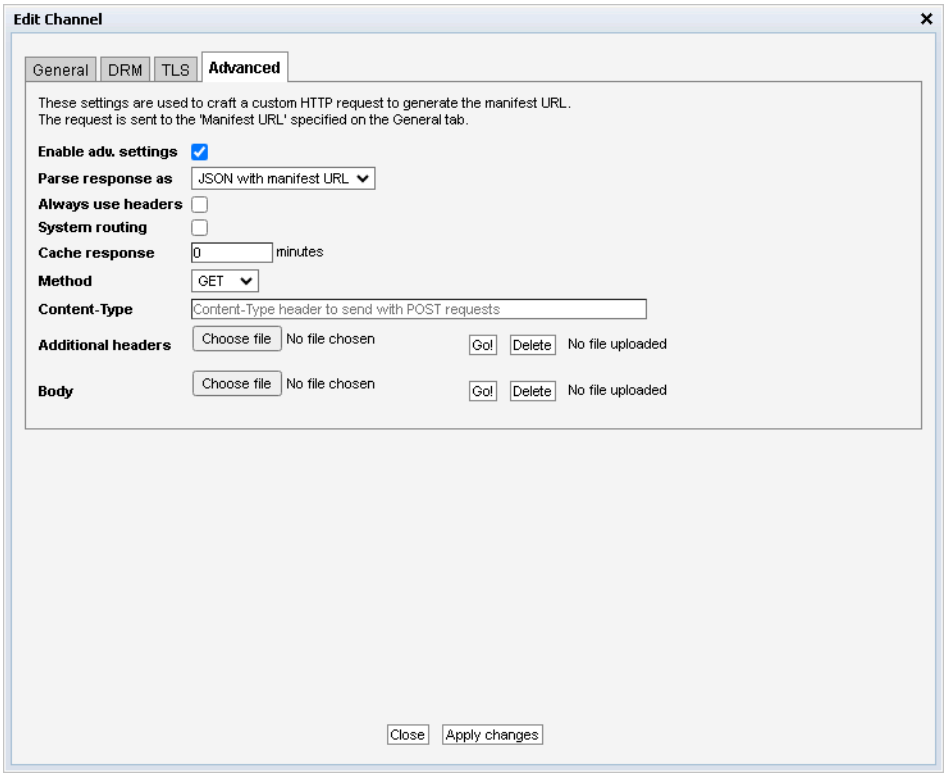
Fixed IV:	The IV to be used during descrambling of the HLS segments. Using this field will override any IV found or calculated during manifest parsing. Use a `0x`-prefixed hex encoded string, like this: `0x86125135375afe3f5f51d4df269caaad`

DRM hostname:	If used with a DRM system, configure enter the IP address or hostname of the DRM server here.
DRM username:	When using the **Irdeto** DRM system, add the username used to log in to the Irdeto server here.
DRM password:	When using the **Irdeto** DRM system, add the password used to log in to the Irdeto server here.
Account ID:	When using the **Irdeto** DRM system, this should be set to the ID of the account that this channel is configured to. Please refer to the Irdeto User Manual for more details.
Content ID:	When using the **Irdeto** DRM system, this should be set to the ID of the channel on the Irdeto server. Please refer to the Irdeto User Manual for more details.
Crypto Period:	When using the **Irdeto** DRM system, this should be set to match the configuration on the Irdeto server. Please refer to the Irdeto User Manual for more details.
System routing:	If enabled, the request for the DRM system or linked key uses the system routing table. If disabled, the request uses the routing configured for the associated OTT engine.



TLS

Verify TLS host	If the channel is requested over a TLS connection, enabling this option verifies that the presented server certificate is valid for the host name used for the request. This setting can be enabled without having the CA certificate available.
CA certificate	If the channel is requested over a TLS connection, selecting a CA certificate here verifies that the presented server certificate is trusted by it. Certificates are uploaded in the **Data — Certificates** view.
Client certificate	If a client certificate is selected here, and the channel is requested over a TLS connection, the Software Probe will present this certificate in outgoing network requests. Enable this setting for mTLS (mutual TLS). Certificates are uploaded in the **Data — Certificates** view.



Advanced	
Enable adv. settings:	Check this box to enable the advanced manifest settings. If unchecked, all settings on this page are ignored.
Parse response as:	Determines how to parse the response returned when requesting the **Manifest URL**. See below for an explanation of the settings.
Always use headers:	If enabled, any headers specified in **Additional headers** configured below will be sent with all requests. If disabled, the additional headers will only be sent in the advanced manifest request.

System routing:	If enabled, the request for the advanced manifest URL uses the system routing table. If disabled, the request uses the routing configured for the associated OTT engine.
Cache response:	Defines for how long the advanced manifest response should be cached. If set to a non-zero value, the server is not queried again for the same URL until at least the configured number of minutes has passed. If the value for *Reset connection after* under **OTT — Settings** is lower, that value takes precedence.
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, or if additional parameters or an alternative HTTP method is required to access it.

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 look-ups through this interface. Set **Parse response as** to *JSON with manifest URL* and have the in-between service return a JSON file with an “url” parameter containing the URL to the master manifest file.

If your channel just needs additional headers and/or an alternative HTTP method to return the master manifest, set **Parse response as** to *Normal manifest*. Enable **Always use headers** if the additional headers are to be supplied in all requests, and not only the request for the top-level manifest.

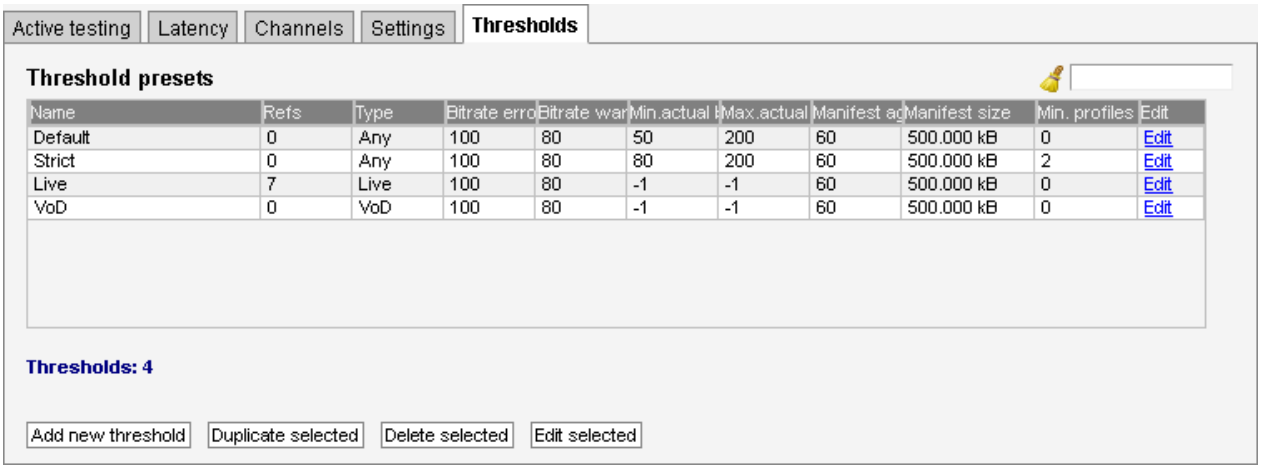
5.3.4 OTT — Settings

The **Settings** view 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.

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.
Page name:	This setting allows names to be associated with different pages. Individual channels can be assigned to different pages in the **OTT — Channels** view, to facilitate easier navigation in the different **OTT** views.

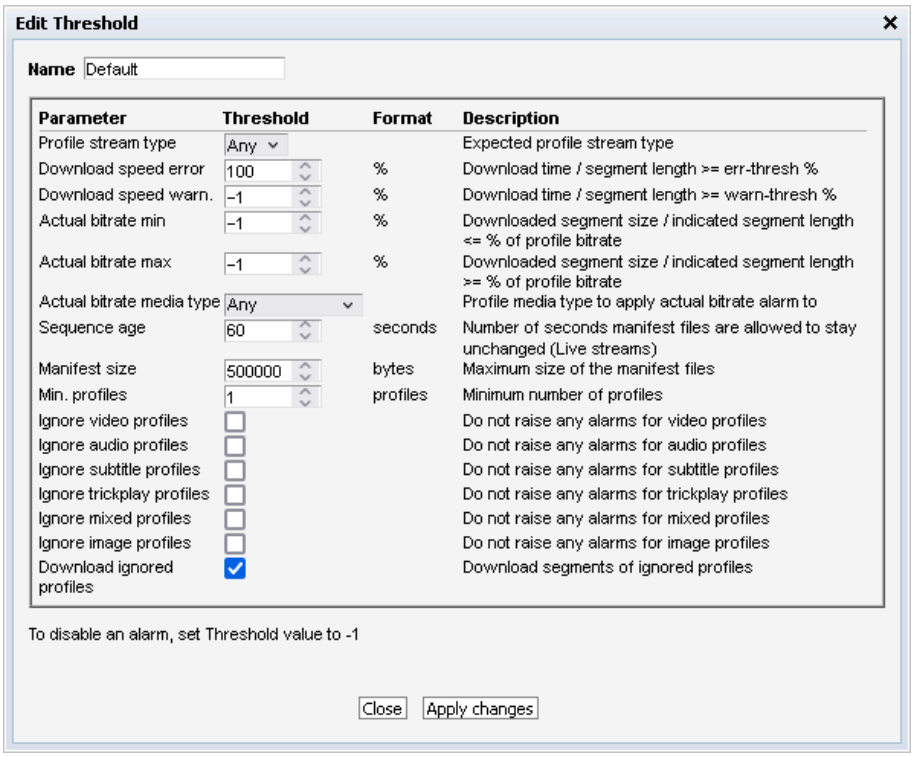
5.3.5 OTT — Thresholds



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.



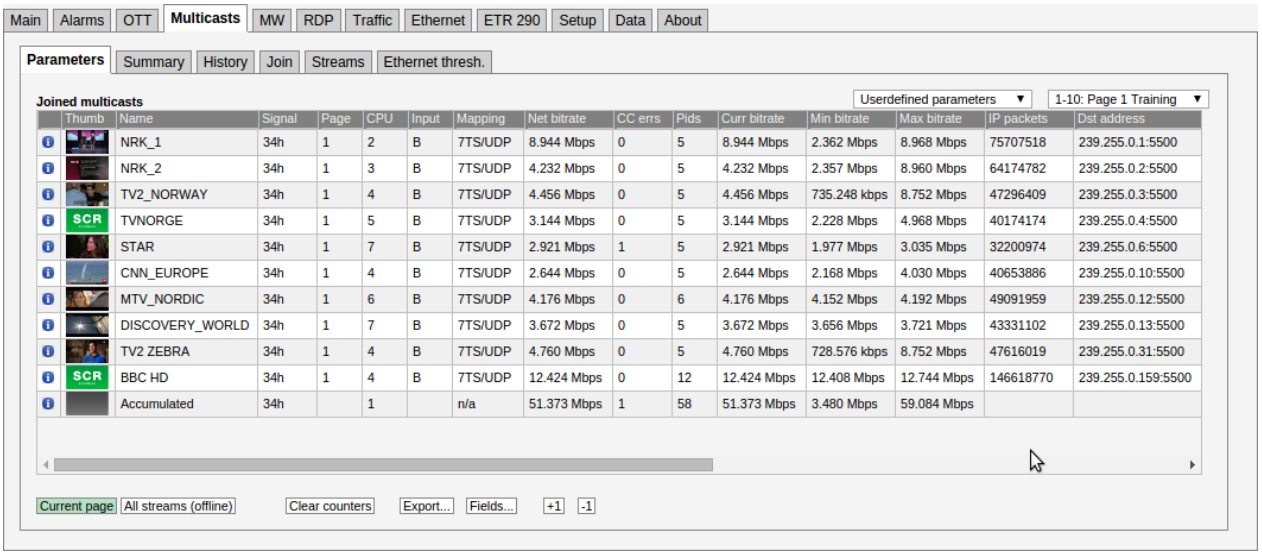
To disable a threshold alarm, set the threshold value to *–1* or *Any*. This does **not** apply for *Manifest XML size*.

Threshold preset	
Name:	The threshold template name defined by the user.
Refs:	The number of channels associated with the threshold template
Profile stream type:	The stream type (*Live* or *VoD*). If any of the profiles have a different type a wrong profile type alarm will be raised.
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.

Actual bitrate media type:	The profile types that the actual bitrate alarm applies to. If set to *Any*, the actual bitrate is checked for all profiles.
Sequence age:	The maximum time a manifest can remain unchanged before a manifest age alarm is raised.
Manifest size:	The maximum detected size of the manifest before a manifest size alarm is raised. Manifests larger than this will not be analyzed. Also applies to profile manifests, where applicable.
Min. profiles:	Minimum number of profiles in the selected channel before an alarm is raised.
Ignore *X* profiles:	When any of these are checked, all alarms are disabled for profiles of the corresponding media types.
Download ignored profiles:	If this is unchecked, no segments will be downloaded for profiles which are ignored above.

5.4 Multicasts

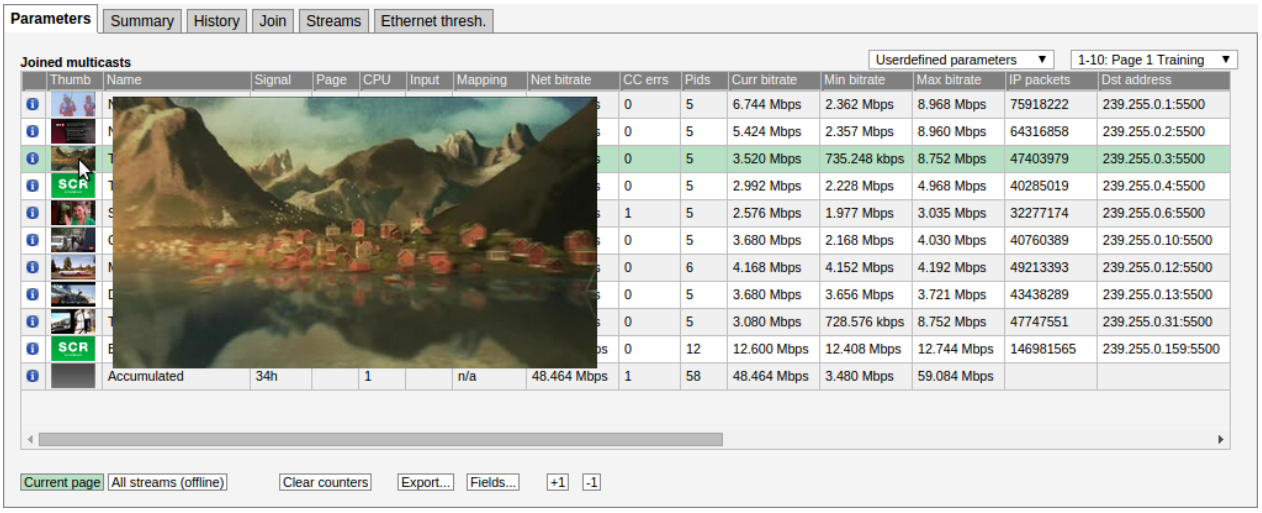
5.4.1 Multicasts — Parameters



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.



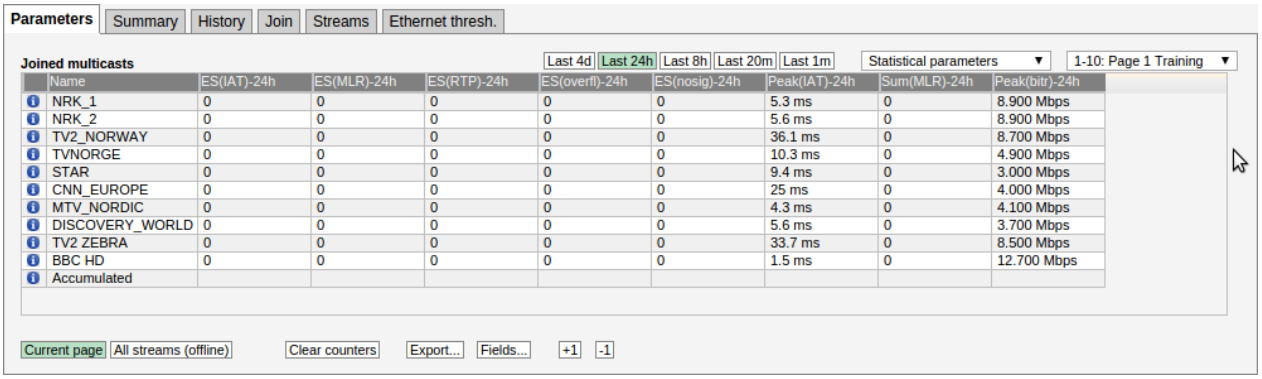
When the **Current page** button is clicked it is possible to select the page from a drop-down menu. The associated thumbnails are shown in the leftmost column of the list of measurements. Click one

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.

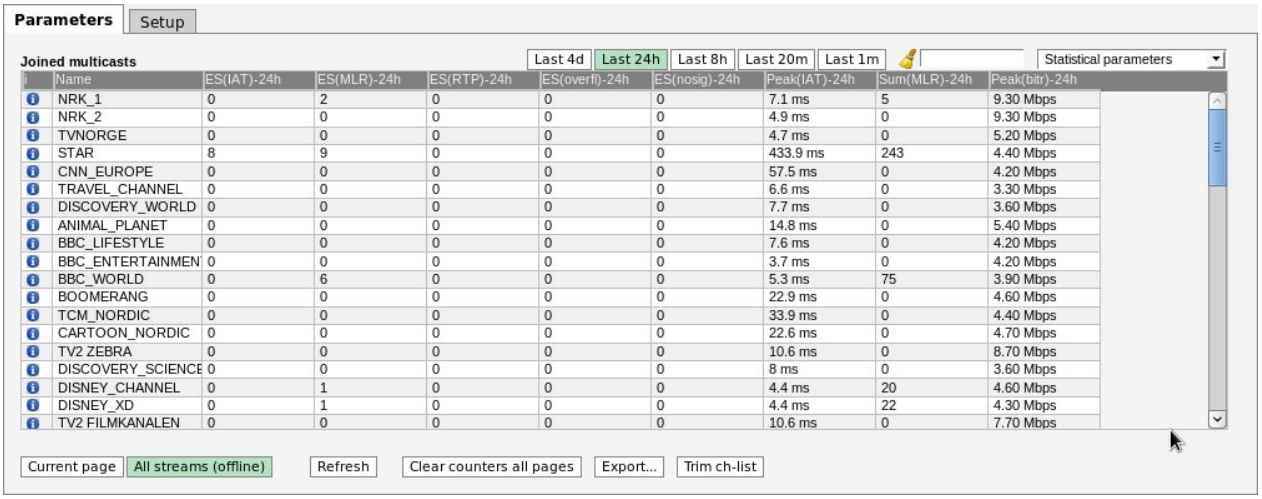
Peak and aggregate measurements are cleared when the **Clear counters** or **Clear counters all pages** button is clicked. Clicking this button also restarts the ETR monitoring for the streams have this enabled.

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



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.



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).

5.4.1.1 Parameter columns

Following is a listing explaining the meaning of the columns which may be shown for the joined multicasts view at **Multicasts — Parameters**. The columns displayed may be selected in see **Multicasts — Parameters — Fields**.

	Common parameters
ⓘ:	Click the information icon to access the **Detailed Monitoring** pop-up view.
Thumb:	If thumbnail extraction has been enabled, a thumbnail is displayed for each unencrypted stream. Click the small thumbnail to view a larger image that is updated more frequently. If thumbnail extraction has not been enabled, or if the thumbnail extraction fails, an informational icon will be displayed instead, see **Thumbnails** below for details on the different icons.
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
CPU:	CPU core monitoring this multicast
Input:	Network interface used to receive this multicast
Mapping:	For MPEG-2 Transport streams, the number of MPEG-2 packets mapped into each RTP, UDP or SRT packet is displayed here. For SMPTE 2022-7 combined streams, “ST 2022-7” is displayed. For MABR streams, when MSYNC packets are detected, “MSYNC<version>/<protocol>” is displayed, where “<version>” is either 1 or 3 and “<protocol>” is either UDP or RTP. For other unsupported RTP streams, “RTP data” is displayed.
	IP parameters
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, and is calculated from the size of the RTP, L2TP or 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. For SMPTE ST 2022-7 combined streams, the path differential (PD) is shown instead, with the sign indicating which of the paths is ahead of the other.
IAT min:	The Minimum Inter-Arrival Time is the minimum registered time between two consecutive IP frames carrying video. Units are in milliseconds. For SMPTE ST 2022-7 combined streams, the minimum path differential is shown instead.
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. For SMPTE ST 2022-7 combined streams, the maximum path differential is shown instead.

TS parameters

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. No bitrate is reported for SMPTE ST 2022-7 combined streams.
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)
#Services:	The number of services found in the multicasts

Ethernet parameters

Src MAC:	Source MAC address
Dst MAC:	Destination MAC address

RTP Parameters

RTP drops:	Accumulated number of dropped IP-frames due to network errors. Only available for multicasts that carry RTP information, and for L2TP streams that carry sequence numbers. 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, and for L2TP streams that carry sequence numbers. 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

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.

MSYNC parameters

MSYNC URI	URI of of the MSYNC object being decoded as given from the `object URI` field of the `Object Info` MSYNC packet.

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, JPEG 2000 and JPEG XS video formats in standard definition, high definition or ultra-high definition are supported in MPEG-2 transport streams. To display thumbnails for JPEG XS services, the JPEGXS-OPT license is required. Thumbnails are not generated for SMPTE ST 2022-7 combined 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 signal cannot be decoded because the Transport Error Indicator bit (TEI) is set.
	The signal cannot be decoded because the video bitstream contains errors. It might be possible to create thumbnails from this stream by enabling the “Ignore bitstream errors” checkbox in the content thresholds associated with the stream.
	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.
	The signal is recognized as being JPEG XS encoded but the thumbnail extractor is unable to correctly decode a thumbnail picture. To display thumbnails for JPEG XS services, the JPEGXS-OPT license is required.
	The signal is recognized as being an uncompressed (raw) video stream but the thumbnail extractor is unable to correctly decode a thumbnail picture.
	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.
	The probe can only generate a thumbnail picture if the video data is not scrambled.
	The stream is configured to be interpreted as MABR.

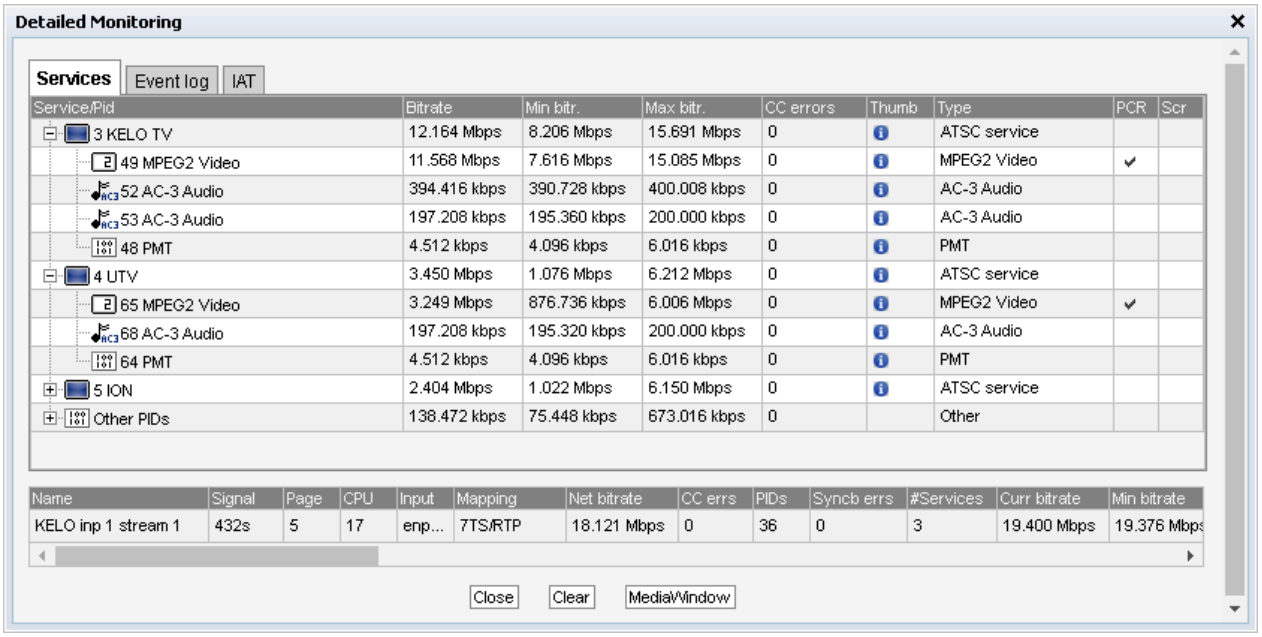
Detailed Monitoring

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

The current parameters for the selected stream are displayed in the bottom of the dialog, as in the **Joined multicasts** list.

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.

Detailed Monitoring — Services

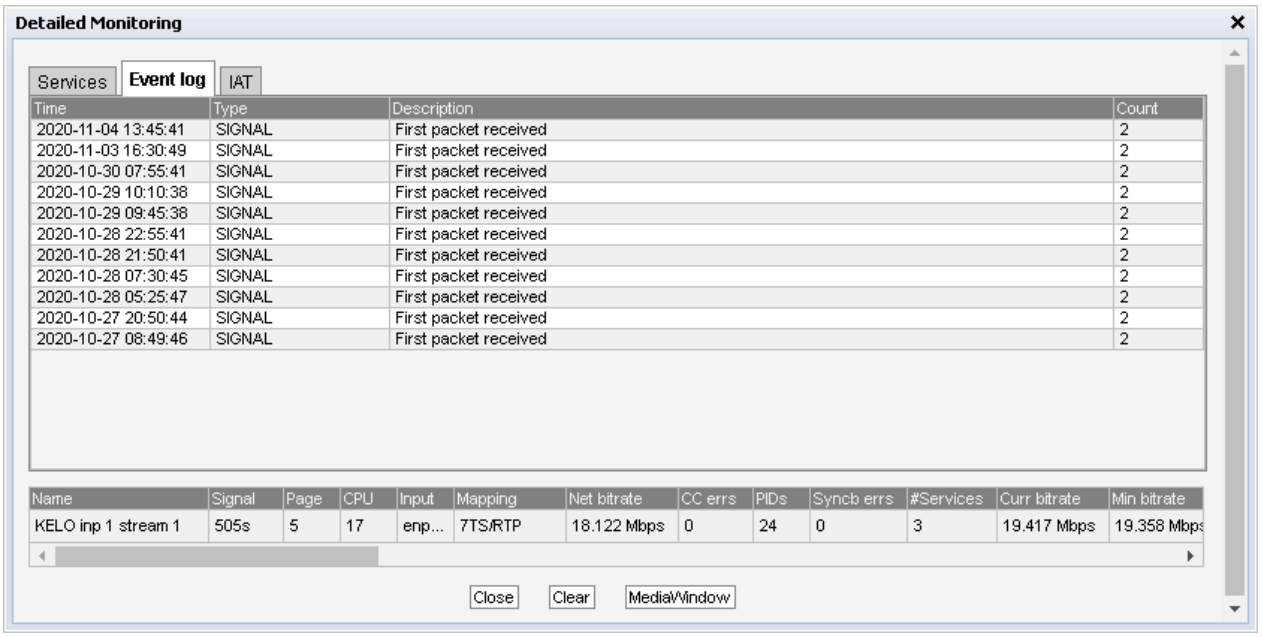


The Software Probe is continuously gathering detailed information for the selected multicast. The VB330-SW will continue updating the detailed information for the selected multicast until another is selected.

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

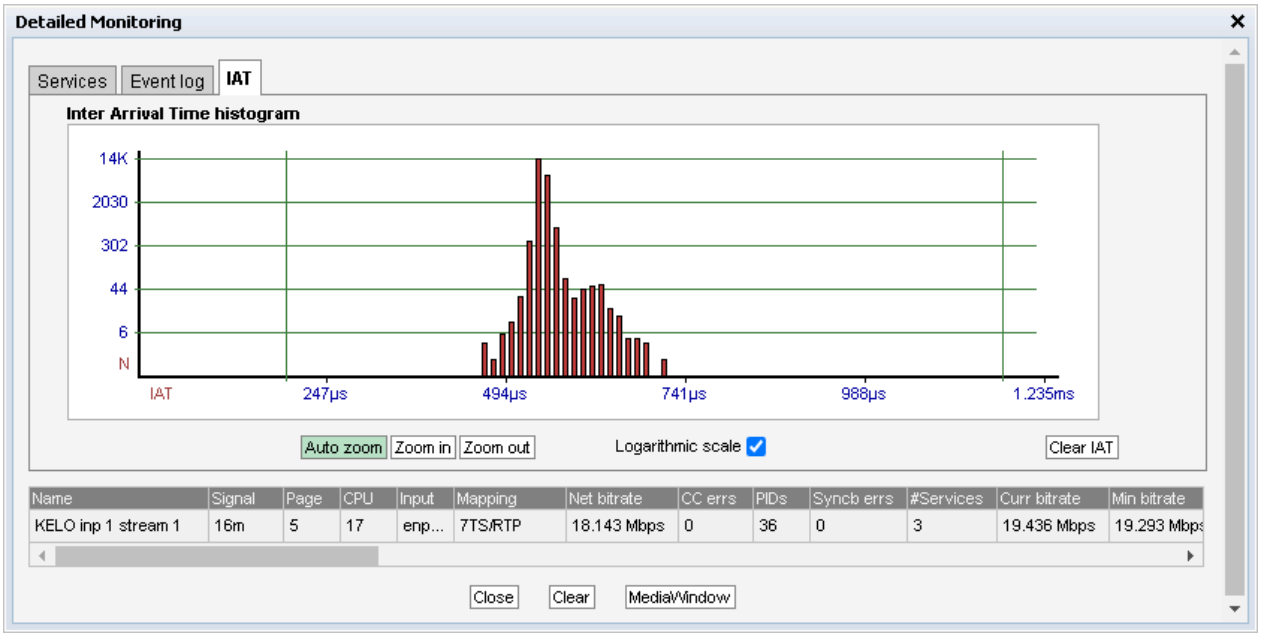
Service/Pid:	For each service, the service-name or service-id is obtained from the PSI/SI tables. PIDs that do not belong to a service are denoted ‘Other PIDs’. The service ID is presented in square brackets.
Bitrate:	Service bitrate in bits per second
Min bitr.:	Minimum service bitrate in bits per second
Max bitr.:	Maximum service bitrate in bits per second
CC errors:	Number of Continuity Counter occurrences
Thumb:	Click the ⓘ 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

Detailed Monitoring — Event Log



The event log contains informative text that may prove helpful for diagnosing transport and bitstream level errors.

Detailed Monitoring — IAT



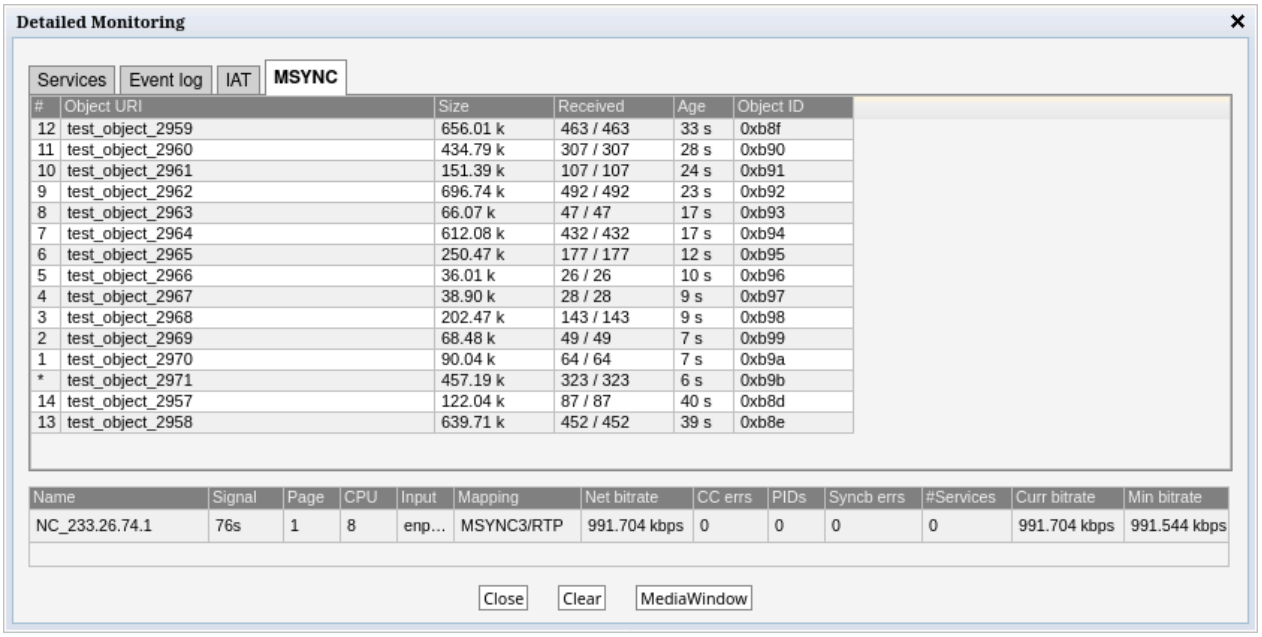
In the **Detailed Monitoring — IAT** view, the **Inter Arrival Time** histogram shows the accumulated number of IAT measurements within each presented interval. Vertical green lines indicate the maximum and minimum IAT values. By clicking the IAT range buttons it is possible to change the zooming of the graph. If the **Auto zoom** 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.

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.

For SMPTE ST 2022-7 combined streams, the path differential (PD) is shown instead.

Detailed Monitoring — MSYNC



#	Object URI	Size	Received	Age	Object ID
12	test_object_2959	656.01 k	463 / 463	33 s	0xb8f
11	test_object_2960	434.79 k	307 / 307	28 s	0xb90
10	test_object_2961	151.39 k	107 / 107	24 s	0xb91
9	test_object_2962	696.74 k	492 / 492	23 s	0xb92
8	test_object_2963	66.07 k	47 / 47	17 s	0xb93
7	test_object_2964	612.08 k	432 / 432	17 s	0xb94
6	test_object_2965	250.47 k	177 / 177	12 s	0xb95
5	test_object_2966	36.01 k	26 / 26	10 s	0xb96
4	test_object_2967	38.90 k	28 / 28	9 s	0xb97
3	test_object_2968	202.47 k	143 / 143	9 s	0xb98
2	test_object_2969	68.48 k	49 / 49	7 s	0xb99
1	test_object_2970	90.04 k	64 / 64	7 s	0xb9a
*	test_object_2971	457.19 k	323 / 323	6 s	0xb9b
14	test_object_2957	122.04 k	87 / 87	40 s	0xb8d
13	test_object_2958	639.71 k	452 / 452	39 s	0xb8e

Name	Signal	Page	CPU	Input	Mapping	Net bitrate	CC errs	PIDs	Syncb errs	#Services	Curr bitrate	Min bitrate
NC_233.26.74.1	76s	1	8	enp...	MSYNC3/RTP	991.704 kbps	0	0	0	0	991.704 kbps	991.544 kbps

When MSYNC monitoring is enabled for a stream, this view displays a list of the objects received. To enable MSYNC monitoring, the stream may be configured as *MSYNC* in **Multicasts — Streams — Edit**.

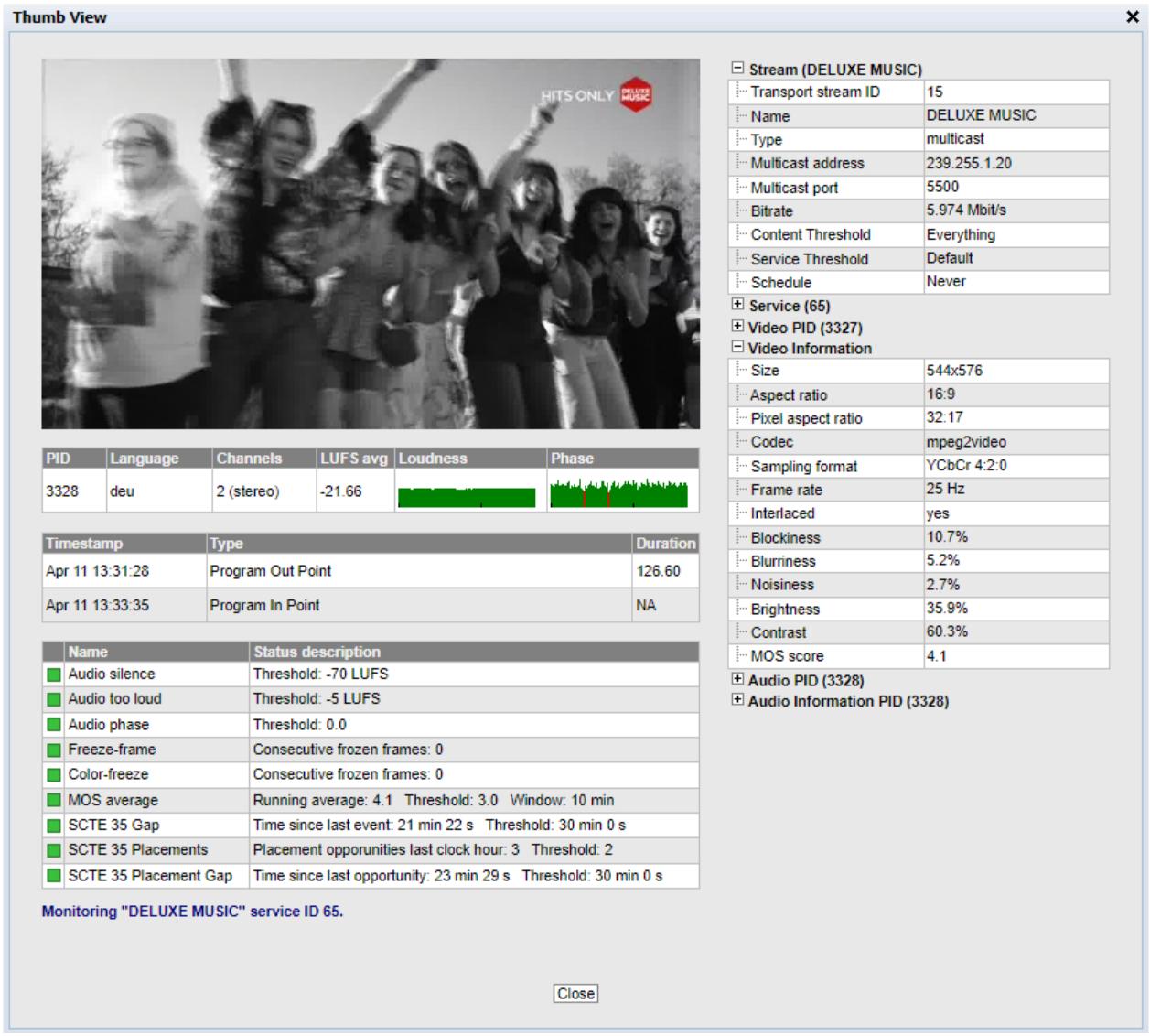
The probe retains a list of the last 15 objects received for each stream configured as *MSYNC*. As new objects are received, they are appended to the bottom of the list. When the probe has filled up the list, it starts writing new objects from the first row again, thereby overwriting the oldest objects. This facilitates viewing the objects which have been received within the last update. In addition it makes reading the lines easier as only the minimum amount of rows are changed between each view update.

The following columns are defined:

#	Object receive order. The most recently received object is indicated with an asterisk (*). The oldest object received is 14.

Object URI	The URI of the object as given from the `object URI` field of the `Object Info` MSYNC packet. If the file contains control information, i.e. the `object type` field of the `Object Info` MSYNC packet is equal to `control` or `Media manifest`, the URI is displayed as a link and the content of the object may be downloaded. The size of the file which the probe keeps is limited to 1 MiB. If the file was not received in its entirety, there will be gaps in the file.
Size	The size of the object as specified by the `object size` field of the `Object Info` MSYNC packet.
Received	Number of packets received / Number of packets in the object. Any difference between these two numbers indicates packet loss. The number of packets in the object is given by the `number of MSYNC packets` field of the `Object Info` MSYNC packet.
Age	The age of the object. This is calculated as the difference between the current time and the reception time of the `Object Info` MSYNC packet.
Object ID	The id of the object as given from the `object identifier` field of every MSYNC packet.

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 loudness and audio phase data are indicated in graphs for each audio component. The same pop-up can be opened from the **Content — Thumbnails** view, see chapter 5.10.1 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
Channels:	The number of channel and the layout of the audio track
LUFS avg:	If loudness monitoring has been enabled for the channel, the average LUFS of the samples displayed in the loudness graph is calculated and shown here.
Loudness:	If loudness monitoring has been enabled for the channel, a loudness graph covering the last ten seconds will be shown here. Portions that fall outside the defined thresholds will be colored red.
Phase:	If the audio phase monitoring has been enabled for the channel, a phase graph will be shown here for stereo sources. Portions that fall outside the defined thresholds will be colored red.

Please note that audio information is only decoded when enabled through the assigned content threshold. Audio information is updated periodically, and the initial display can take up to ten seconds. For more details on the content thresholds, please refer to the **Content — Content thresh.** view.

If caption monitoring has been enabled for the channel, the last two caption events for the service are displayed. For more details on these events, compare the **Content — Captions** view. In the case of DVB Subtitling, the subtitles are overlaid on the thumbnail image. The subtitle track to display can be selected in the dialog view.

If SCTE 35 monitoring has been enabled for the channel, the last two SCTE 35 events for the service are displayed. For more information on these events, compare the **Content — SCTE 35** view.

The following stream status information will be displayed (bulbs will be green for status OK, red to indicate an active alarm and grey if the associated check has been disabled):

	Status description
Audio silence:	A bulb indicates the audio silence status with reference to the defined requirement. **Threshold:** The audio silence detection threshold (LUFS/LKFS) as defined in the stream threshold template associated with the stream.
Audio too loud:	A bulb indicates the audio too loud status with reference to the defined requirement. **Threshold:** The audio peak detection threshold (LUFS/LKFS) as defined in the stream threshold template associated with the stream.
Audio phase:	A bulb indicates the audio phase status with reference to the defined requirement. **Threshold:** The audio phase detection threshold as defined in the stream threshold template associated with the stream.

Freeze-frame:	A bulb indicating the freeze-frame detection status. The freeze-frame error timeout value is set as part of the content threshold group associated with each multicast (refer to the **Content — Content thresh.** and **Multicasts — Streams — Edit** views). **Consecutive frozen frames:** The number of consecutive equal frames that have been detected
Color-freeze:	A bulb indicating the color-freeze detection status. The freeze-frame error timeout value is set as part of the content threshold group associated with each multicast (refer to the **Content — Content thresh.** and **Multicasts — Streams — Edit** views). **Consecutive frozen frames:** The number of consecutive single color frames that have been detected
MOS average:	A bulb indicating the MOS average status. The MOS averaging window is set as part of the content threshold group associated with each multicast (refer to the **Content — Content thresh.** and **Multicasts — Streams — Edit** views). **Running average:** The current running average MOS score **Threshold:** The MOS average threshold as defined in the content threshold template associated with the stream. **Window:** The window over which the MOS average is calculated.
SCTE 35 Gap:	If the probe has been licensed with the SCTE 35 Signaling Analysis and Logging option, this displays a status bulb indicating whether the SCTE 35 Command Gap alarm is active. The SCTE 35 alarming threshold values are set as part of the content threshold template associated with each multicast (refer to the **Content — Content thresh.** and **Multicasts — Streams — Edit** views). **Time since last event:** The number of seconds since the last received SCTE 35 event is displayed here. **Threshold:** The SCTE 35 Command gap threshold as defined in the content threshold template associated with the stream.

SCTE 35 Placements:	If the probe has been licensed with the SCTE 35 Signaling Analysis and Logging option, this displays a status bulb indicating whether the Too few SCTE 35 placement opportunities alarm is active. The SCTE 35 alarming threshold values are set as part of the content threshold template associated with each multicast (refer to the **Content — Content thresh.** and **Multicasts — Streams — Edit** views). **Placement opportunities last clock hour:** The number of placement opportunities found during the previous clock hour, or N/A if the service was not monitored for the whole previous clock hour. **Threshold:** The SCTE 35 Minimum number of placement opportunities per clock hour threshold as defined in the content threshold template associated with the stream.
SCTE 35 Placement Gap:	If the probe has been licensed with the SCTE 35 Signaling Analysis and Logging option, this displays a status bulb indicating whether the SCTE 35 placement gap alarm is active. The SCTE 35 alarming threshold values are set as part of the content threshold template associated with each multicast (refer to the **Content — Content thresh.** and **Multicasts — Streams — Edit** views). **Time since last opportunity:** The number of seconds since the start of the last placement opportunity is displayed here. **Threshold:** The SCTE 35 Maximum opportunity gap threshold as defined in the content threshold template associated with the stream.

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

Multicast	
Transport stream ID:	The ID of the selected stream as shown in the list of multicasts; non-TS services display *1* here
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, unicast or SRT Stream (a type of unicast)
Multicast address:	The multicast address of the stream containing the selected service. Multicasts only; not displayed for SRT streams.
Multicast port:	The port number of the multicast containing the selected service. Multicasts only; not displayed for SRT streams.
SRT Mode:	The SRT mode of operation selected to receive an SRT stream. SRT streams only; not displayed for multicasts.

SRT Latency:	The configured latency for the SRT connection. SRT streams only; not displayed for multicasts.
SRT Host:	The host address of the SRT stream source. SRT streams only; not displayed for multicasts. Not displayed in case of SRT mode 'Listener'.
SRT Port:	The port used to receive from the SRT stream source. SRT streams only; not displayed for multicasts.
Bitrate:	The total stream bitrate of the multicast containing the selected service (bits/s)
Content Threshold:	The name of the content threshold template assigned to the multicast
Service Threshold:	The name of the service threshold template assigned to the multicast
Schedule:	The name of the content alarm masking schedule template assigned to the multicast

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
Number of PIDs/Components:	The number of PIDs or components associated with the selected service

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

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
Pixel format:	The video sampling format of the selected service
Frame rate:	The video frame rate of the selected service (Hz)

Interlace:	Whether the video source is interlaced or not

Video color metadata	
Range:	Whether the range of visual content values in the video source are limited or not. ***Possible ranges:*** Full range, Narrow range
Color primaries:	The specific primary colors used to encode all colors in the video source. ***Possible color primaries:*** BT.709, BT.470 System M, BT.470 System B, G, ST 170, ST 240, Film, BT.2020, ST 428-1, ST 431-2, ST 432-1, EBU 3213
Matrix coefficients:	What matrix coefficients the video source specifies to use to convert between RGB and Y'CbCr. ***Possible matrix coefficients:*** RGB, BT.709, FCC NTSC, BT.470 System B, G, ST 170, ST 240, YCgCo, BT.2020 non-constant luminance, BT.2020 constant luminance, ST 2085, Chromaticity-derived non-constant luminance, Chromaticity-derived constant luminance, ST ICtCp
Transfer characteristics system:	What transfer characteristics system the video source specifies to use to convert between RGB and Y'CbCr. ***Possible transfer characteristics systems:*** BT.709, Gamma 2.2, Gamma 2.8, ST 170, ST 240, Linear, Logarithmic, Logarithmic square root, xvYCC (IEC 61966-2-4), BT.2020 (10-bit), BT.2020 (12-bit), PQ, ST 428-1, HLG (ARIB-STD-B67)

Last QoE information (Displayed if QoE scoring is enabled)	
Updated:	Indicates the time when QoE scores were last generated.
Blockiness:	Detected picture blockiness, in percent.
Blurriness:	Detected picture blurriness, in percent.
Noisiness:	Detected picture noisiness, in percent.
Brightness:	Detected picture brightness, in percent.
Contrast:	Detected picture contrast, in percent.
MOS score:	Calculated picture quality score, on a scale from 1.0 to 5.0, where 5.0 is best.

Audio PID/Component

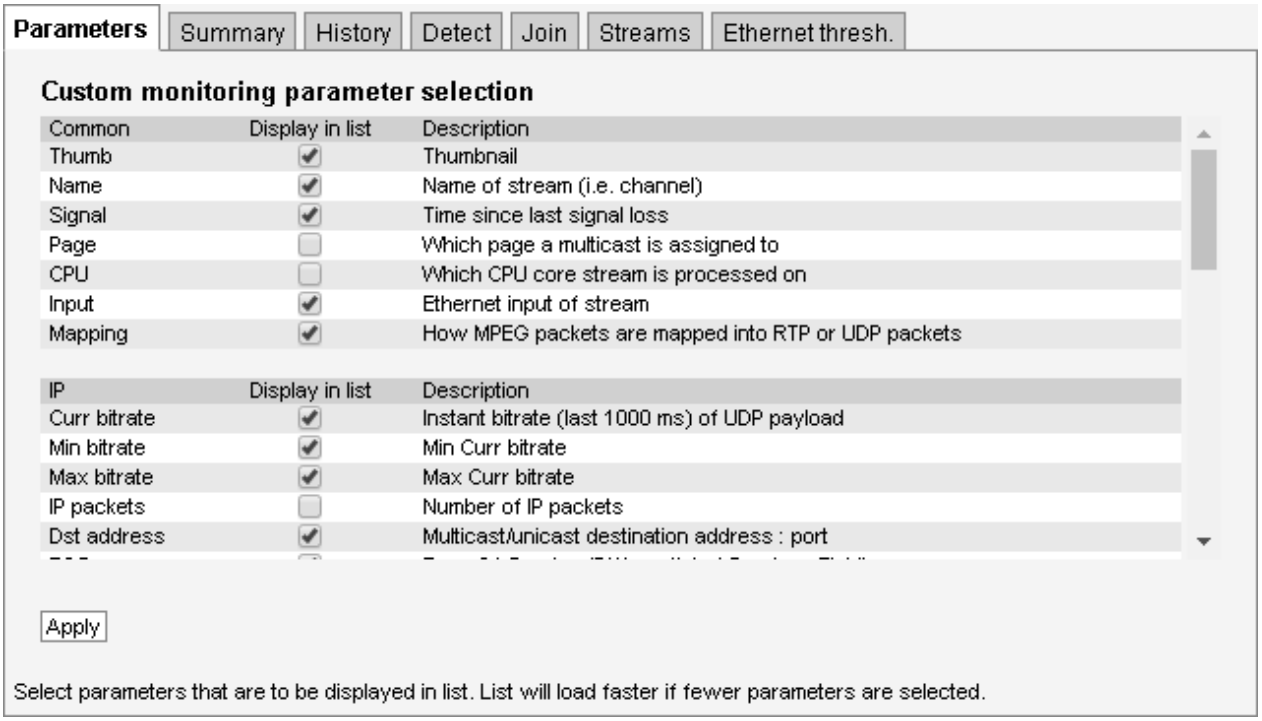
PID/Component:	The audio PID of the selected service for MPEG-TS services, or the audio component number for non-TS services Note that there may be several audio PIDs or components associated with a service
Type:	The audio encoding standard
Has PCR:	Yes if the selected Audio PID contains PCR
Bitrate:	The audio bitrate for this PID or component (bit/s)
Language:	The language of the audio, as defined in the MPEG-TS Program Map Table (PMT)

Audio Information PID/Component	
Codec:	The audio encoding format
Sample rate:	The audio sample rate (Hz)
Channels:	The number of audio channels represented by the audio PID or component
Layout:	The audio channel layout

Subtitle PID/Component	
PID/Component:	The subtitle PID of the selected service for MPEG-TS services, or the subtitle component number for non-TS services Note that there may be several subtitle PIDs or components associated with a service
Type:	The subtitling standard
Has PCR:	Yes if the selected subtitle PID contains PCR
Bitrate:	The subtitle bitrate for this PID or component (bit/s)
Language:	The language of the subtitle, as defined in the MPEG-TS Program Map Table (PMT)

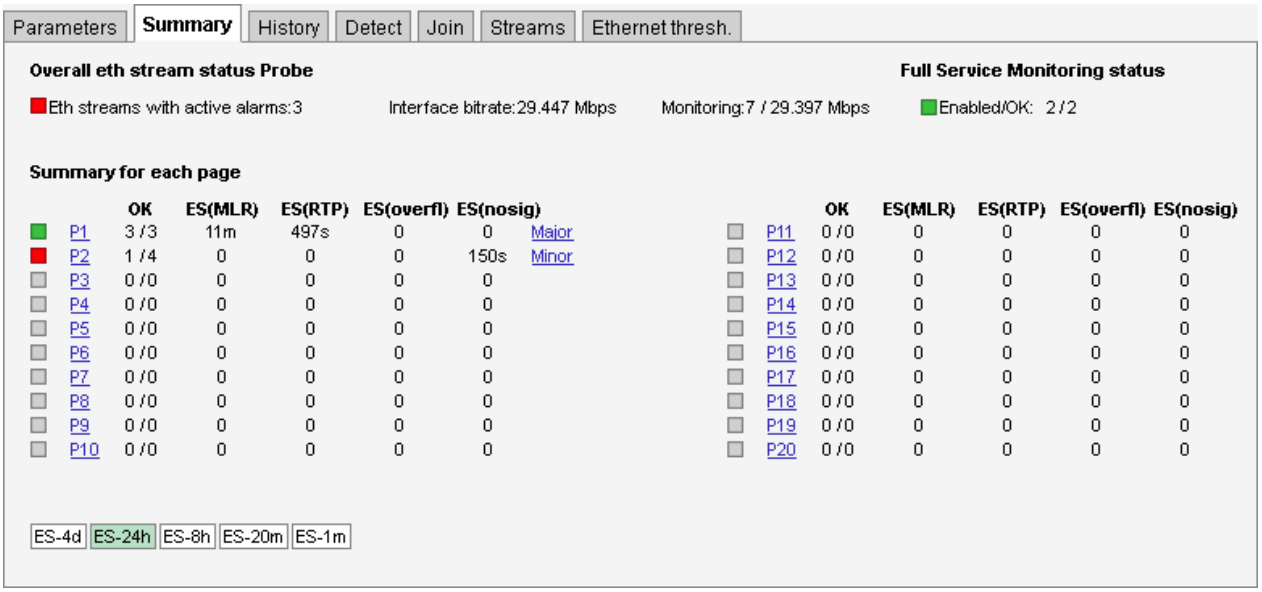
Subtitle Information PID/Component	
Codec:	The subtitle encoding format
Size:	The video picture size of the selected subtitle

5.4.2 Multicasts — Parameters — Fields



The **Multicasts — Parameters — Fields** view enables selection of the parameters to be displayed in the **Multicasts — Parameters** view. They are only in effect when *User-defined parameters* is selected as shown in **Multicasts — Parameters**. 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 ServiceMonitoring 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.

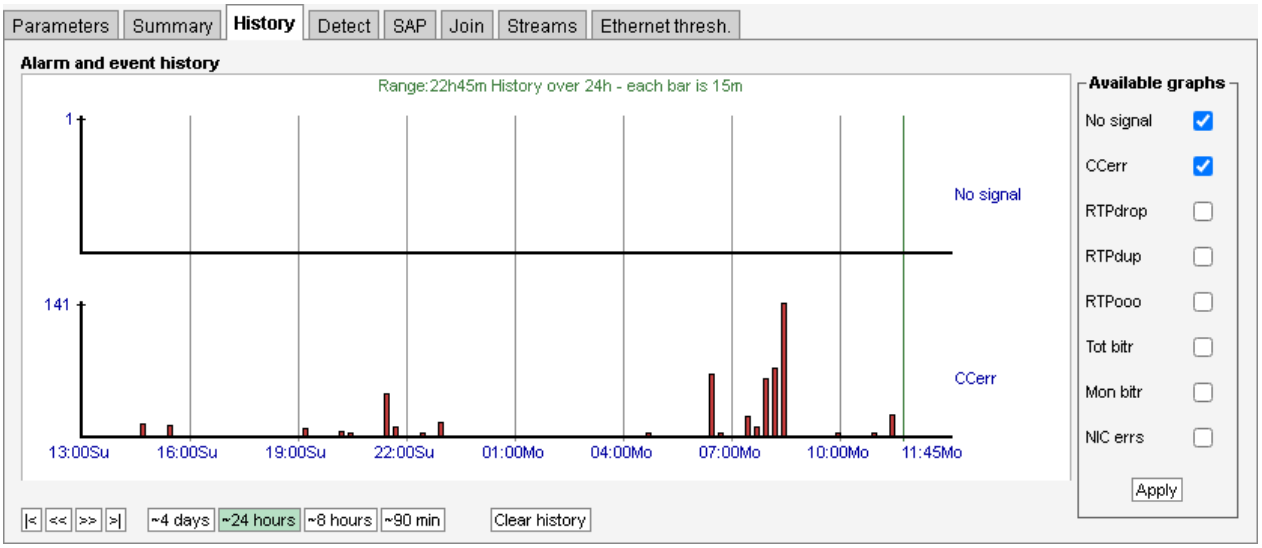
The error-second statistics interval is selected by clicking the buttons. For example, clicking the **ES–8h** button will present error-seconds for the last 8 hours. If 10 streams for a page have been without signal for the last 8 hours, the **nosig** will show as 80hours.

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.

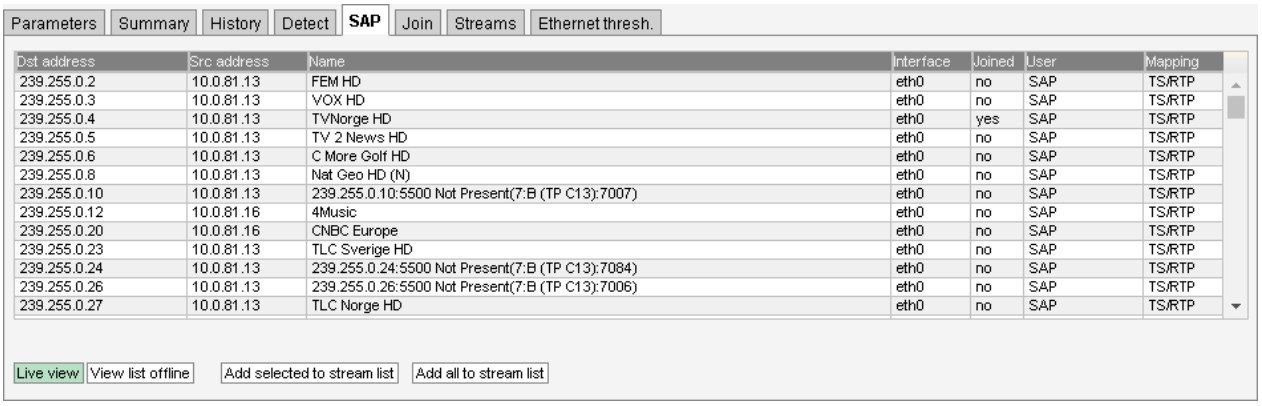
RTPdrop:	Accumulated number of dropped IP-frames due to network errors in the interval represented by the bar. This parameter corresponds to the sum of **RTP drops** reported by all streams.
RTPdup:	Accumulated number of duplicate IP-frames in the interval represented by the bar. This parameter corresponds 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.
NIC errs:	Detected NIC errors. NIC errors are most likely caused by a bad cable or a misconfigured router. A NIC 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 124.

5.4.6 Multicasts — SAP



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

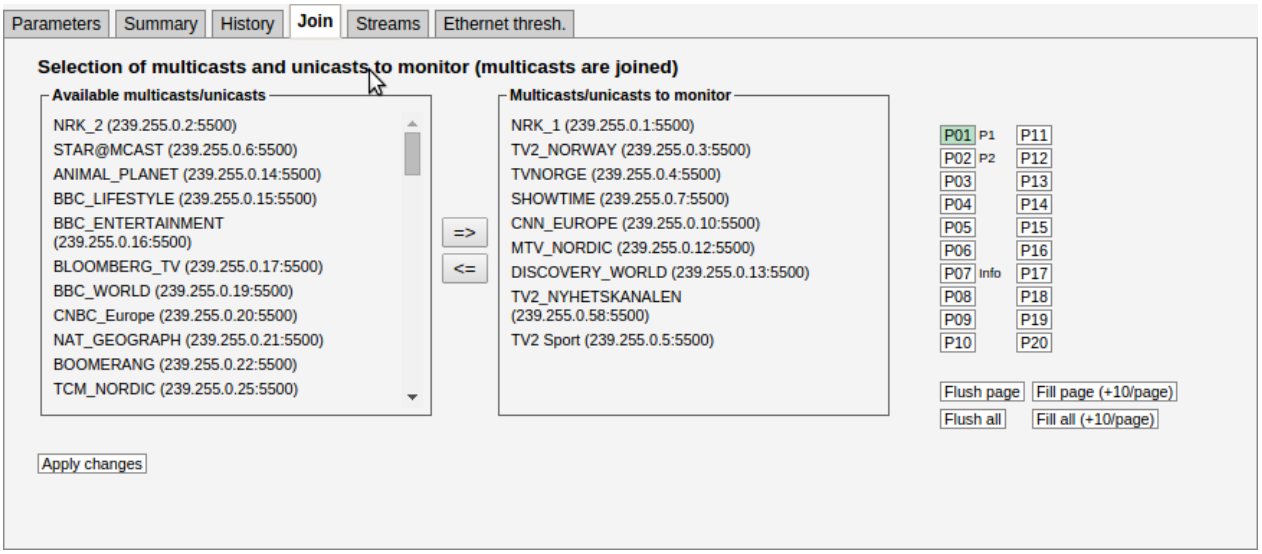
As long as **Enable SAP discovery** is enabled in the **Setup — Params** view, the VB330-SW will continuously try to detect streams. Click the **View list offline** button to view the stream list in offline mode. Click the **Refresh** button to update the stream list in offline mode.

The source address makes it possible for the 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 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.

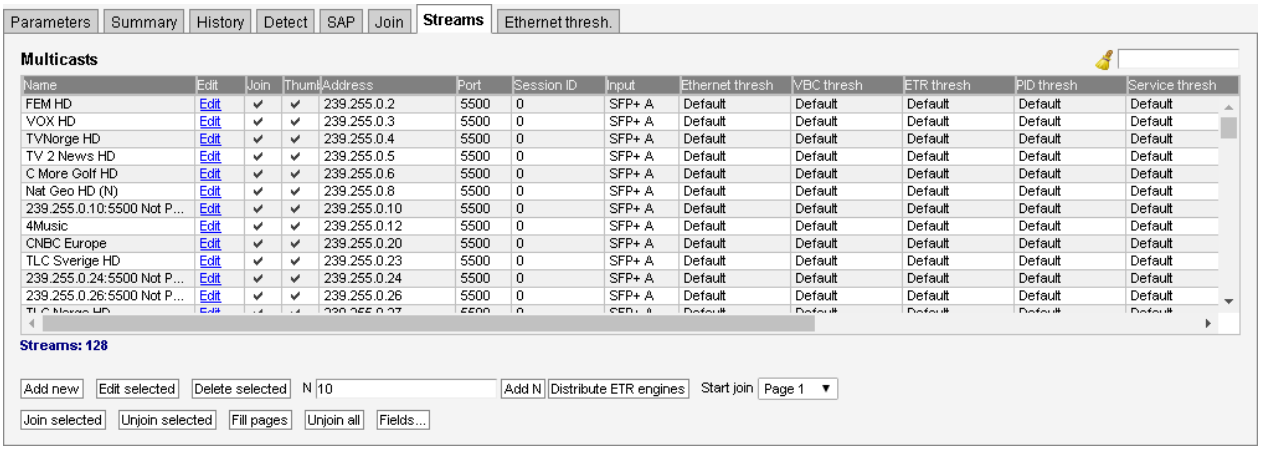
Streams defined in the **Multicasts — Streams** view will appear as available streams on the left hand side of the arrows in this view. Select streams to be monitored by clicking them and moving them to the right hand side of this view using the arrow. Changes should be confirmed by clicking the **Apply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

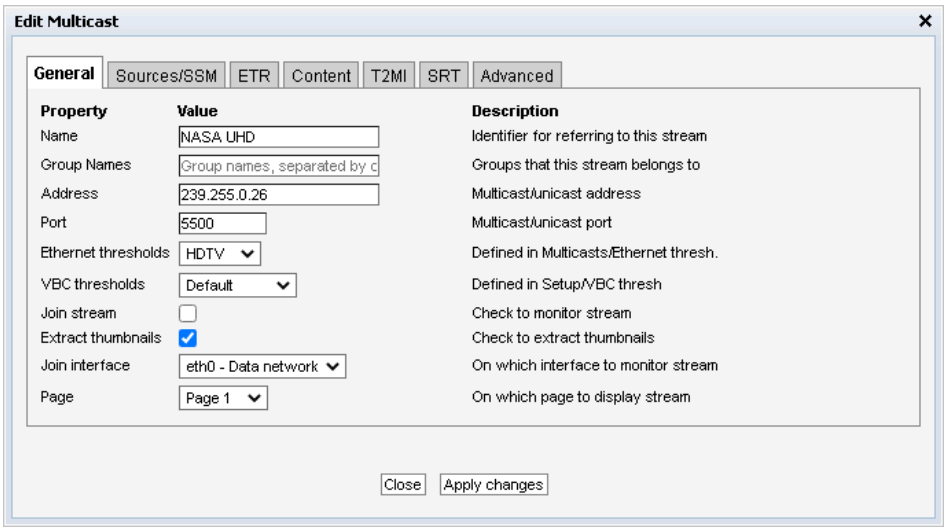
Note that both multicast and unicast addresses can be entered here.

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 VideoBRIDGE Controller.
To enable SMPTE ST 2022-7 monitoring, create two streams with the same name, but with a different class name, for each of the paths, and enable **SMPTE ST 2022-7 monitoring** on the **Advanced** tab. The class name is everything added after @ in the name.

Group Names: A comma separated list of groups this stream belongs to. The first group in this list will be used as the stream's group for EBP monitoring. See section 5.10.3.

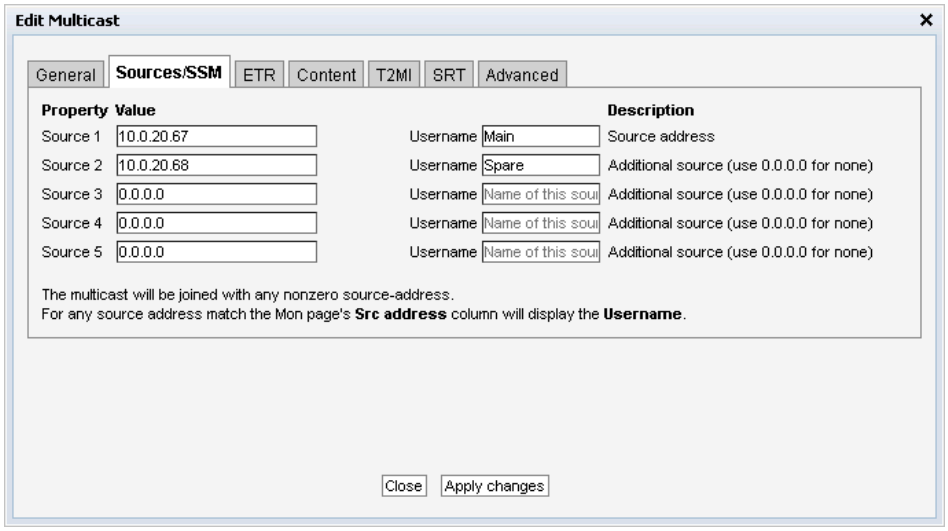
Address: The IP address of the unicast or multicast. For a SRT, T2MI inner or SMPTE ST 2022-7 combined stream, enter a dummy address that falls within the range 224.0.0.0 to 239.255.255.255.

Port: The port number of the unicast or multicast. For a SRT, T2MI inner or SMPTE ST 2022-7 combined stream, enter a dummy port number.

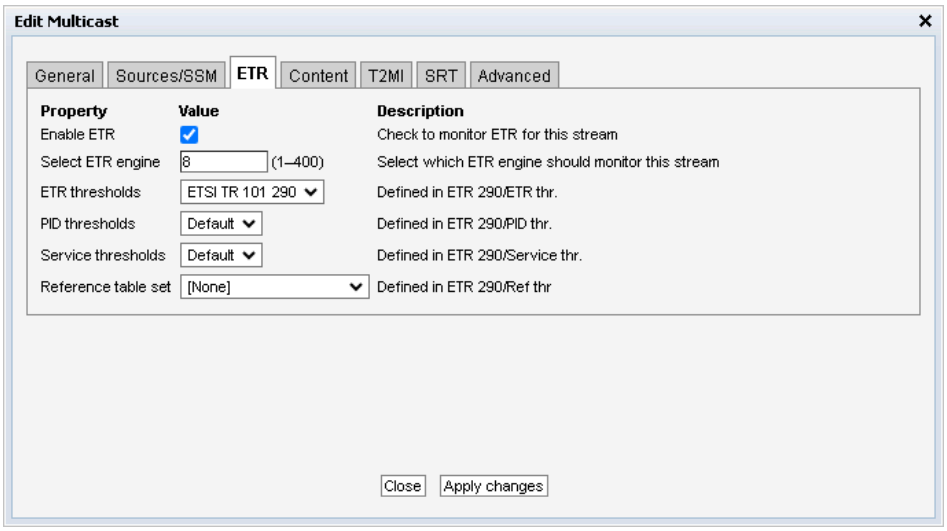
Ethernet thresholds: The Ethernet thresholds specify various error limits. Selectable Ethernet thresholds templates are defined in the **Multicasts — Ethernet thresh.** view. For a T2MI stream select a dummy threshold template.

VBC thresholds: The VBC thresholds specify various error limits to be used by VideoBRIDGE Controller to generate alarms. These thresholds are only relevant if the VideoBRIDGE Controller is used. VBC threshold templates are defined in the **Setup — VBC thresh.** view.

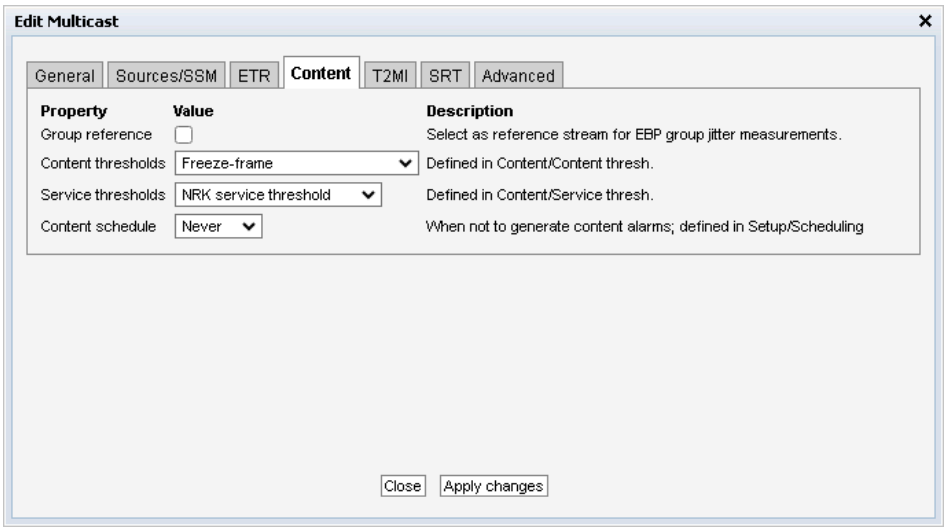
Join stream:	Check the 'Join stream' check box to join a multicast or unicast. Only joined streams are analyzed. A stream may also be joined from the **Multicasts — Join** or **Multicasts — Streams** views, and the status of this check box will be updated accordingly.
Extract thumbnails:	When enabled, 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**.



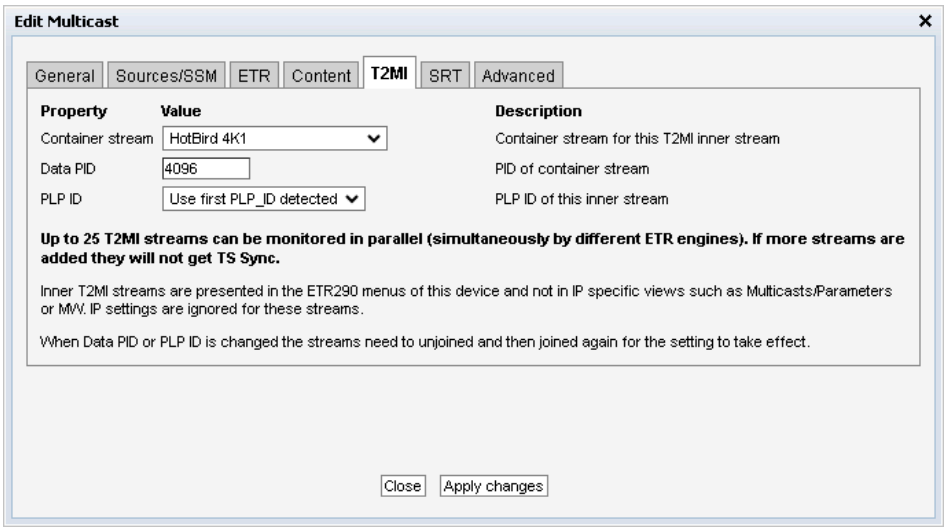
Sources/SSM	
Source 1:	If a zero source address is specified for a multicast it will be joined without a source. This allows both source specific multicasts and non-source specific multicasts to co-exist in the same network and be joined by the VB330-SW.
Source 2–5:	Additional SSM source addresses may 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.
Username:	For each of the sources listed it is possible to specify a name for this source. In the **Multicasts — Parameters** view, this name will be displayed in the **Src address** column instead of the source IP address. This can be used to easier distinguish between the main and backup transmitters etc.



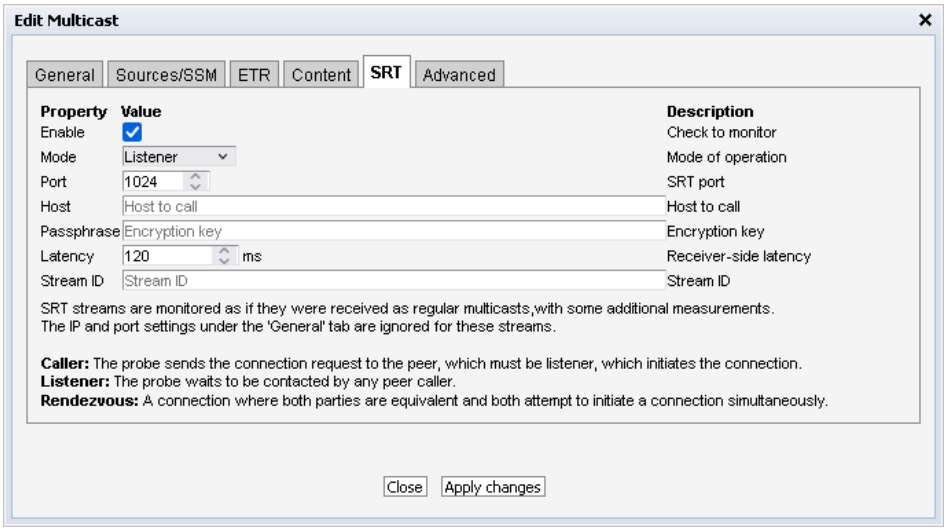
ETR (ETR290 Option)	
Enable ETR:	ETR monitoring of a stream will not take place unless it is enabled by this setting. This parameter is only relevant if the probe is ETR enabled. ETR monitoring is not supported for SMPTE ST 2022-7 combined streams.
Select ETR engine:	If the probe is licensed for several Ethernet ETR engines the user may select which engine should be used to analyze the stream. The default ETR engine selection is IPTV1. 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.



Content	
Group reference:	This option is used to set a group reference for EBP and IDR frame PTS skew measurements. A group reference's name will be emboldened in the **Content — EBP** view.
Content thresholds:	The Content thresholds specify content alarming options. Selectable Content thresholds templates are defined in the **Content — Content thresh.** view.
Service thresholds:	The Content service threshold group that should be assigned to the multicast. Content service threshold groups that have been defined in the **Content — Service thresh.** view are available for selection from the drop-down menu.
Content schedule:	The scheduling scheme that should be assigned to the content monitoring for the multicast. Scheduling schemes that have been defined in the **Setup — Scheduling** view are available for selection from the drop-down menu. Scheduling allows masking content alarms at predefined time periods. The schedules can be overridden for specific services using Content service thresholds.



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.

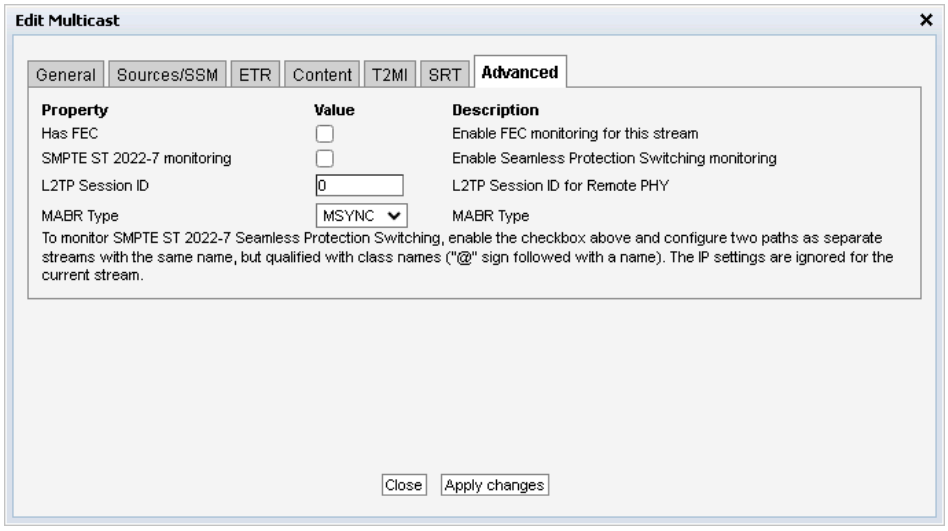


SRT	
Enable:	Enable to monitor SRT stream
Mode:	The mode of operation the probe should use; either a *Listener*, a *Caller* or *Rendezvous*.

Port:	The port number to receive the SRT stream through.
Host:	The host address of the SRT stream source. (ignored for Listener mode)
Passphrase:	In case the SRT stream you want to receive is encrypted. If left blank the stream is assumed to be unencrypted.
Latency:	Defines the minimum receiver buffering delay before analyzing the video content in an SRT data packet. A larger value gives a larger window of time for the SRT protocol to retransmit lost packets, and vice versa.
Stream ID:	A free-form string sent by a caller to the opposing listener during connection initiation. Will have no effect if set on Rendezvous or Listener mode.

The probe currently supports up to 200 concurrent SRT receive sessions. When operating SRT in **Listener** mode the probe will await an external caller to connect to the specified UDP port before data reception occurs. Select the network interface to listen on under the **General** tab.

More information on SRT streams can be found in F Appendix: SRT Streams.



Advanced	
Has FEC:	The stream carries COP3 (SMPTE ST 2022-5) Forward Error Correction. If enabled, statistics about FEC drops and correctible errors will be reported for the stream.
SMPTE ST 2022-7 monitoring:	This is a Seamless Protection Switching (SMPTE ST 2022-7) combined stream.
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.

MABR Type:	The MABR kind. Possible values are: *Disabled* and *MSYNC*. When the setting is *Disabled*, the stream is decoded normally. When set to *MSYNC*, the stream is interpreted as MSYNC. If the stream may be decoded as MSYNC, the MSYNC objects received are stored and listed in **Detailed Monitoring — MSYNC**.

Seamless Protection Switching (SMPTE ST 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.

To enable SMPTE ST 2022-7 monitoring, set up a combined stream with the **SMPTE ST 2022-7 monitoring** checkbox enabled. The IP settings are ignored for this stream. Then set up the two path streams, giving the same name, but with different class names. The class name is everything added after @ in the name.

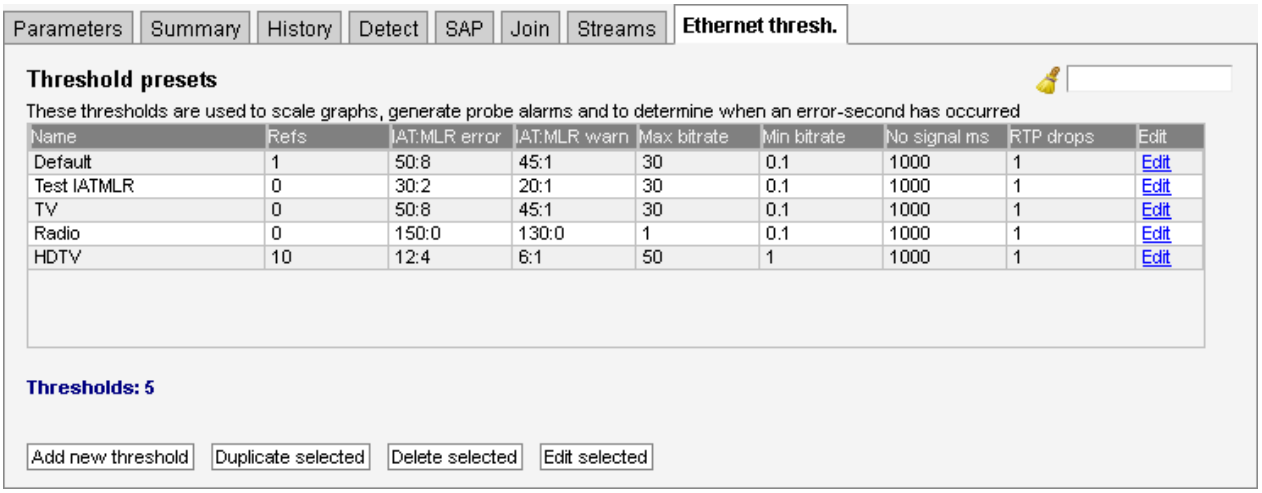
The VB330-SW supports monitoring as a receiver class C for SBR streams, as defined in SMPTE ST 2022-7:2019.

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 L2TP 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.

If the L2TP stream carries valid sequence numbers, dropped or duplicated frames will be analyzed by the Software Probe in a manner similar to RTP streams.

5.4.9 Multicasts — Ethernet thresh.

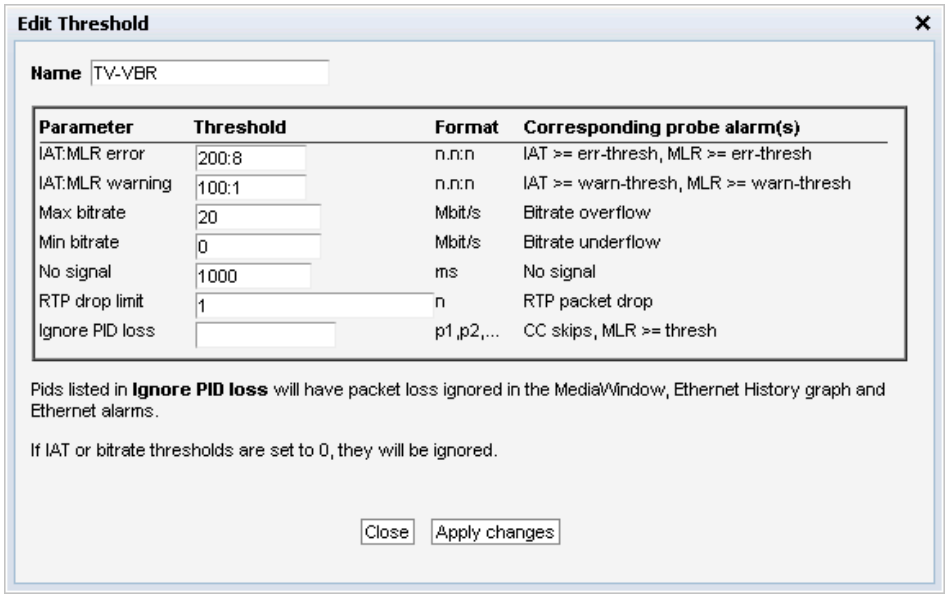


Thresholds are used to determine when to actually raise an alarm upon detection of an error. The Ethernet thresholds are used for generating Ethernet probe alarms as well as for calculating error-seconds. Error seconds and ETH probe alarms are issued whenever measurements exceed the defined threshold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

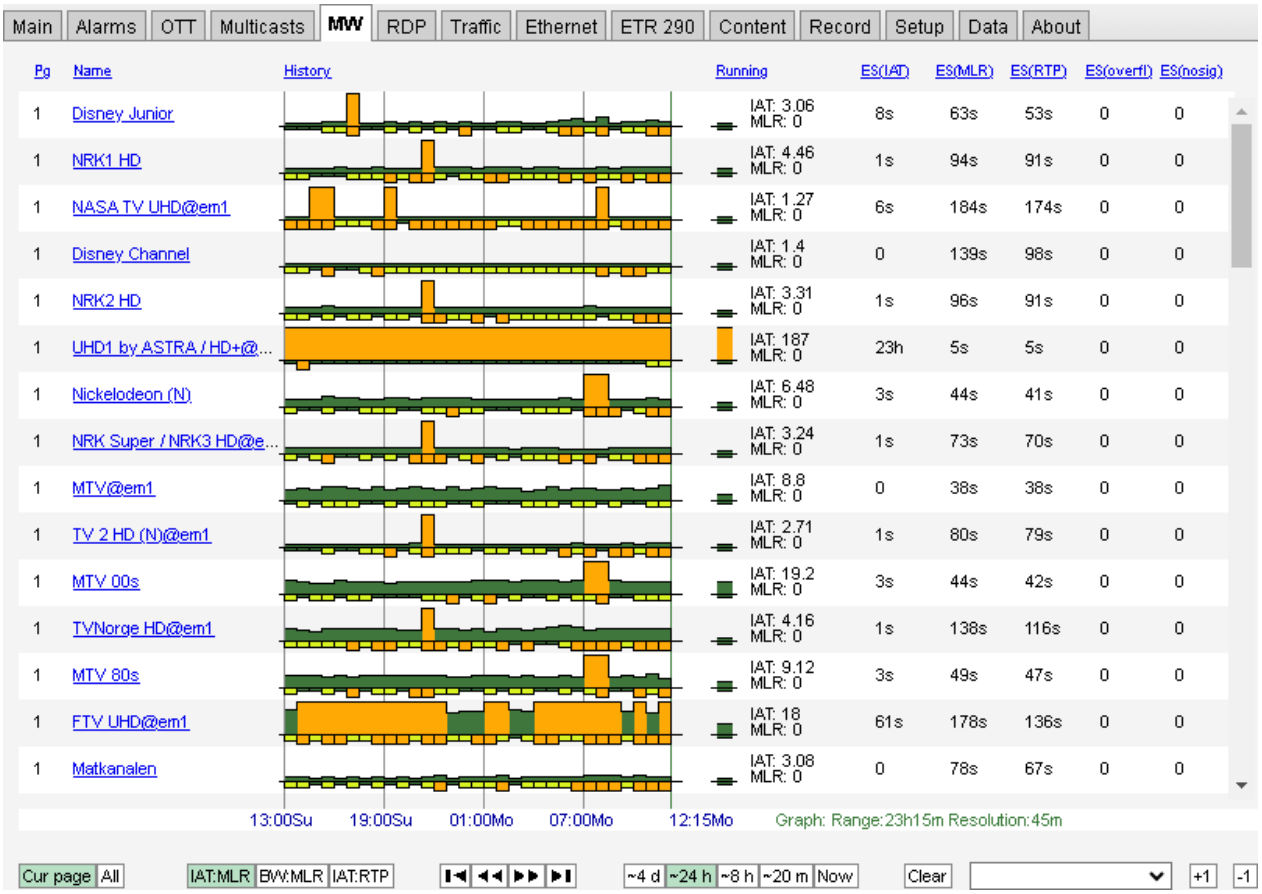
In the threshold presets list the 'Refs' column displays how many streams are associated with each stream threshold template.



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, in milliseconds, is the first parameter (before the colon), the MLR limit, in number of TS packets, 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, in milliseconds, is the first parameter (before the colon), the MLR limit, in number of TS packets, 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).

The patented Sencore VideoBRIDGE **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-

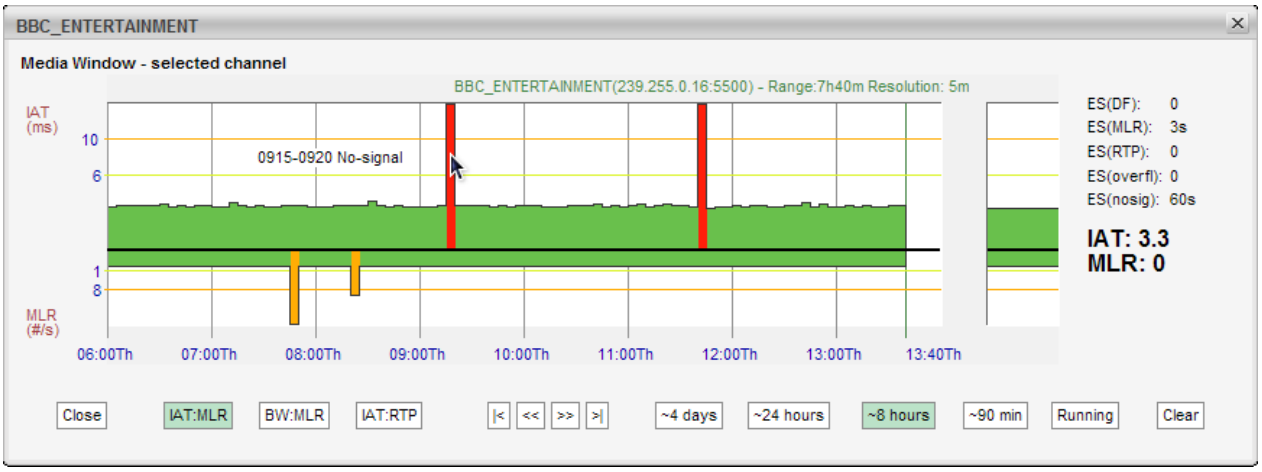
interval that depends on the range of the graph selected. Periods of no sync are also displayed in the graph.

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.

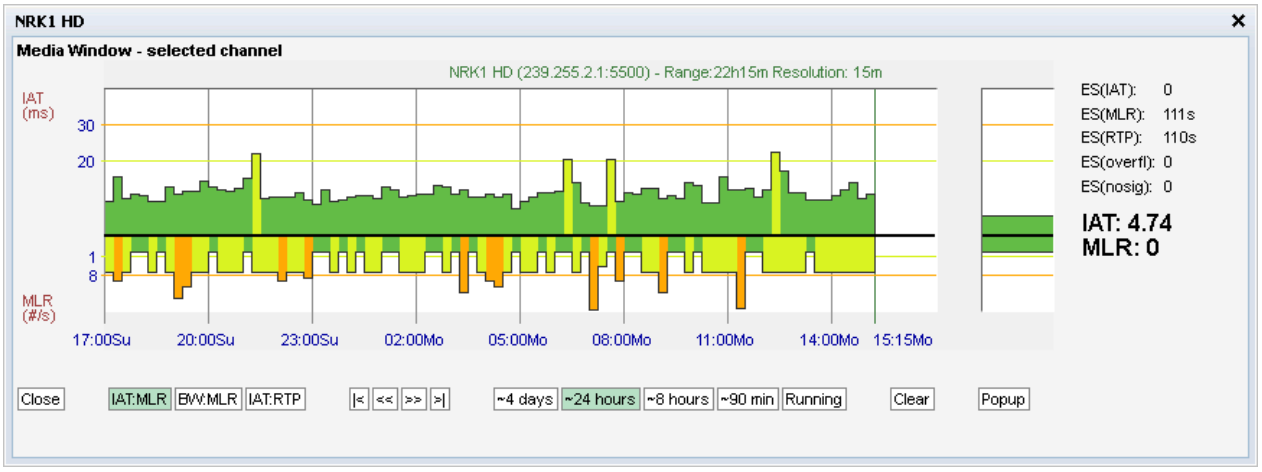
Red color is used to indicate that within the period represented by the bar there has been one or more occurrences of no-signal. Orange is used to indicate error while yellow indicates warning. The error and warning thresholds are allocated to each multicast in the **Multicasts — Streams** view.

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.



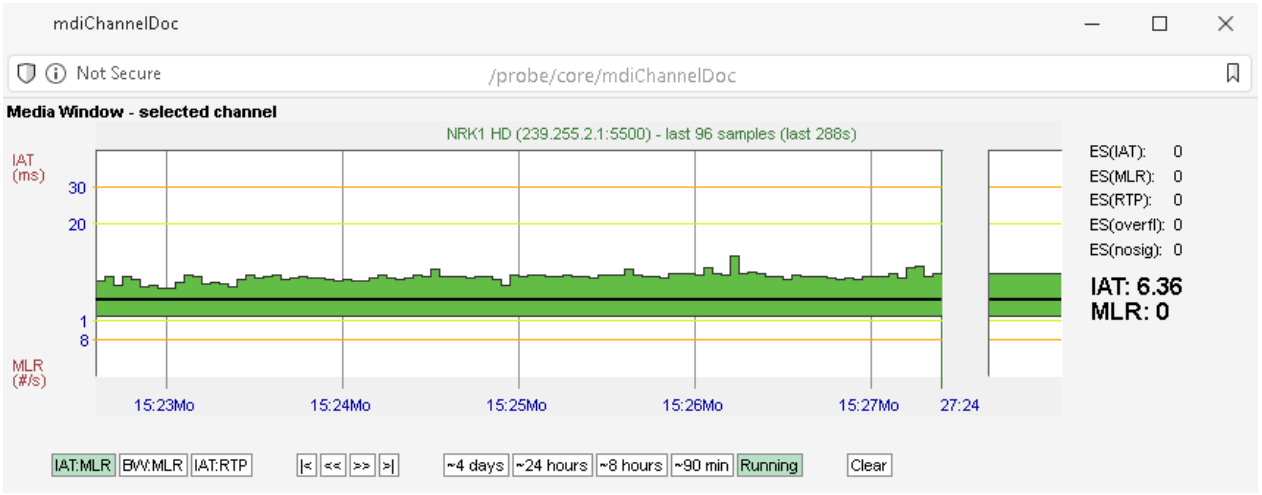
By zooming and panning the user can pinpoint more accurately when errors occurred. In the above diagram tool-tip reveals that 'No signal' occurred between 9:15 and 9:20.

5.5.1 Media Window — Selected channel



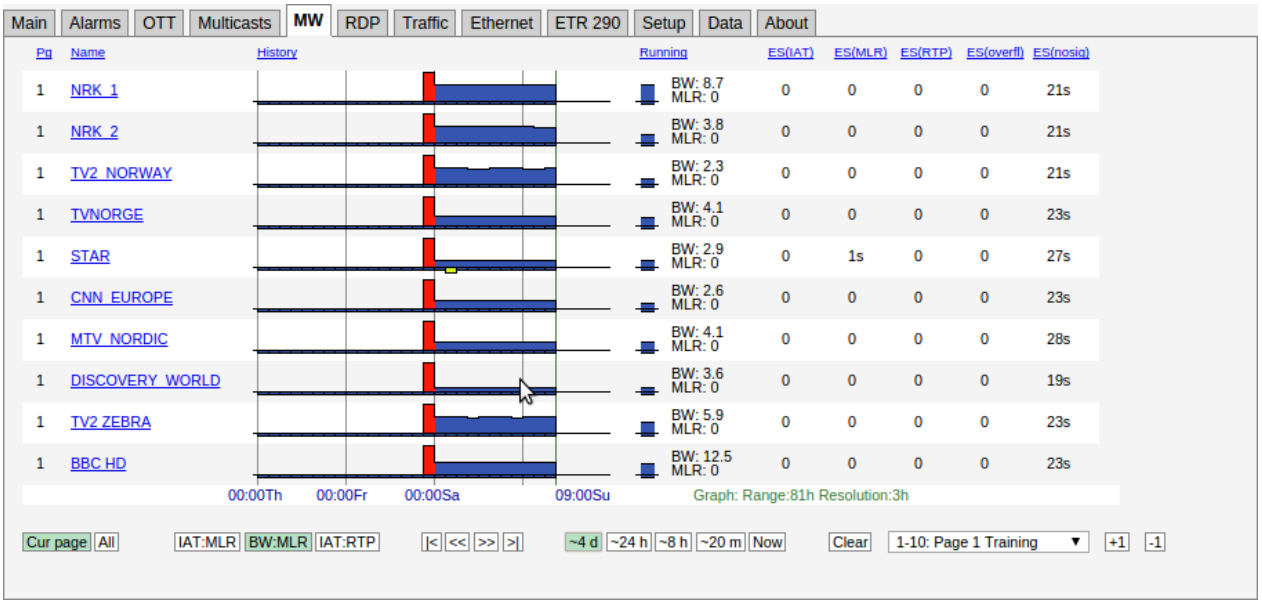
The **Media Window — selected channel** view is activated by clicking a multicast label in the **MW** page. Clicking anywhere in the running graph will zoom in, unless you already are at the maximum zoom level.

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

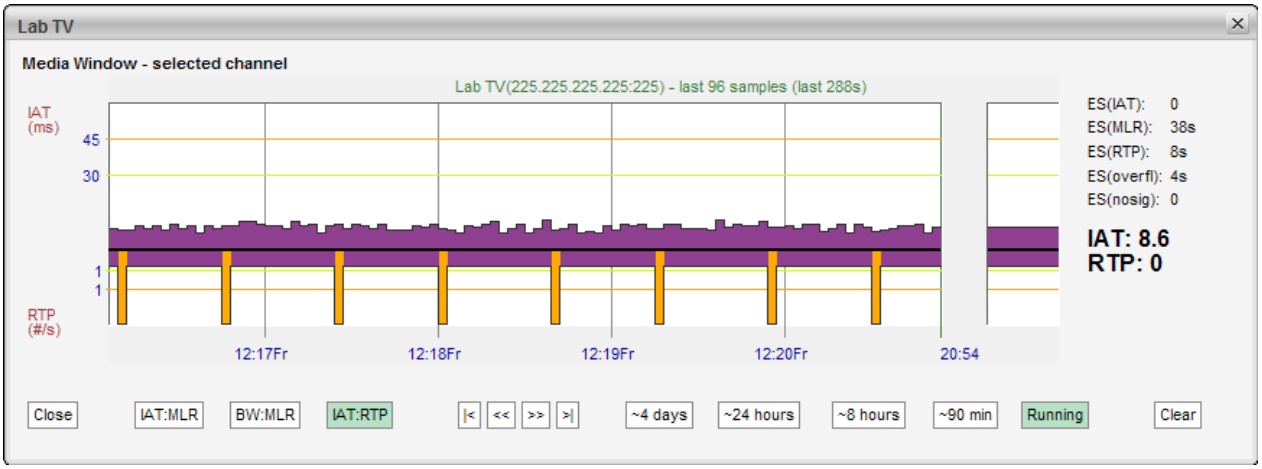


By clicking the **BW:MLR** button the graph displays the peak bandwidth as a function of time. The negative part of the composite graphs is still the packet loss (i.e. the MLR).

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

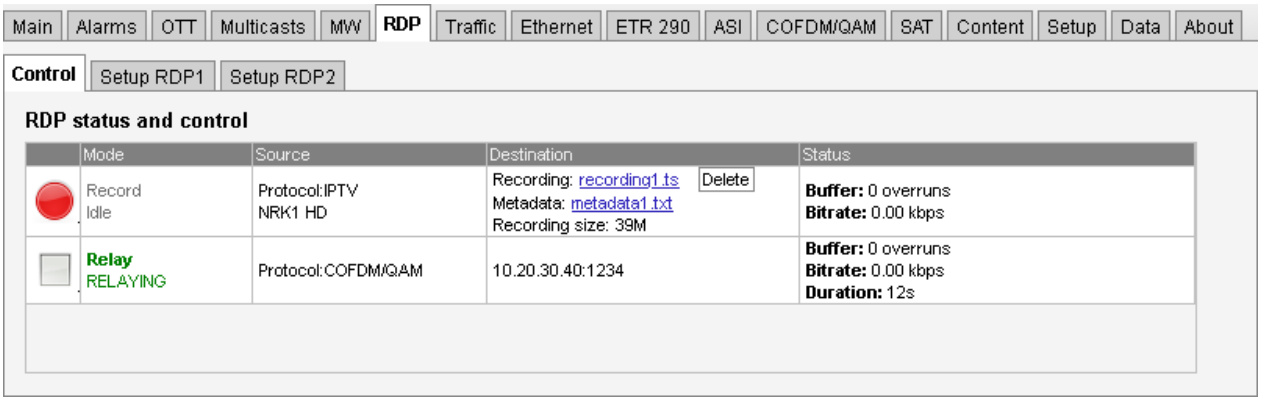


By clicking the **IAT:RTP** button the graph displays the packet jitter as a function of time. The composite graphs displays the RTP packet loss below the X-axis. If the monitored stream is not RTP encapsulated, IAT will be represented by grey color and there will never be any indication of packet loss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

5.6.1 RDP — Control



Click the icons in the **Control** view 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:

Relay	
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**, **RTP** or **SRT** 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	
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.

When encapsulation **SRT** has been selected the SRT Transmit options are:

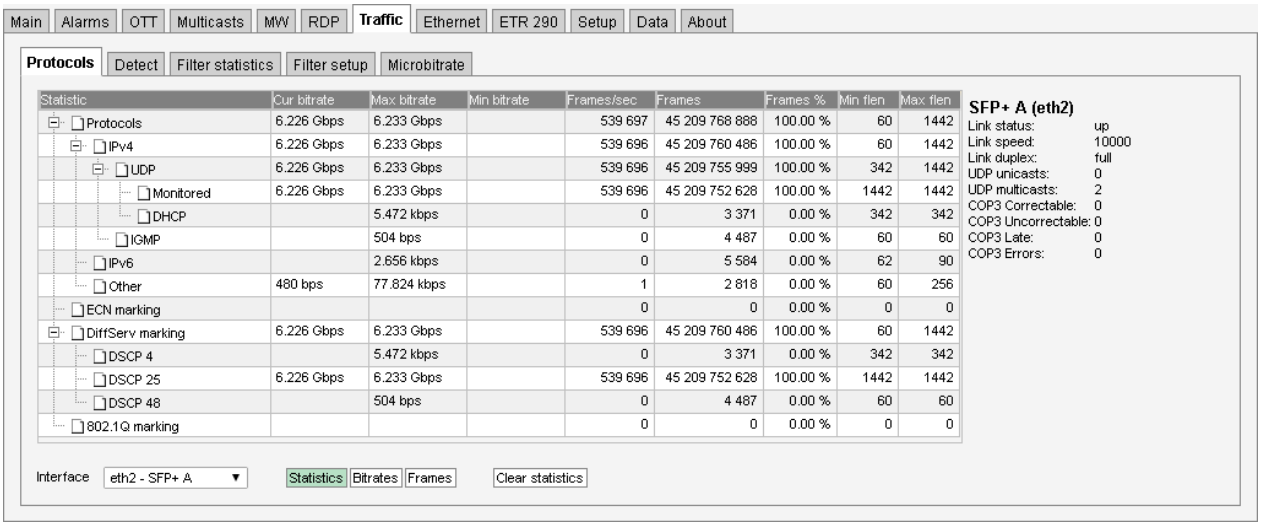
SRT configuration options

Mode:	SRT can be connected using one of three connection modes: **Caller:** the probe sends the connection request to the peer, which must be **listener**, to initiate the connection. **Listener:** the probe waits to be contacted by any peer **caller**. **Rendezvous:** the probe and the peer (which must be in **rendezvous** mode as well) both attempt to initiate a connection simultaneously.
Passphrase:	Specifies a passphrase to encrypt the forwarded stream.
Latency setting:	The latency value (milliseconds) insisted upon by the sender side as a minimum value for the receiver.

Please refer to appendix F for more details on SRT.

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

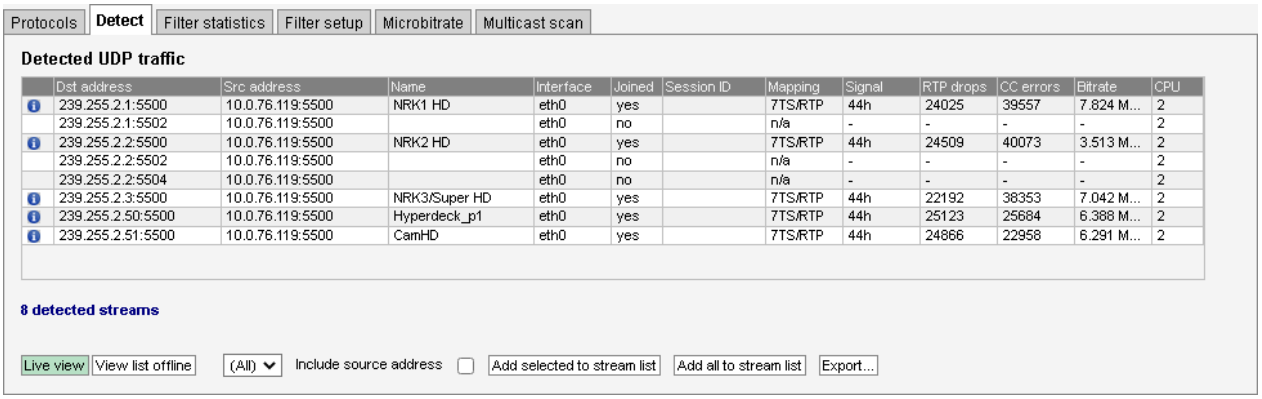
Bitrates	
Statistic:	As above
Cur bitrate:	As above
Bitrates:	A graph displaying the bitrate over time, displaying the last five minutes
Bitrate graph:	Click the bitrate graph button to display a detailed bitrate graph for the specified protocol

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 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**. If the checkbox **Include source address** is checked, the detected source address is added to the configuration, which will instruct the probe to request the stream as a source specific multicast; this setting can be configured globally in **Setup — Params**. 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.

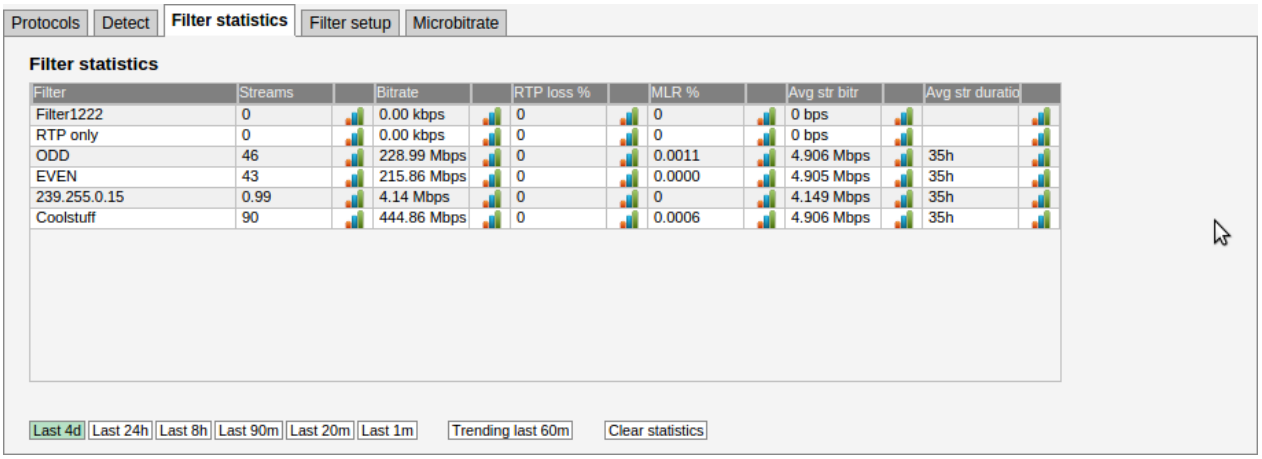
A drop down menu allows filtering of detected streams, making is possible to view streams of a specific type only. Stream types are defined in the **Traffic — Filter setup** view. If the AEO option is

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 if the stream is already monitored.
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'.
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.
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
CPU:	The probe CPU used to analyze the stream (1-7)

Please note that the **Multicast scan** and the **Detect** features are mutually exclusive, so it is necessary to click the **Exit scan mode** in the **Multicast scan** view to resume population of the **Detect** list.

5.7.3 Traffic — Filter statistics

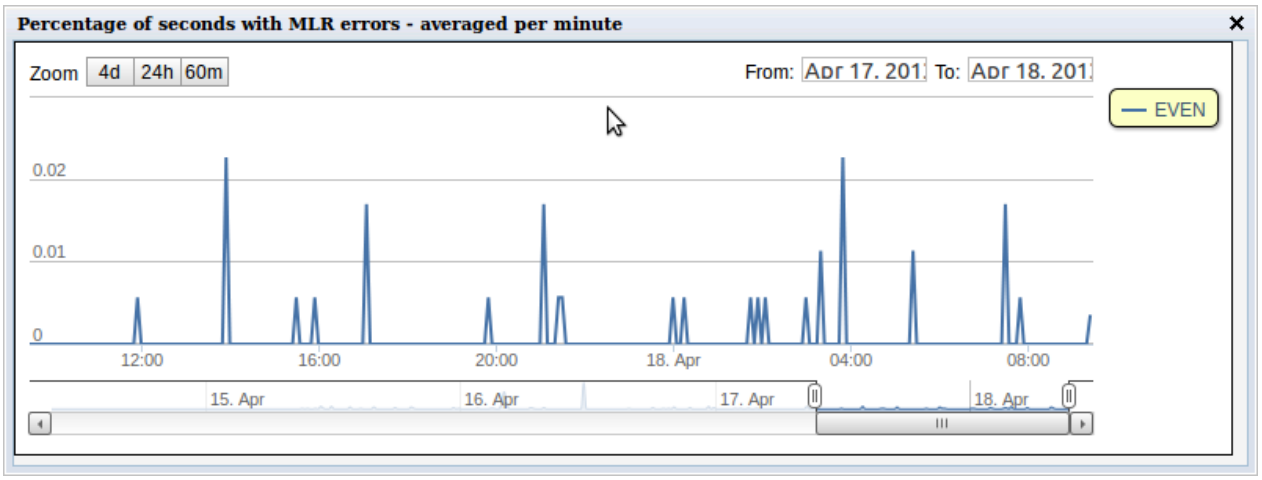


The **Traffic — Filter statistics** view makes it possible to view statistics for different stream types. Stream types are defined by the user in the **Traffic — Filter setup** view.

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, averaged over the selected time duration.
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

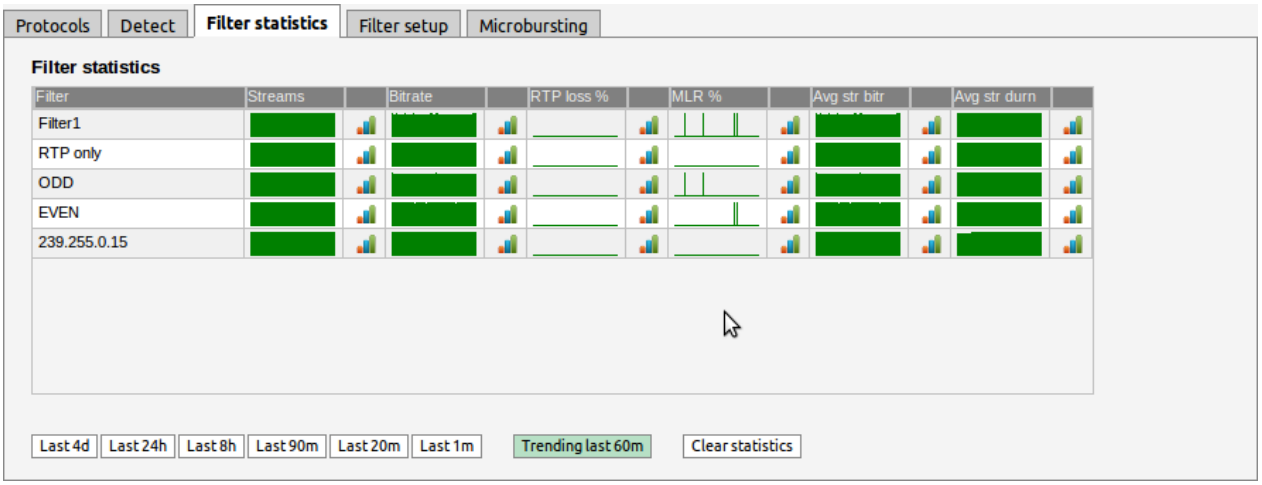
Clicking the icon next to each value brings up the detailed graph window.



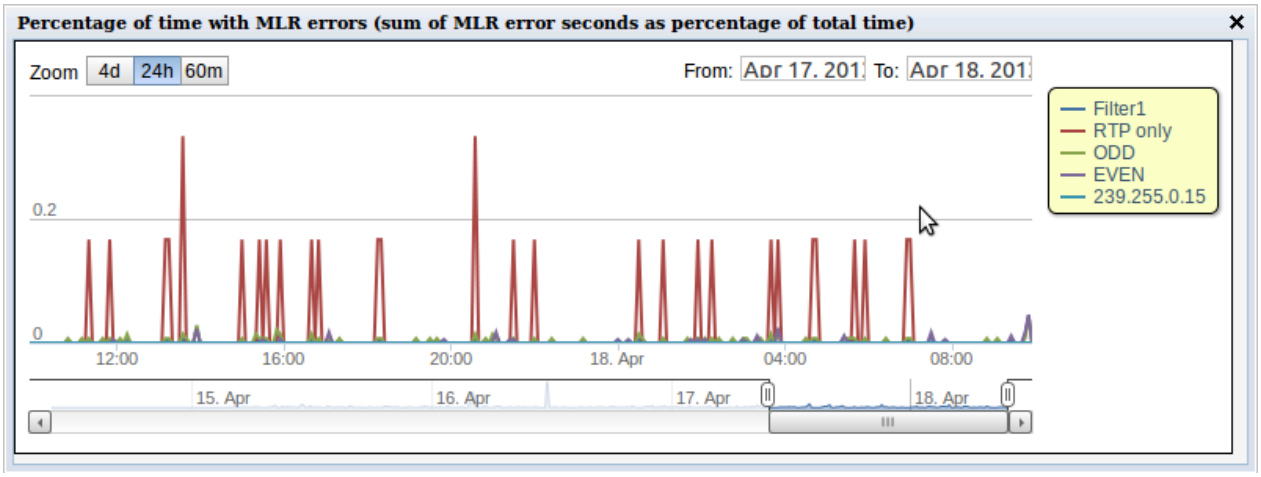
The detailed graph window displays up to 4 days of history.

Trending

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

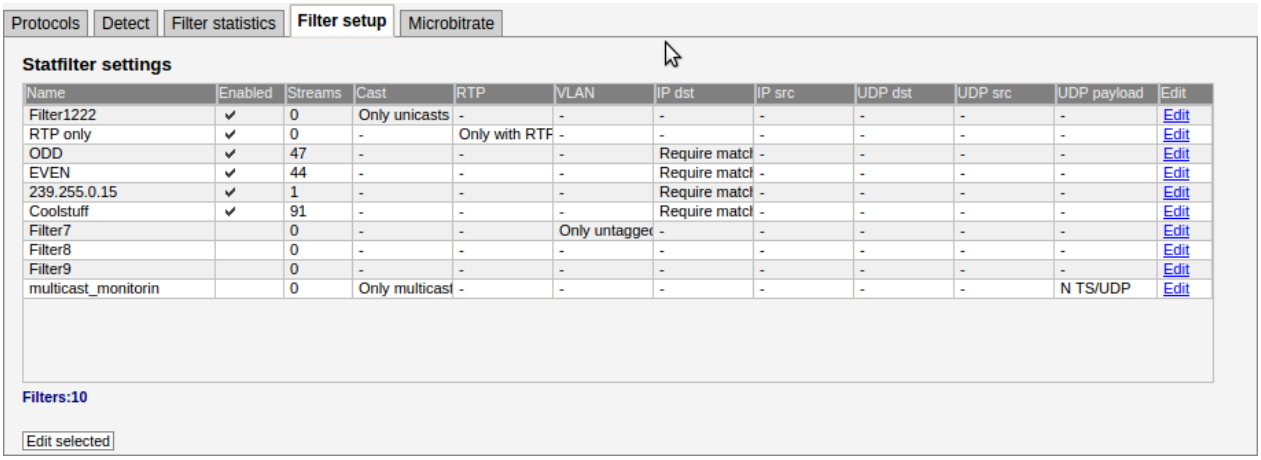


Clicking a graph icon displays the corresponding detailed graph for the selected filter. Clicking the trend graphs itself will bring up the same detailed graph but will plot all the filters so that they can easily be compared.



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

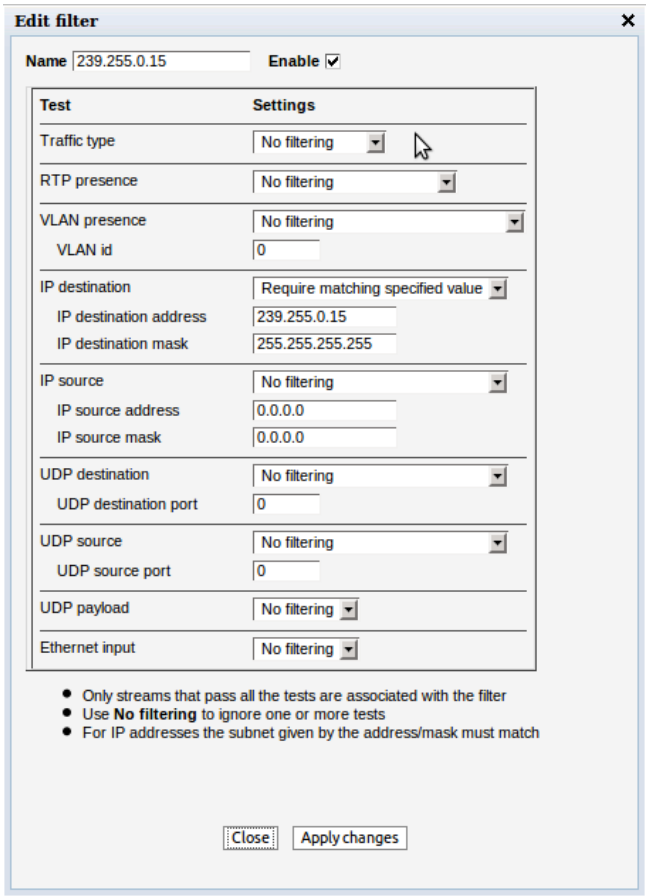
5.7.4 Traffic — Filter setup



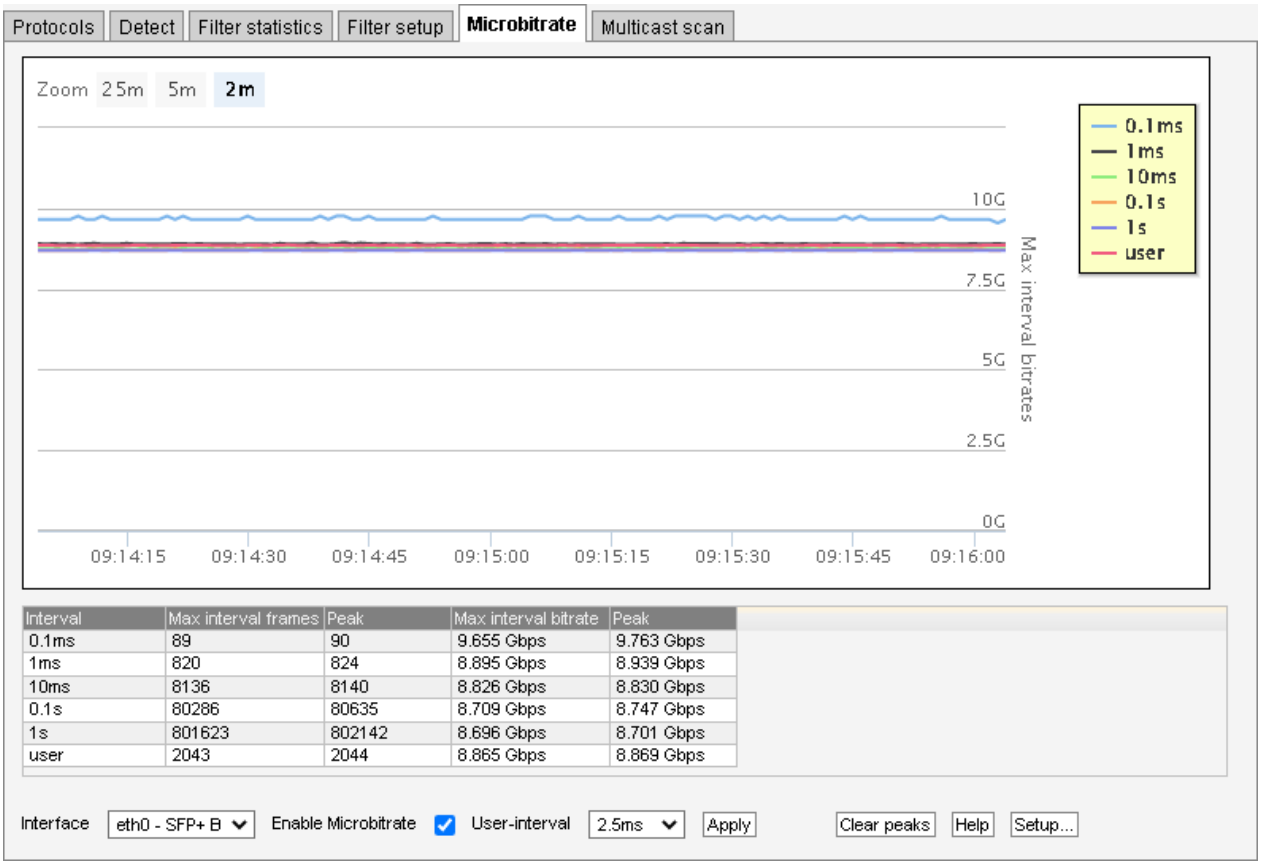
The **Traffic — Filter setup** view makes it possible to define stream filter requirements affecting the **Traffic — Detect** and **Traffic — Filter statistics** views. Ten filters can be defined and enabled by the user.

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 bitrates at various sampling intervals. Due to quantisation error, the 0.1ms interval may show higher peak values than the theoretical maximum.

The **Interval** is the sampling interval of each bitrate calculation. There are six intervals tracked simultaneously, the five pre-defined intervals and the **user-interval**. The **User-interval** is a user-given sampling interval shown in the graph and used for microbitrate alarming.

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.

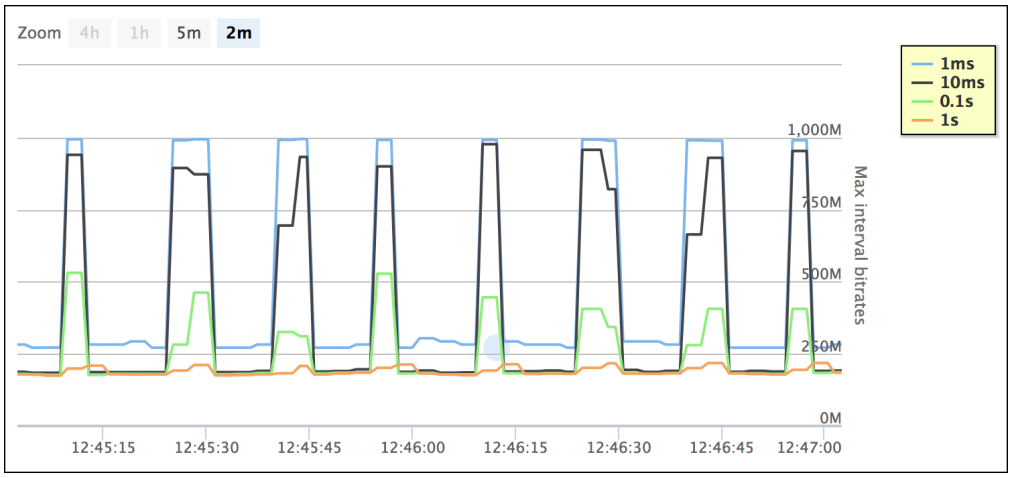


Figure 5.2: OTT traffic example

Figure 5.2 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 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.

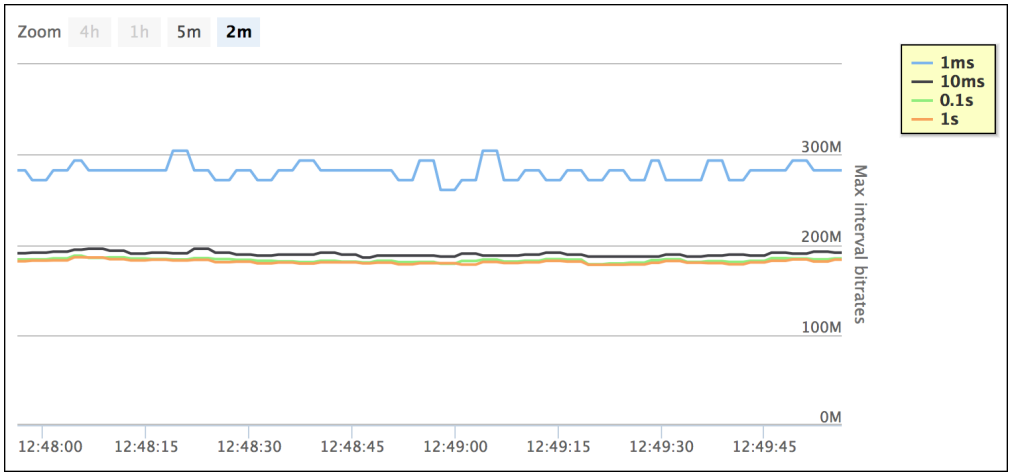
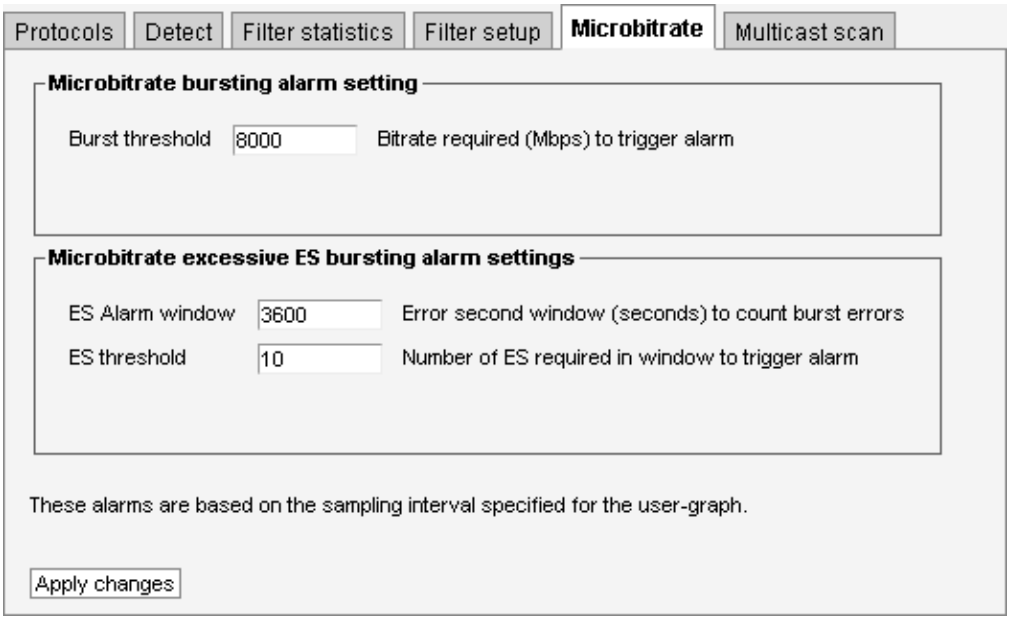


Figure 5.3: Multicast traffic example

For multicast type traffic the traffic pattern will look more like the graph in figure 5.3. 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.

Microbitrate Setup



There are two alarms defined for Microbitrate:

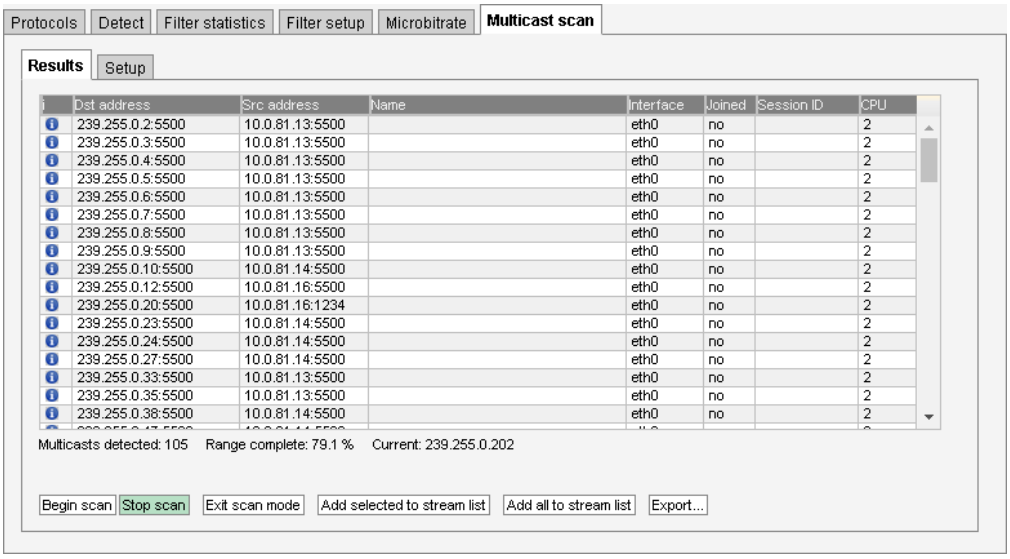
- Microbitrate bursting
- Microbitrate excessive ES bursting

These alarms are both associated with the user-interval, which is a user-specified graph sampling interval.

If the bitrate of the user-interval exceeds the **Burst threshold** setting, the **Microbitrate bursting** alarm will be raised.

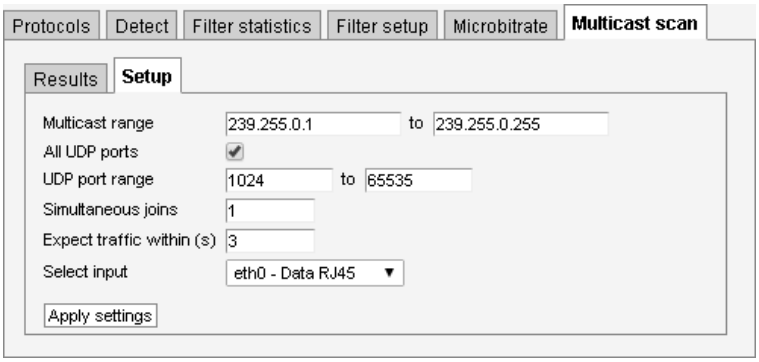
Sometimes this will yield a lot of alarms, so a second alarm has been defined. Whenever the bitrate of the user-interval exceeds the **Burst threshold** for **ES threshold** number of seconds during the **last ES Alarm window** seconds, the **Microbitrate excessive ES bursting** alarm is raised.

5.7.6 Traffic — Multicast scan



The **Multicast scan** feature is useful for scanning an IPv4 multicast interval to see which multicasts are available in the network. Detected multicasts can easily be added to the stream list. The parameters displayed are the same as in the **Traffic — Detect** view, please see chapter 5.7.2 for details.

Configure the scan interval and other scan parameters in the **Setup** view.



Setup	
Multicast range:	The multicast range to scan (IPv4 addresses).
All UDP ports:	Check this to disable filtering on UDP port.
UDP port range:	Filter to be used for UDP port unless **All UDP ports** is checked.
Simultaneous joins:	Number of joins performed simultaneously.
Expect traffic within (s):	The probe will wait this long to determine if the multicasts joined actually exist.
Select input:	Input interface to scan.

In fast networks it is useful to increase the **Simultaneous joins** to a larger number.

Please note that the **Multicast scan** and the **Detect** features are mutually exclusive, so it is necessary to click the **Exit scan mode** to resume population of the **Detect** list.

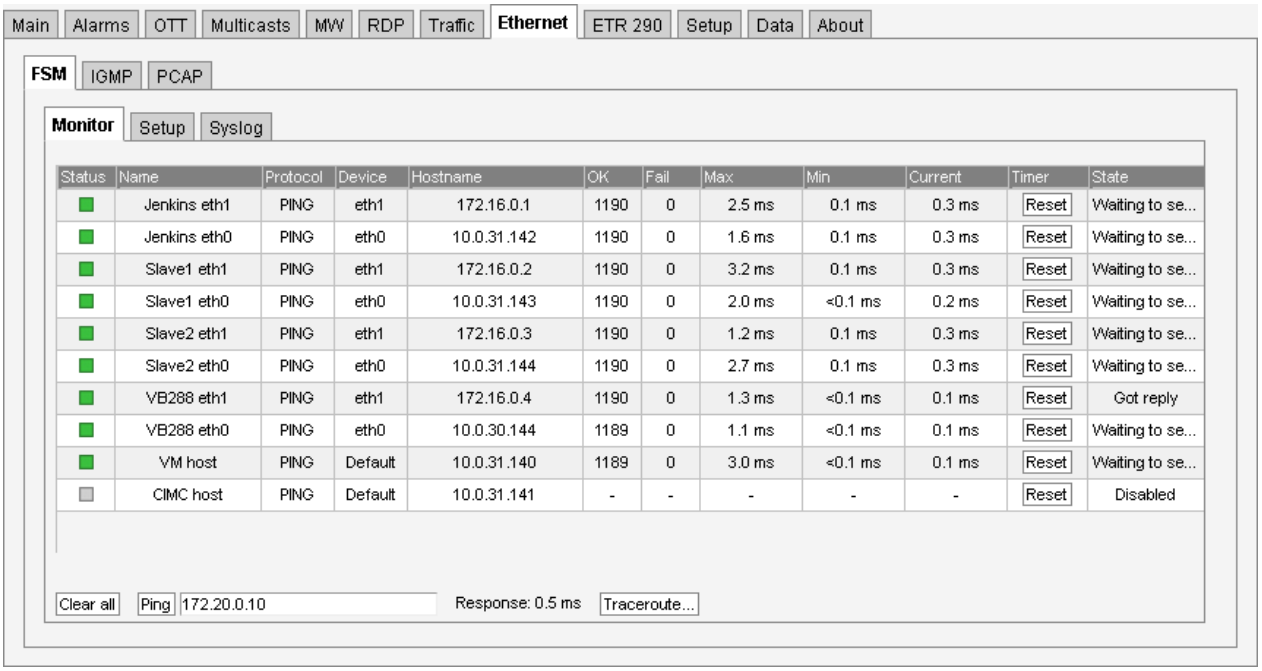
5.8 Ethernet

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

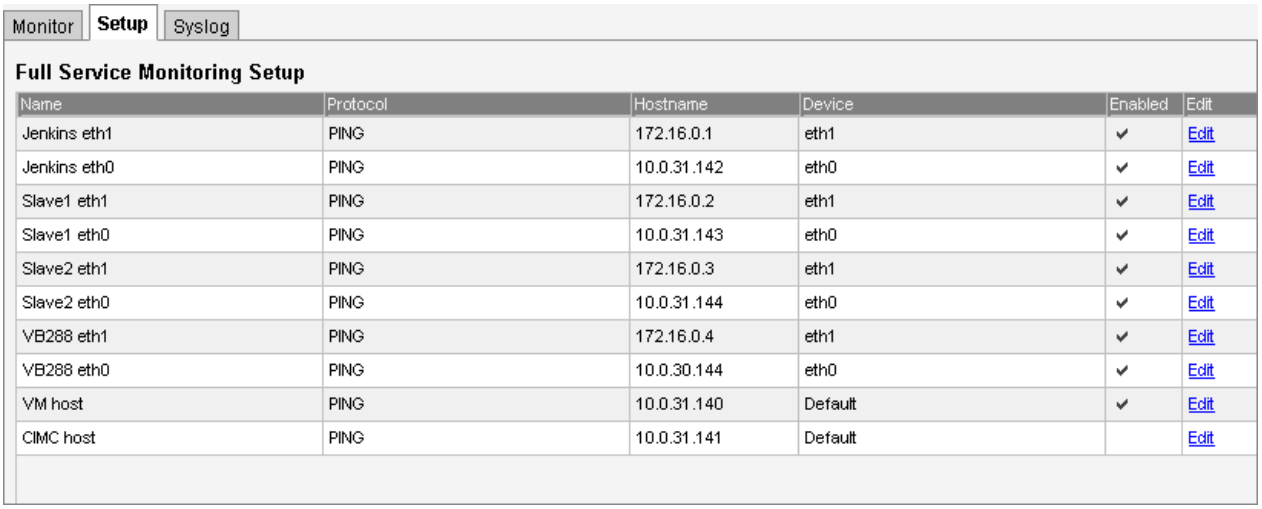
IP address:	IP address. Must be numeric, host name is not accepted
OK:	Total number of valid checks
Fail:	Total number of invalid checks
Max:	Maximum response time recorded
Min:	Minimum response time recorded
Current:	The current (most recent) response time
Timer:	Button to reset and immediately restart 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.

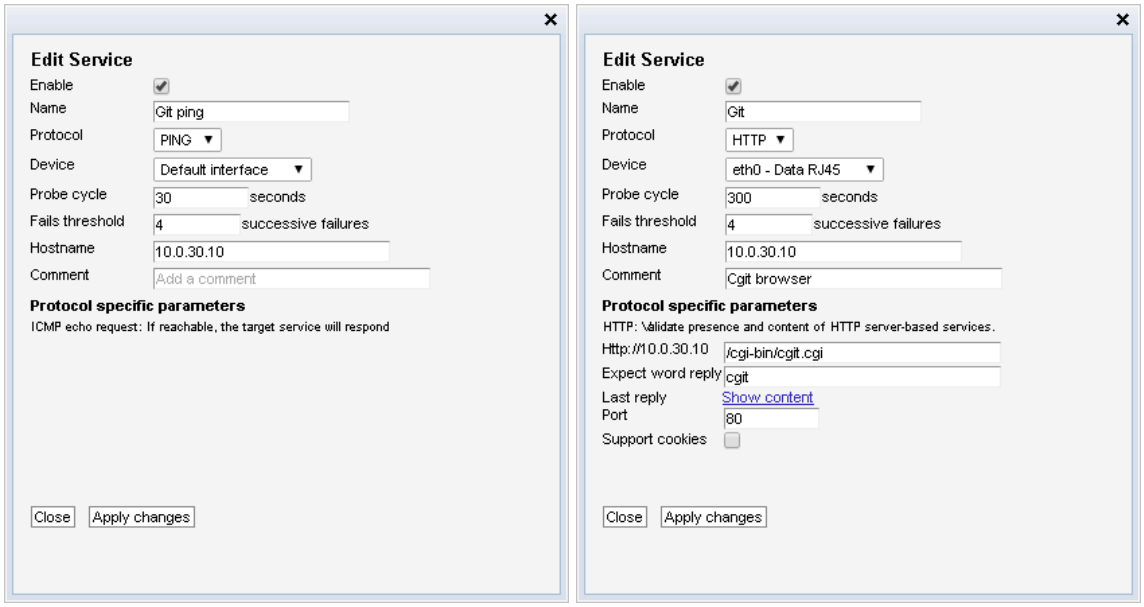
5.8.1.2 Ethernet — FSM — Setup



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:

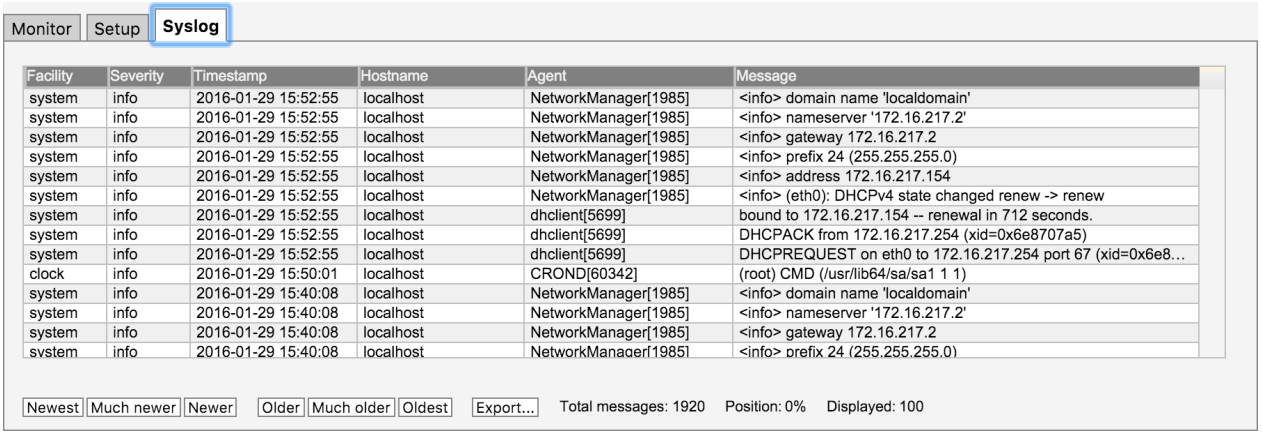
Enable:	Enable by checking toggle button.

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.

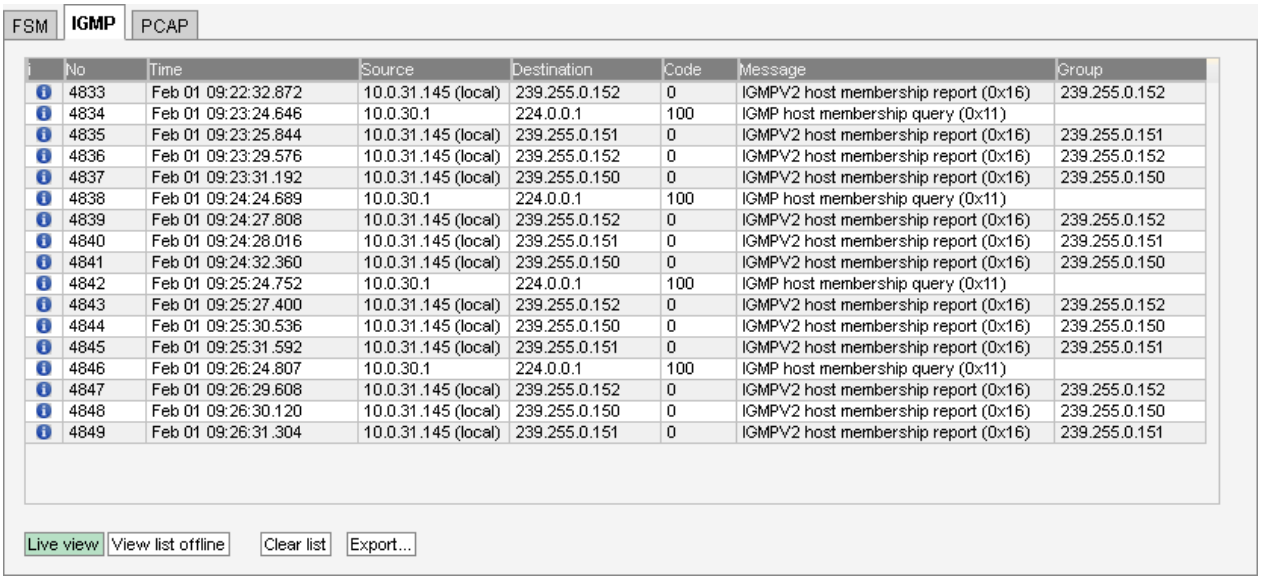
Since the syslog server typically stores about 100 pages of messages there is a group of buttons for a fast navigation:

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

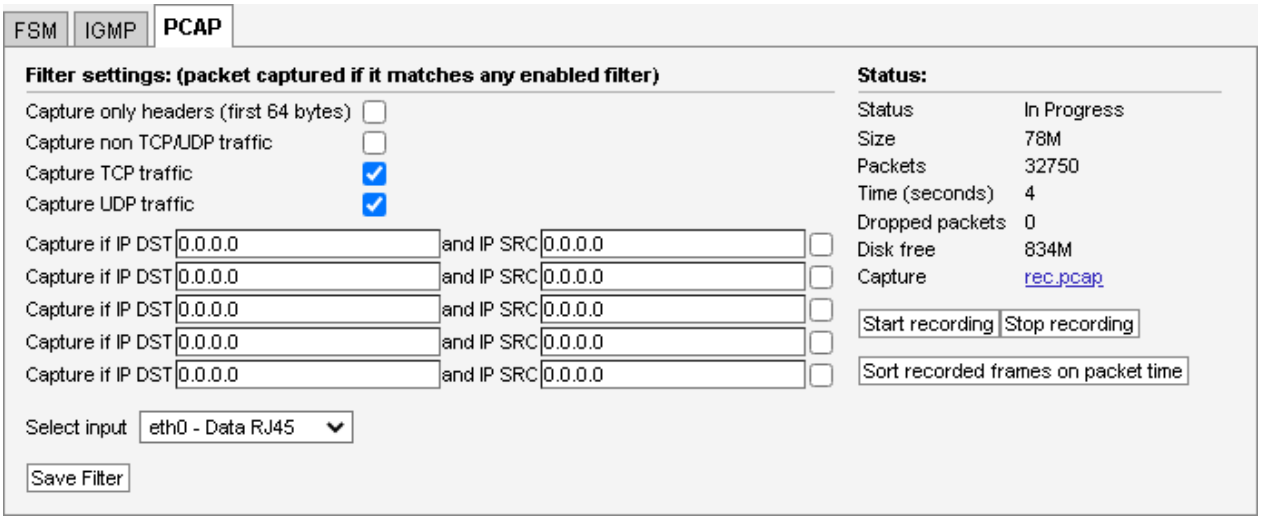
The IGMP view shows all IGMP (version 2 or 3) messages detected by the probe. This includes IGMP query messages sent by routers, IGMP reply messages sent by the probe itself and IGMP reply messages sent by other probes and devices on the same subnet.

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. If the DATA-LOG option is available, the recorded PCAP files can be moved to the internal hard drive using the **Data — Storage** view. 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).

Filter settings	
Capture only header (first 64 bytes):	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
Select input:	Chooses the network interface to capture traffic on

Status	
Status:	Show the current recording status
Size:	Size of current recording
Packets:	Number of packets in the recording
Time (seconds):	Duration of the 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.
Disk free:	Remaining disk size
Capture:	Link to download 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.

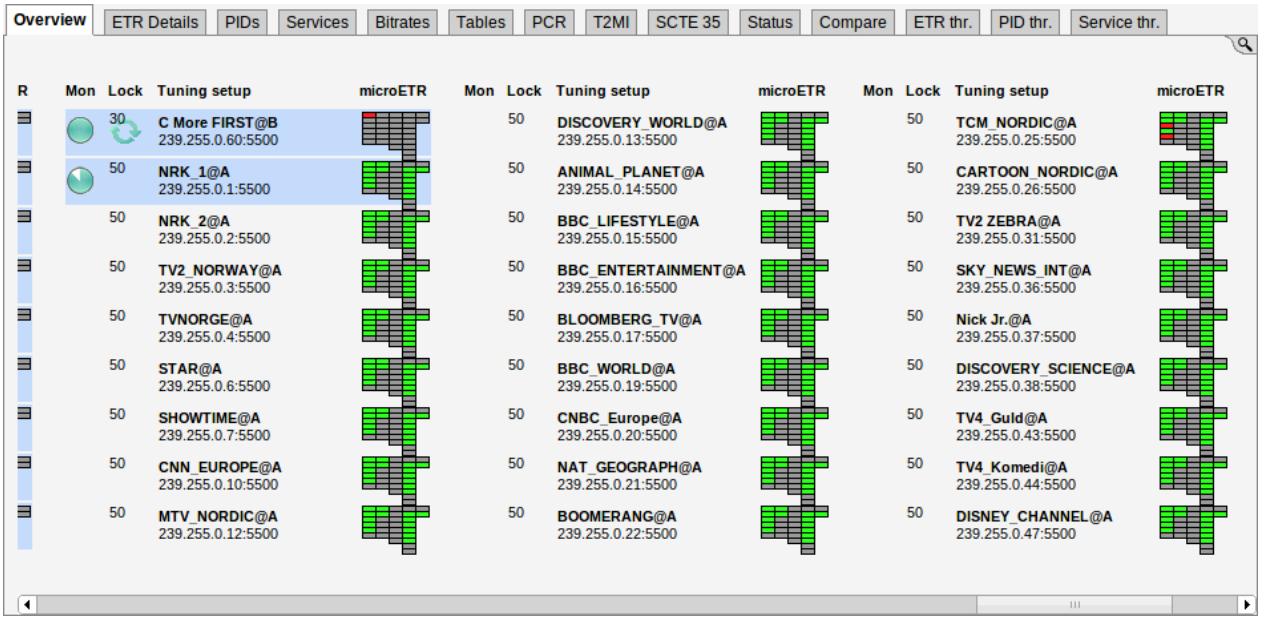
The ETR 290 views show information as reported by the ETSI TR 101 290 monitoring engines.

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 1000 engines. 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 — Overview



The **ETR 290 — 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. Click the magnifying glass icon to open a search field, making it possible to filter the list of monitored streams.

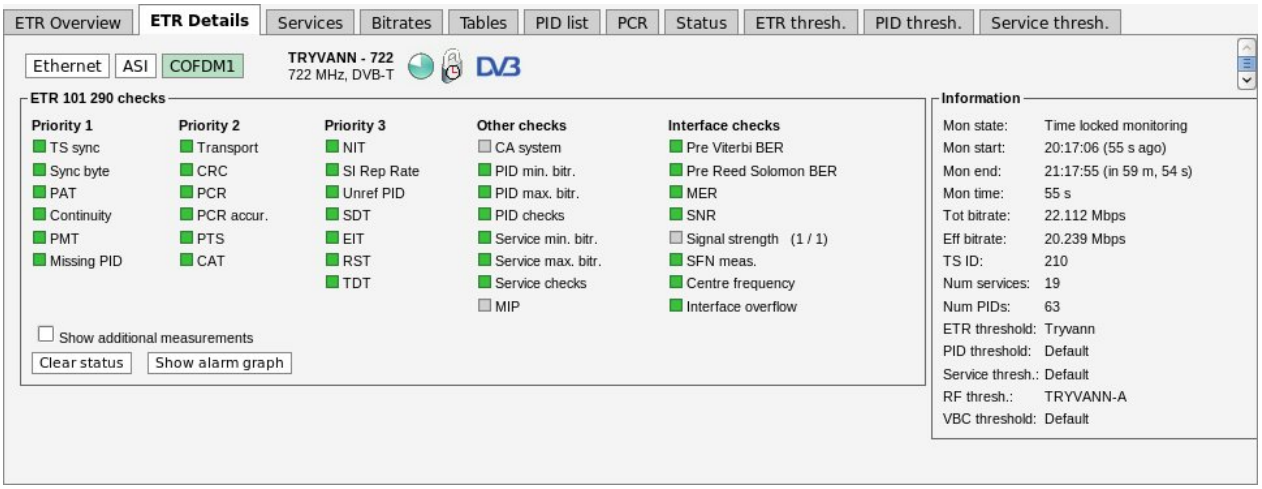
Note that it is possible to deactivate individual ETR 290 alarms by defining appropriate **ETR thresholds**.

To examine one particular Ethernet stream in more detail, 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. Click **Show all inputs** to again display information about all inputs.

5.9.2 ETR 290 — ETR Details

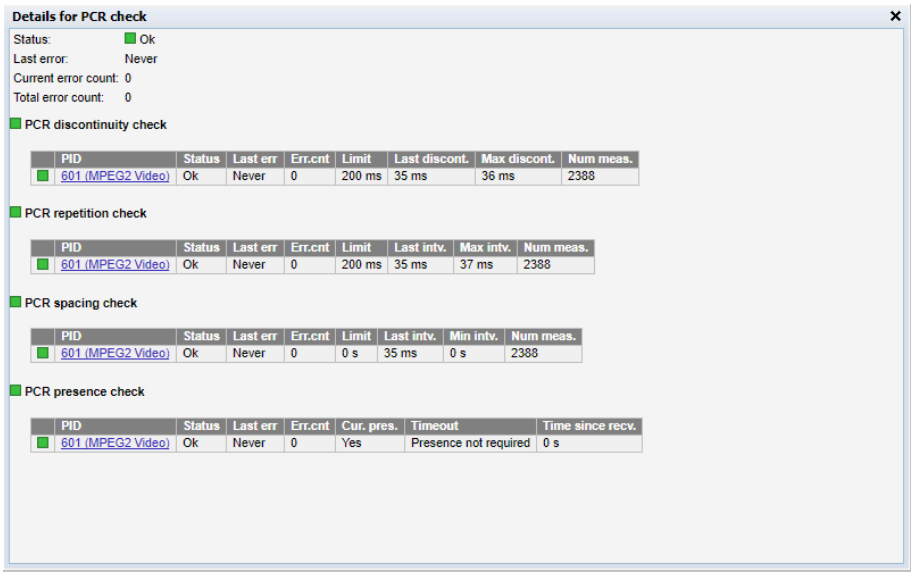


The **ETR Details** view shows the ETR 290 status for the current stream of the user-selected input. The name of the current stream is displayed in addition to the two round-robin indicator icons when relevant: the time cycle icon and the lock icon. By clicking the lock icon the round-robin tuning process is stopped (locked to the current frequency) or resumed. A DVB, ATSC or ISDB 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 Sencore allowing CA system checks, custom PID and service checks 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.



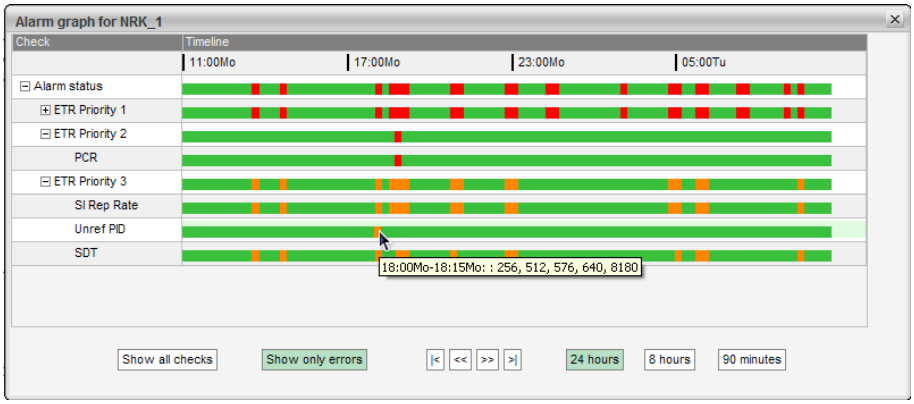
Enable the **Show additional measurements** checkbox to view additional measurements that are performed but which are ignored when determining the alarm status. These will appear with a 'half-bulb' icon indicating that the check is disabled whilst also showing the status of this element. As an example 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 **Sencore VideoBRIDGE ETR 290 Details — Extended ETSI TR 101 290 Testing**.

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

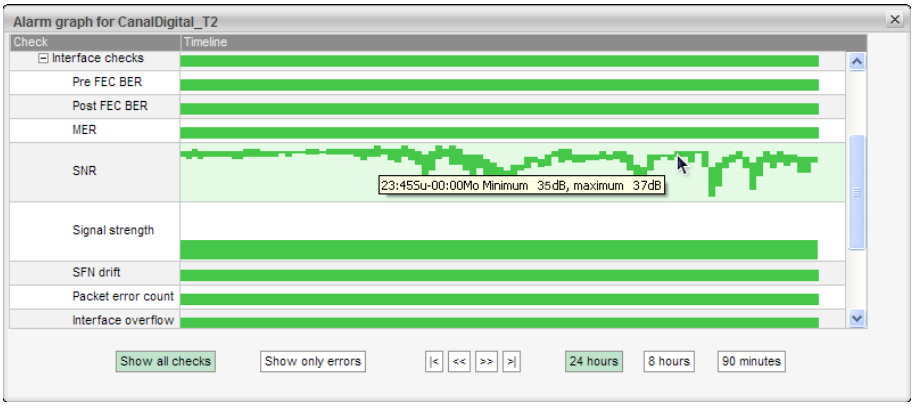


The alarm graph shows the ETR alarm status over time in the form of a status timeline. The timeline bar shows the stream status for a time span of 90 minutes, 8 hours or 24 hours as selected by

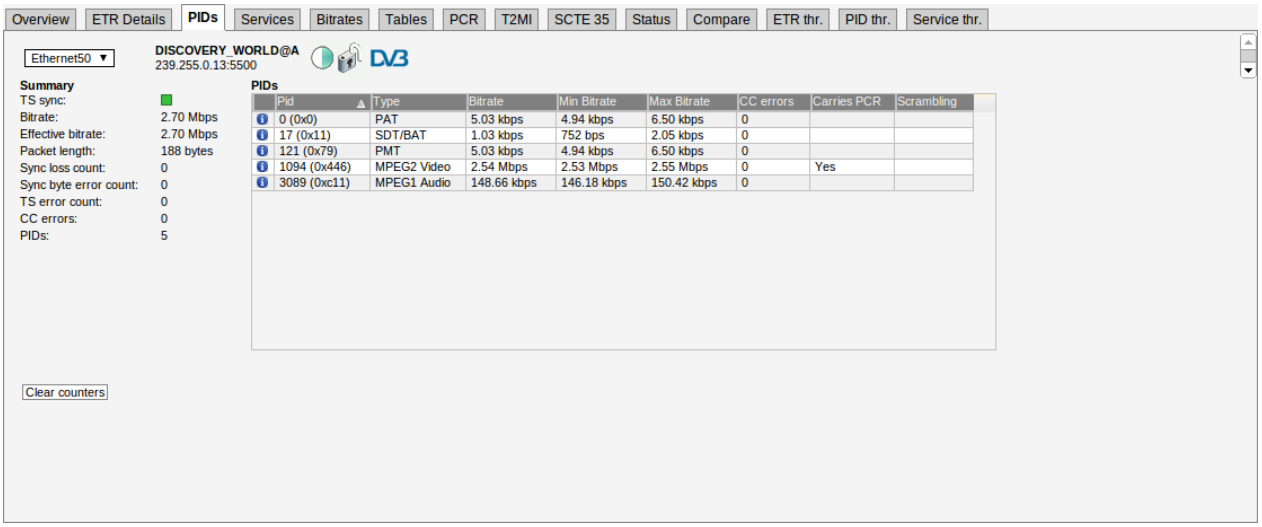
clicking the time selection buttons below the timelines. The stream bar reveals any alarm that has been present during the selected time period. The bar color is either green for OK or colored in accordance with the alarm severity if an alarm has occurred. Refer to **section 5.2.2** for a description 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. Tool-tips reveals details about an error incident such as which PIDs have had CC errors.

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

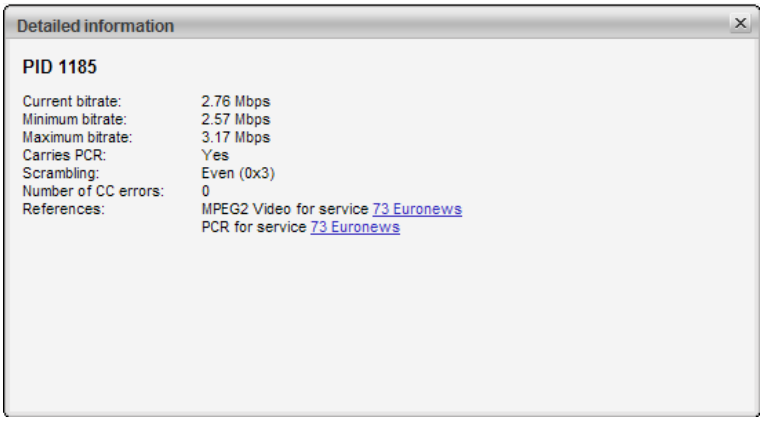


This view lists the PIDs of the currently active stream of the selected input. The PID list can be sorted by clicking a table column header.

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, ATSC or ISDB 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.

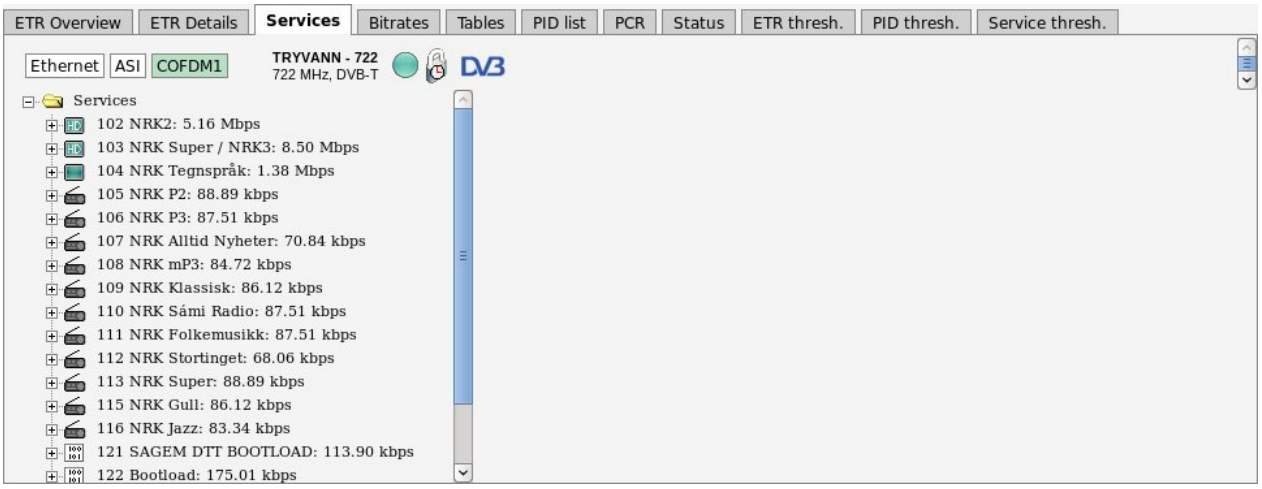


The following PID details are displayed:

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 290 — ETR Details** view.)
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 **Multicasts — Parameters** view.
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

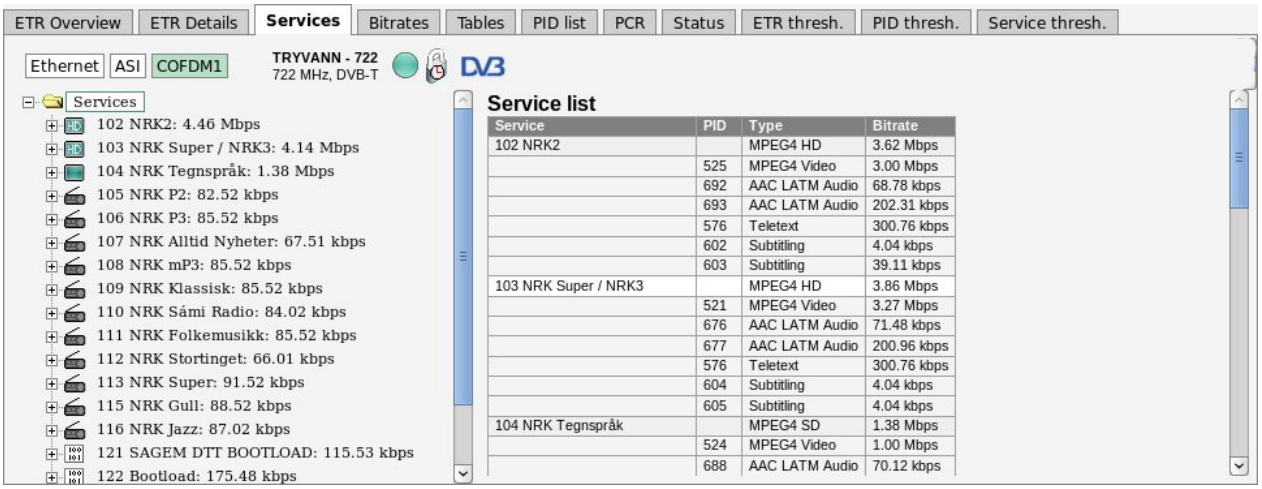


The **ETR290 — Services** view lists the services and service components of the current stream of the selected input.

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, ATSC or ISDB icon indicates the analysis mode. The analysis mode is defined as part of the ETR thresholds.

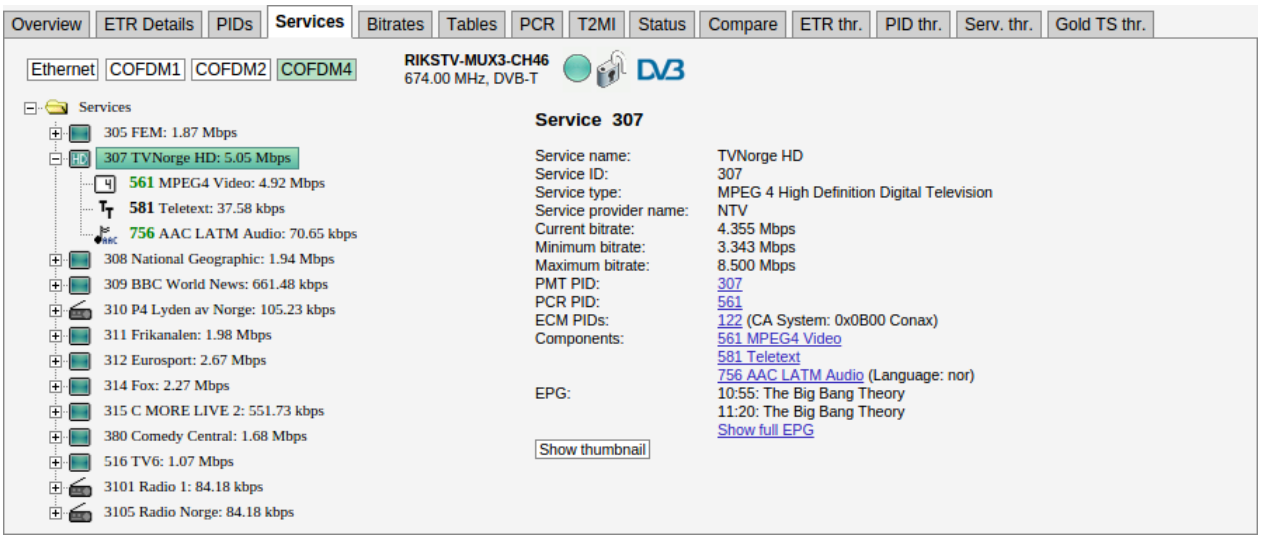
When tree nodes are selected, detailed information will be displayed on the right hand side of the view.

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.

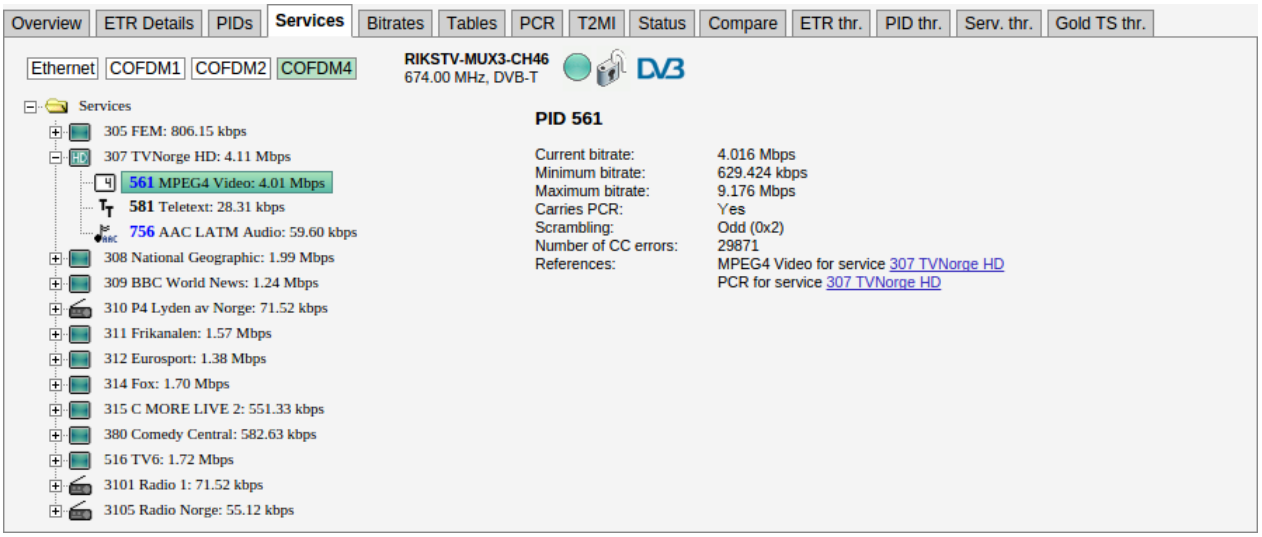


If a PID is scrambled this is indicated in the service tree by the color green or blue (for even and odd scrambling respectively). A missing PID is indicated by the color red. Click on the PID to show more details.

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

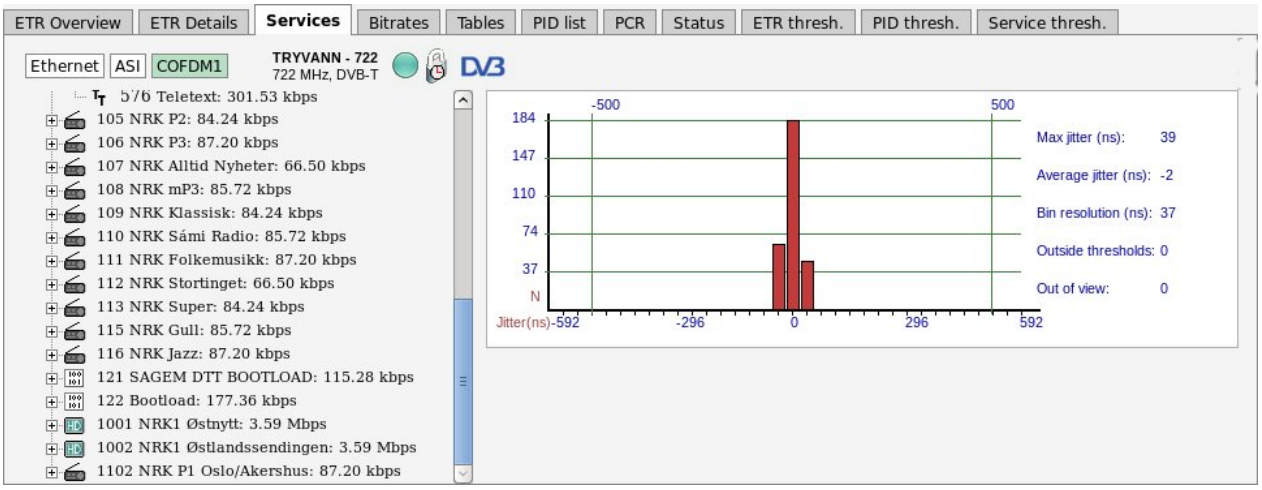
Service node	
Service name:	Name of the highlighted service, as signaled in SDT or VCT
Service ID:	Service ID number
Service type:	Service type as signaled in SDT
Service provider name:	The name of the service provider as signaled in SDT. Not applicable for ATSC streams.
Current bitrate:	The current 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 **Clear status** in the **ETR 290 — ETR Details** view.)
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, the EIT check is enabled in the ETR template used by the stream and EIT table IDs are configured in the **Setup — ETR** view, EIT present/following is displayed. For ATSC streams, EIT present/following is displayed if there are EITs present in the stream. 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. The same pop-up details are displayed as when opened from the **Content — Thumbnails** view. To display thumbnails for JPEG XS services, the JPEGXS-OPT license is required.

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

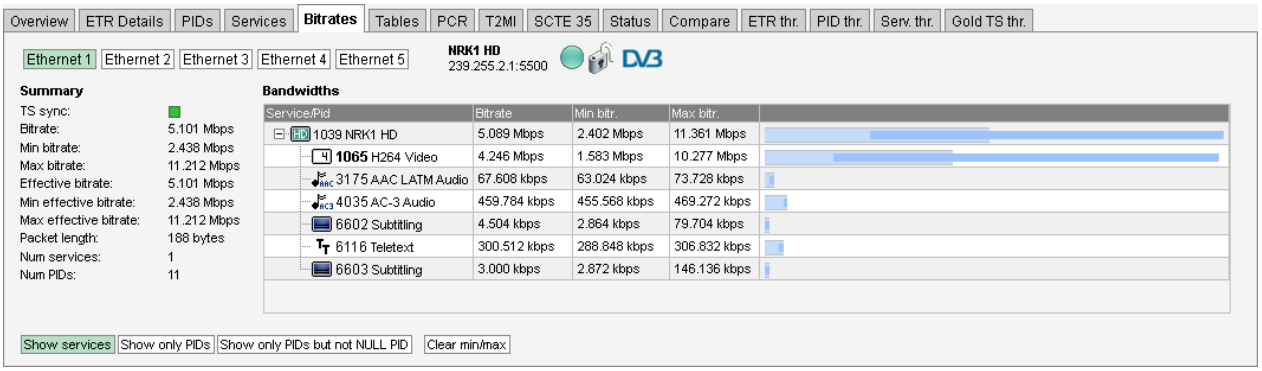


For PIDs carrying PCR it is possible to view a PCR jitter histogram by clicking the blue ‘show histogram’ link. If one of the blue service links is clicked, service details are shown.

Service component node	
Current bitrate:	The current bitrate measurement for this 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 **Clear status** in the **ETR 290 — ETR Details** view.)
Maximum bitrate:	The maximum bitrate measurement for this PID 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, ATSC or ISDB 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.

Click **Clear min/max** to reset the minimum and maximum bitrate measurements.

5.9.6 ETR 290 — Tables

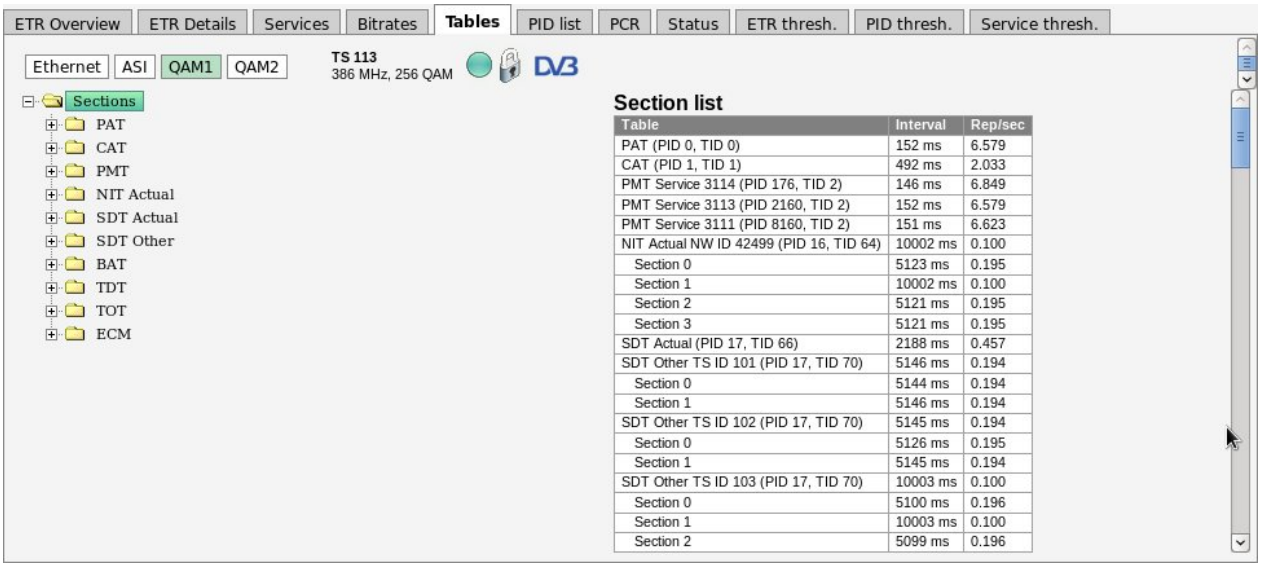


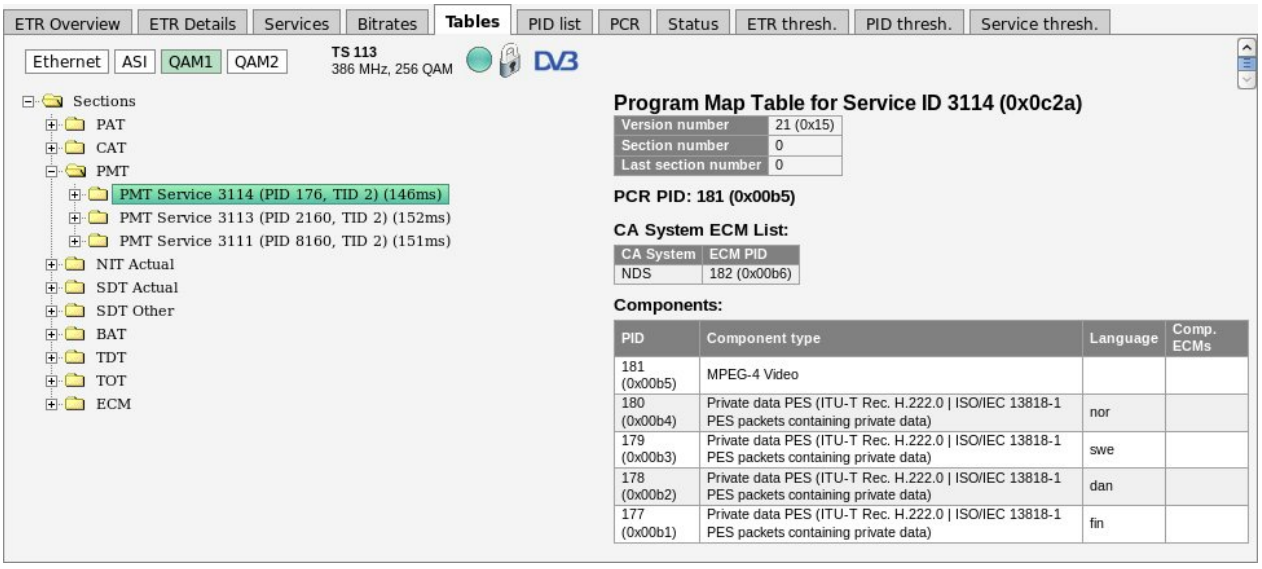
Table	Interval	Rep/sec
PAT (PID 0, TID 0)	152 ms	6.579
CAT (PID 1, TID 1)	492 ms	2.033
PMT Service 3114 (PID 176, TID 2)	146 ms	6.849
PMT Service 3113 (PID 2160, TID 2)	152 ms	6.579
PMT Service 3111 (PID 8160, TID 2)	151 ms	6.623
NIT Actual NW ID 42499 (PID 16, TID 64)	10002 ms	0.100
Section 0	5123 ms	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, ATSC or ISDB 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:

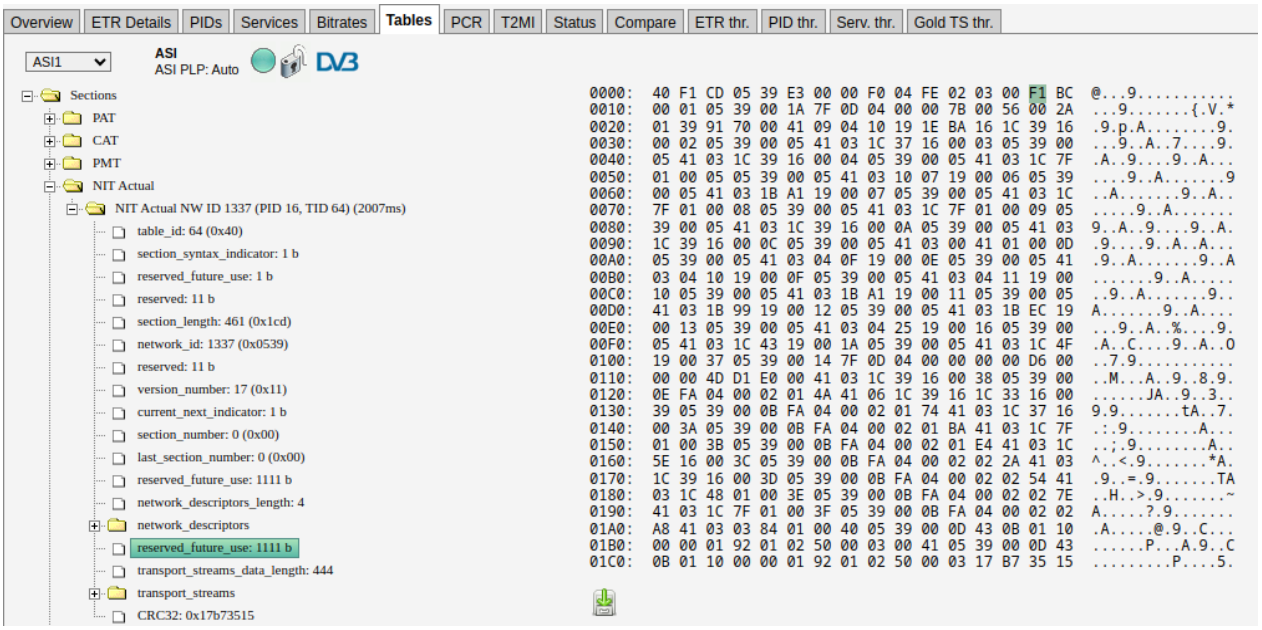
CA System	ECM PID
NDS	182 (0x00b6)

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.

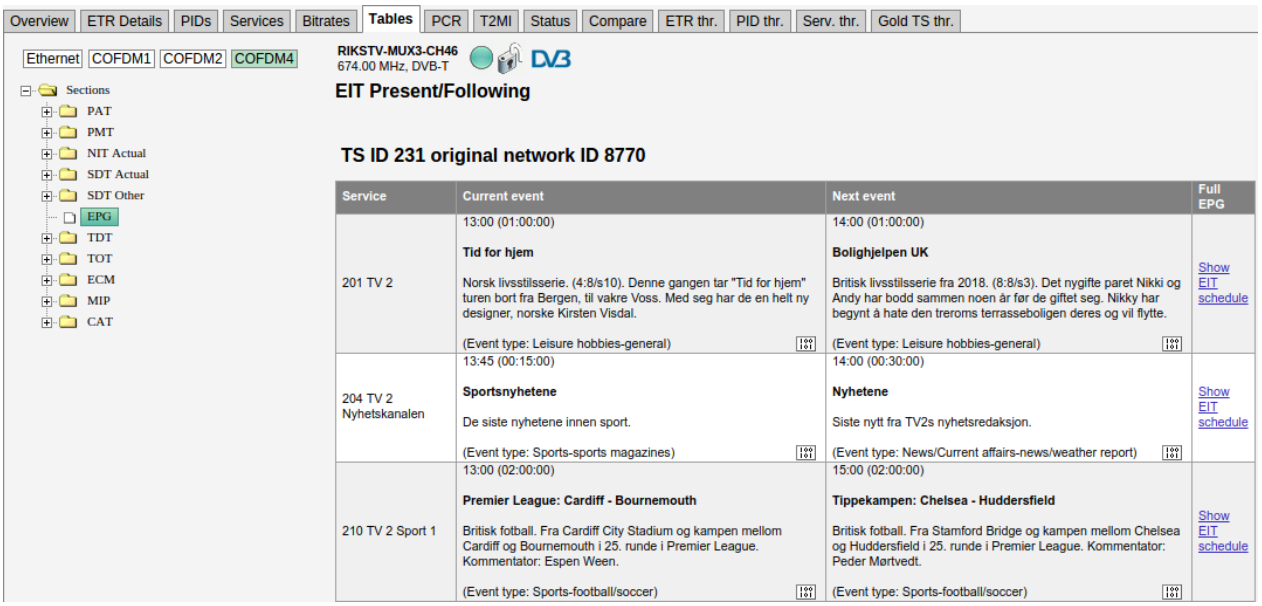


The selected table entry is highlighted in the table dump. Note that values shown in the table list may not correspond directly to the highlighted hex dump byte(s), because some of the table entries do not add up to whole bytes.

By hovering the cursor over the items in the tree a tool-tip 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.

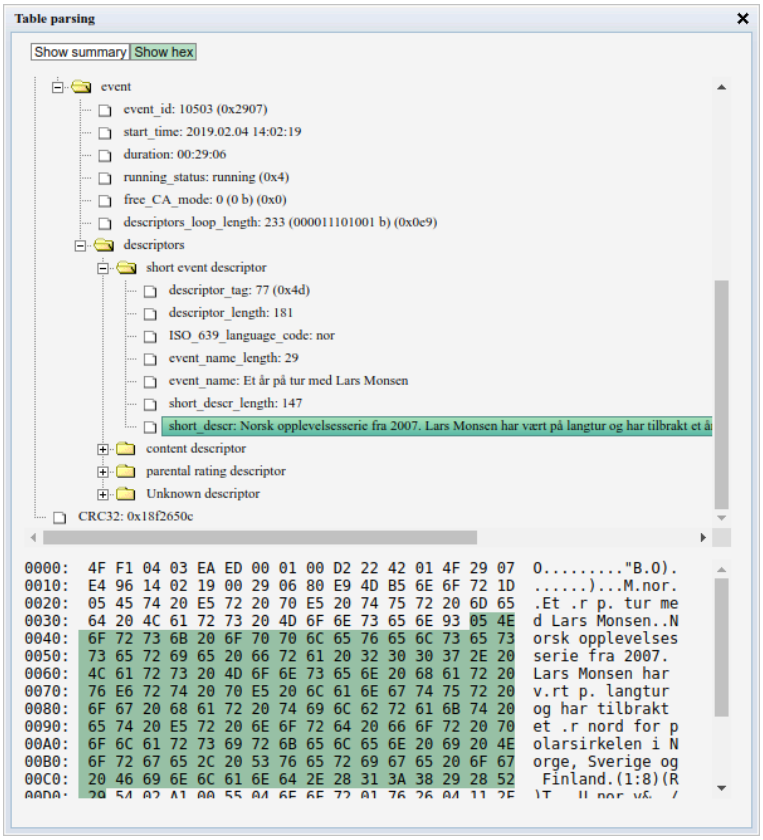
A description of each PSI/SI table is beyond the scope of this manual, please refer to the specifications for more information about PSI/SI.

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.

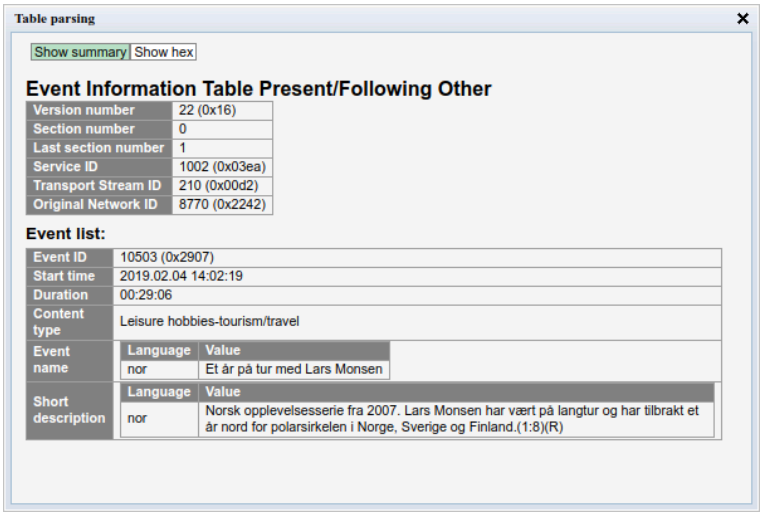


For streams which have electronic program guide (EPG) information in the EIT table and the extraction of this information is enabled (in **ETR thresholds** and in **Setup — ETR**) the tree will show the text **EPG** (for ATSC streams EPG will be displayed regardless if EITs are present in the stream). 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 (not available for ATSC). 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.

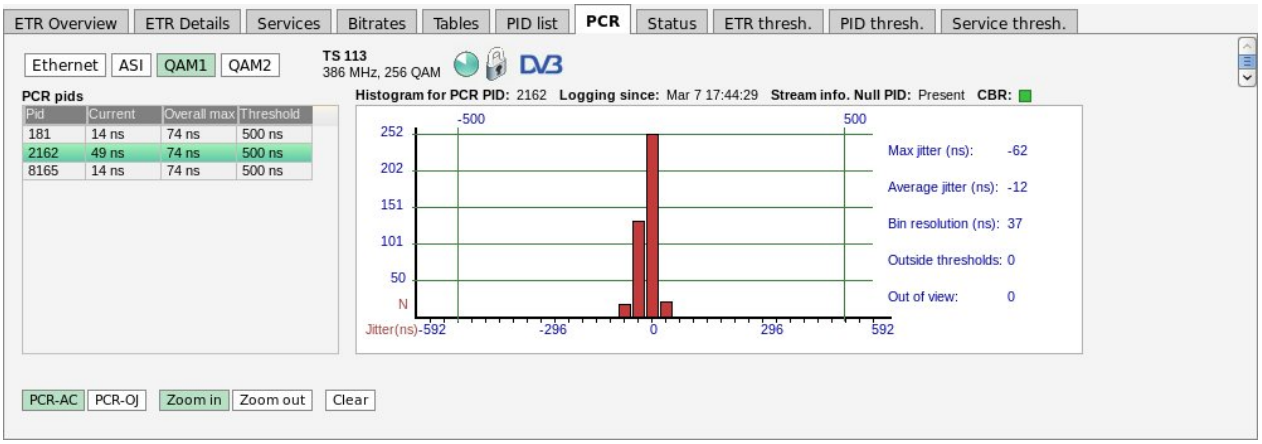
To get detailed information about one event, click the binary symbol . This will open a popup window with parsing of the underlying EIT table. The information can be displayed either in detailed hex mode:



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 push-buttons **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.

Tool-tip 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.

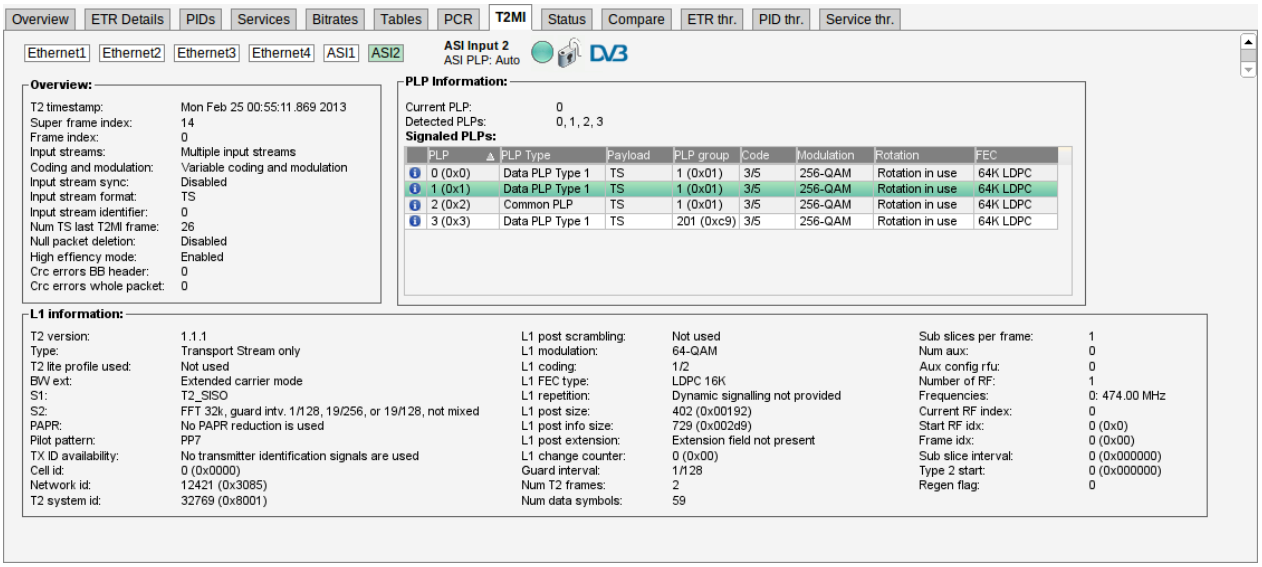
The PCR PID list displays the following parameters:

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 licensed 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.

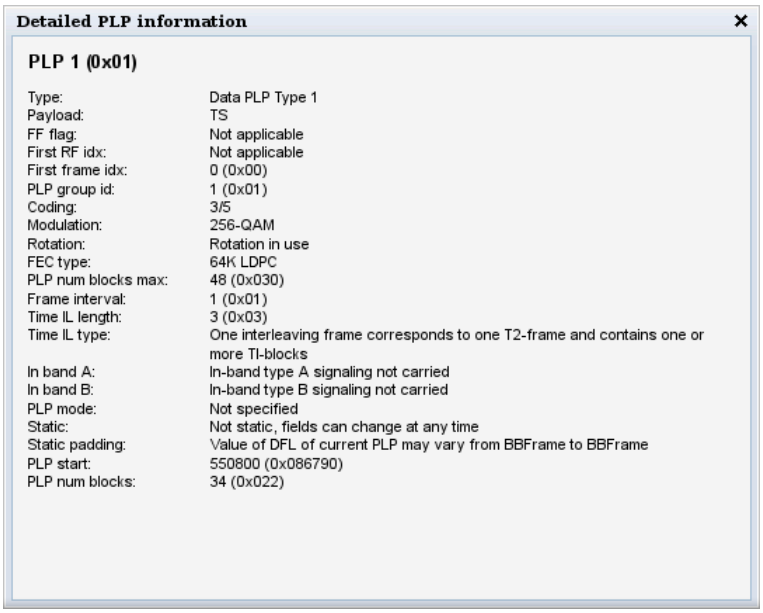
Crc Errors BB header:	The number of CRC errors on the BB header detected since the monitoring of the stream started.
Crc Errors whole packet:	The number of CRC errors calculated over the whole T2MI packet since the monitoring of the stream started.

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

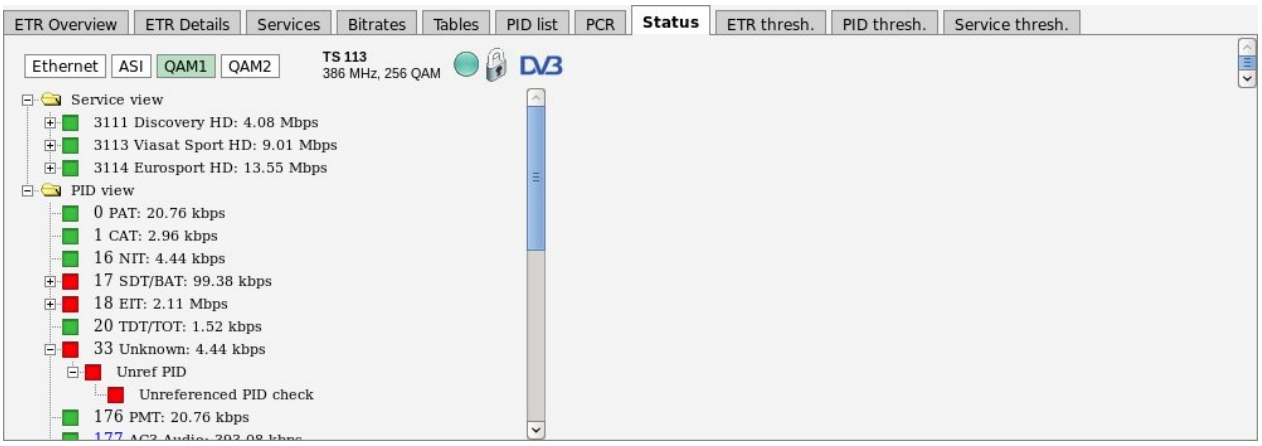
Clicking the blue information symbol in the PLP list will bring up more detailed information for that PLP.



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 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.

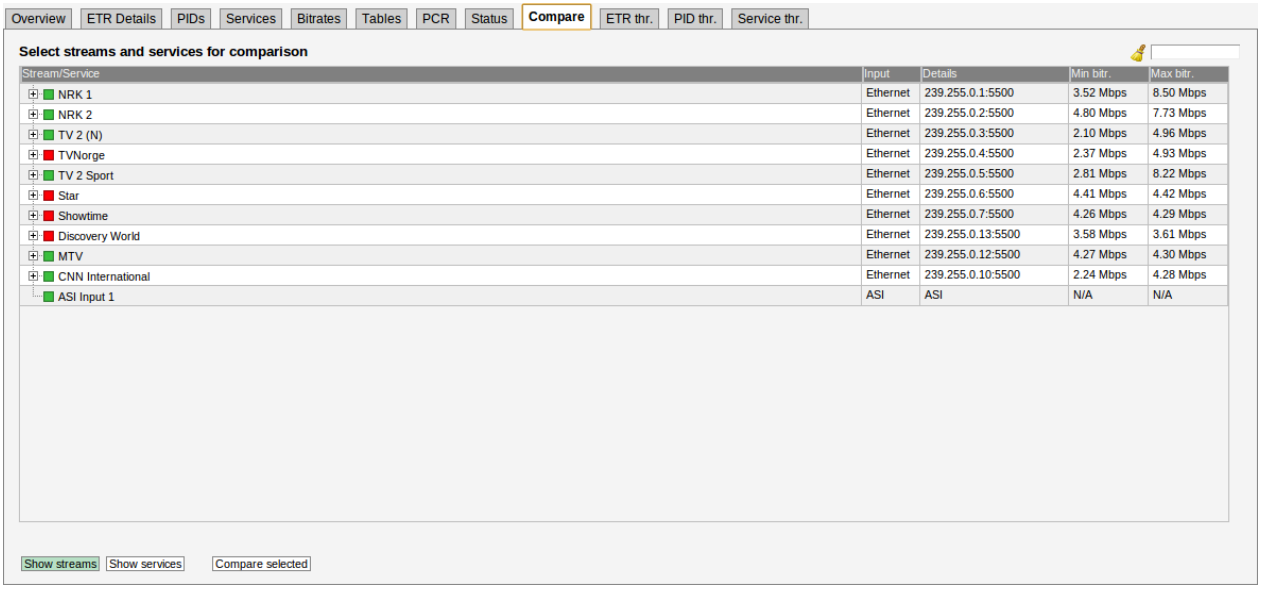
5.9.9 ETR 290 — Status



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.

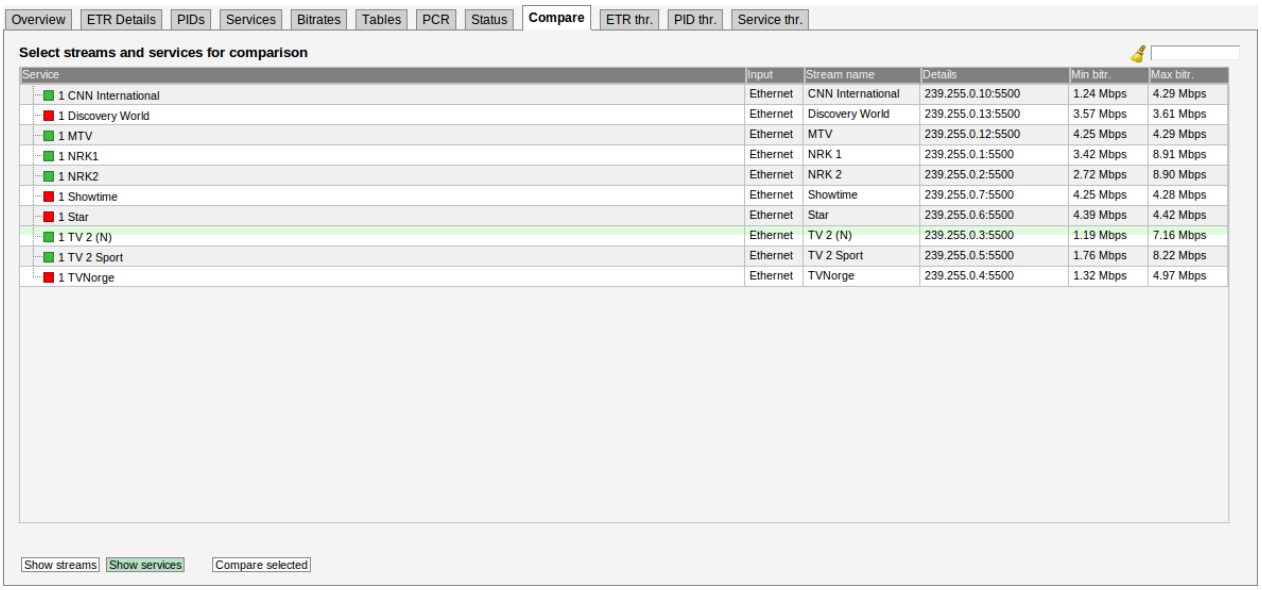
By clicking any of the ‘view’, service or PID nodes, more information will be displayed on the right hand side of the table. This information is described in **ETR 290 — Services**.

5.9.10 ETR 290 — Compare



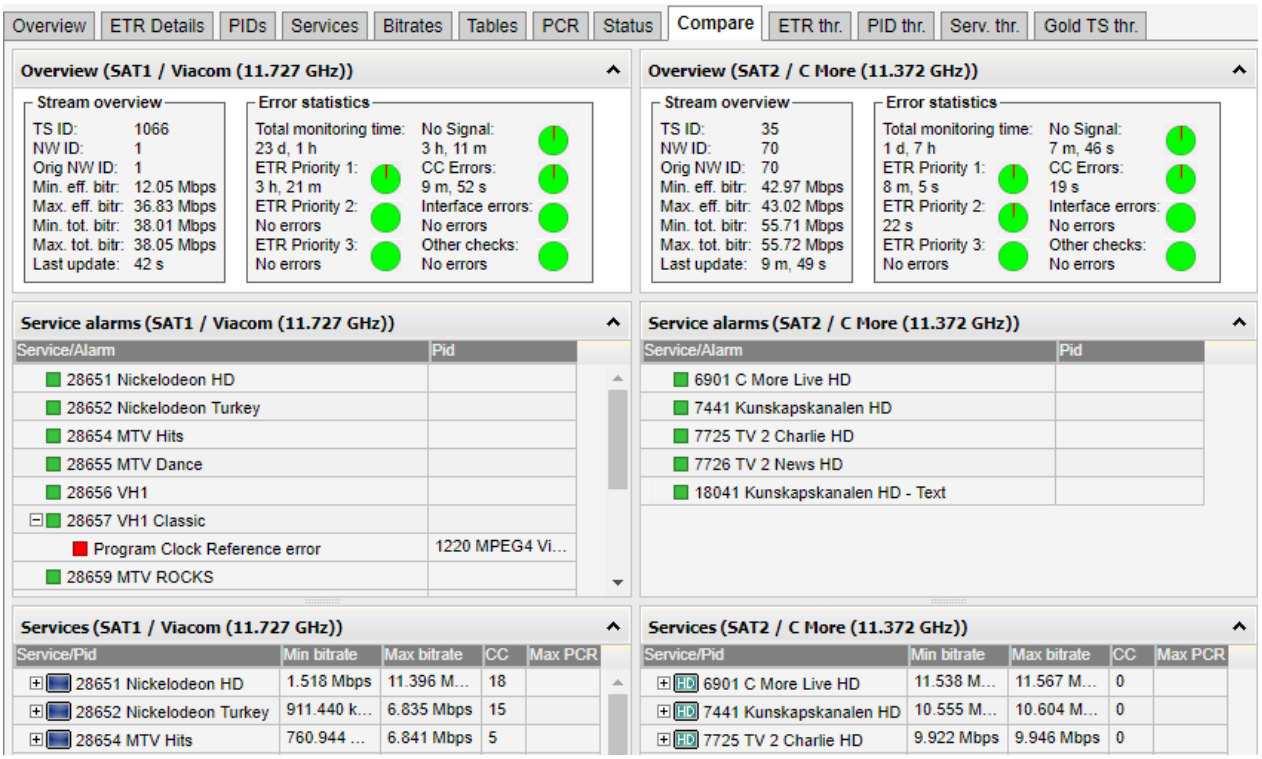
The **Compare** view is based on analysis performed by the ETSI TR 101 290 engine and only the streams monitored by ETR will be listed.

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.



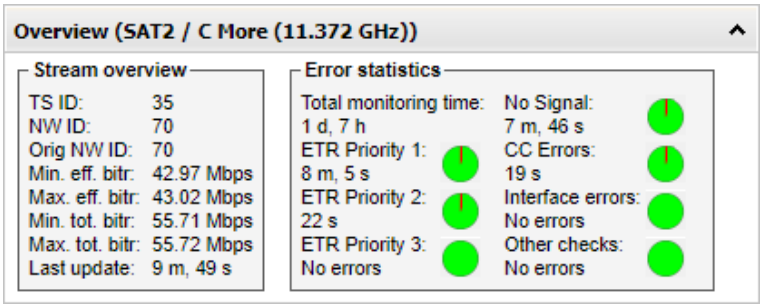
One or more services or transport streams are selected by clicking and later *Ctrl* + clicking items from the list. Clicking the **Compare selected** button will launch a condensed overview page that allows status parameters for services or streams to be viewed side by side. Key parameters are

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.

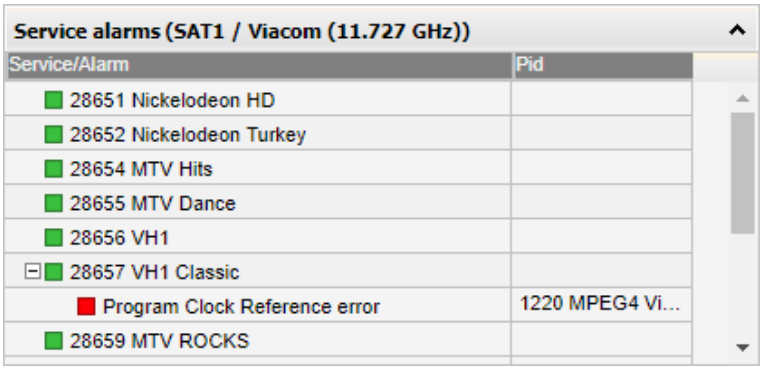
Stream overview	
TS ID:	The transport stream ID of the selected stream or the stream containing the selected service
NW ID:	The network ID of the selected stream or the stream containing the selected service
Orig NW ID:	The original network ID of the selected stream or the stream containing the selected 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’.

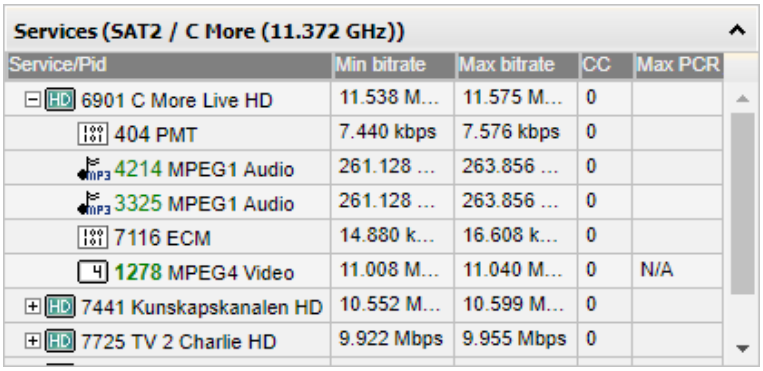
Service alarm



If a transport stream is selected for comparison the **Service alarms** sub-view 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 sub-view simply shows the selected service and any active alarms affecting the service.

Services

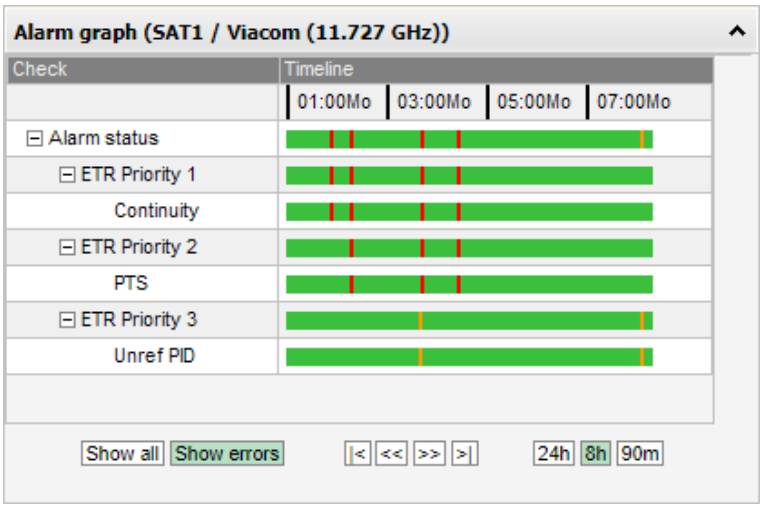


If a transport stream is selected for comparison the **Services** sub-view displays a list of services present in the stream. Clicking the plus icon at a service will expand the service tree, displaying the service's individual components. The minimum and maximum effective bitrates of a service/-component 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.

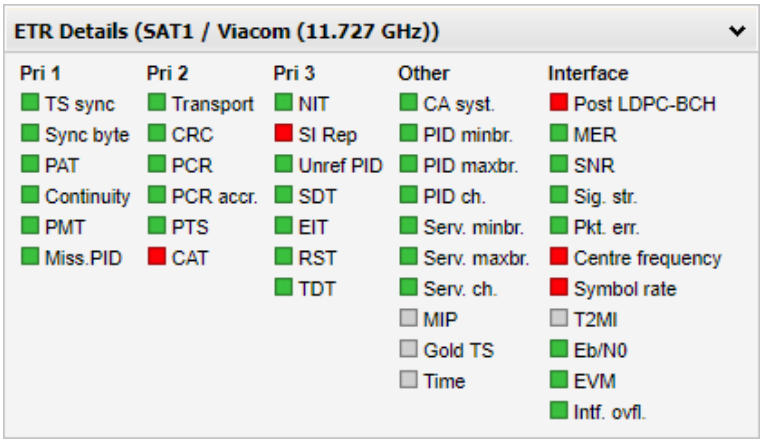
Note that all references to a PID will result in a PID entry, i.e. one PID may be displayed several times in the list.

Alarm graph



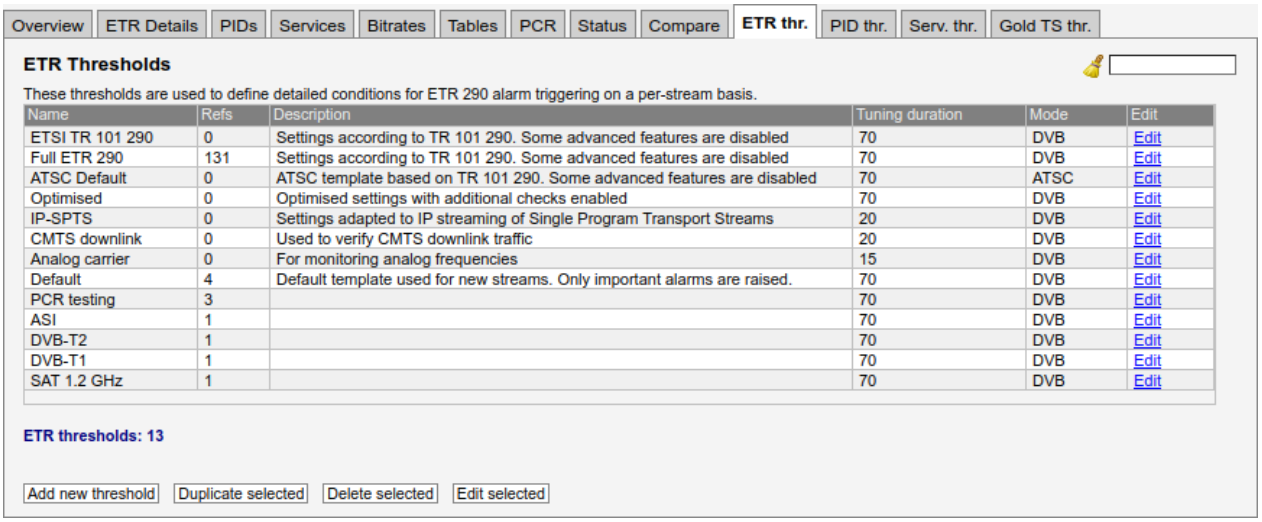
The Alarm graph sub-view shows similar alarm graphs as the **ETR 290 — ETR Details — Alarm graph popup** view. Please refer to the **ETR 290 — ETR Details** section of this User's Manual for a comprehensive description of this view.

ETR Details



The ETR details sub-view 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.

5.9.11 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:

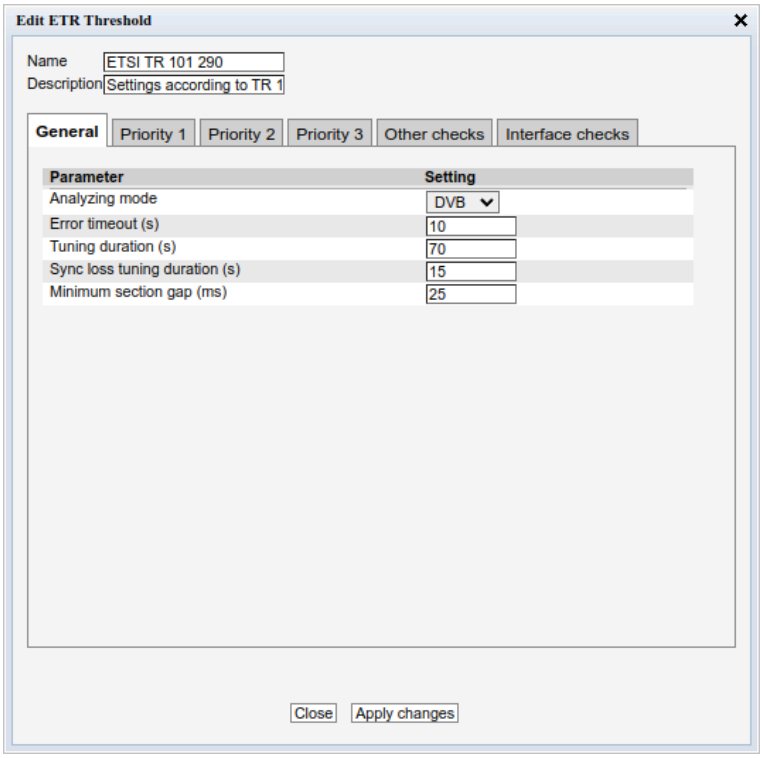
- Default
- ETSI TR 101 290
- ATSC Default
- Optimised
- IP-SPTS
- CMTS downlink
- Analog carrier

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.



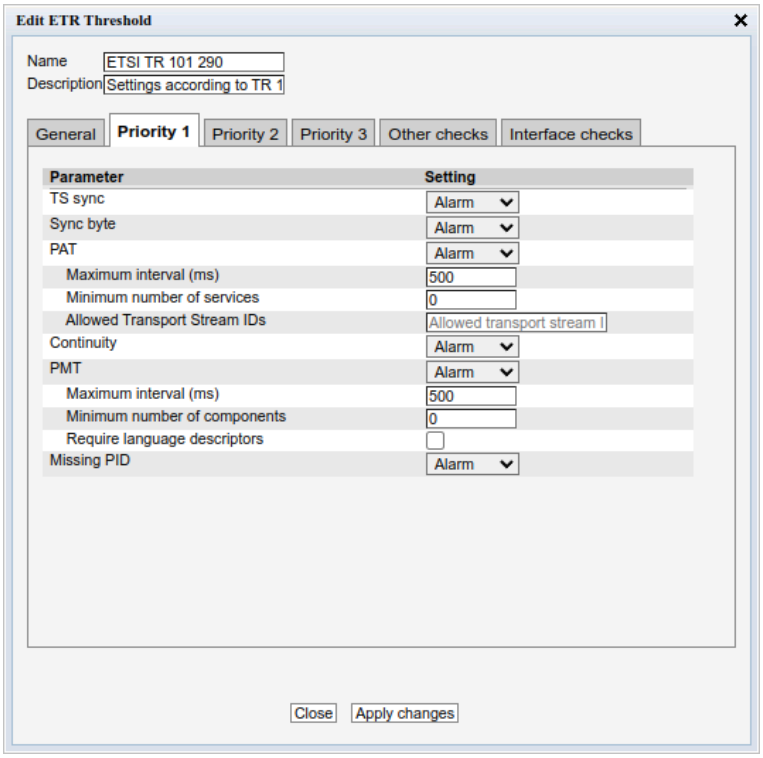
The ETR threshold dialog is divided into tabs for easier access to the relevant settings and has the following settings:

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

ETR Thresholds — General:	
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

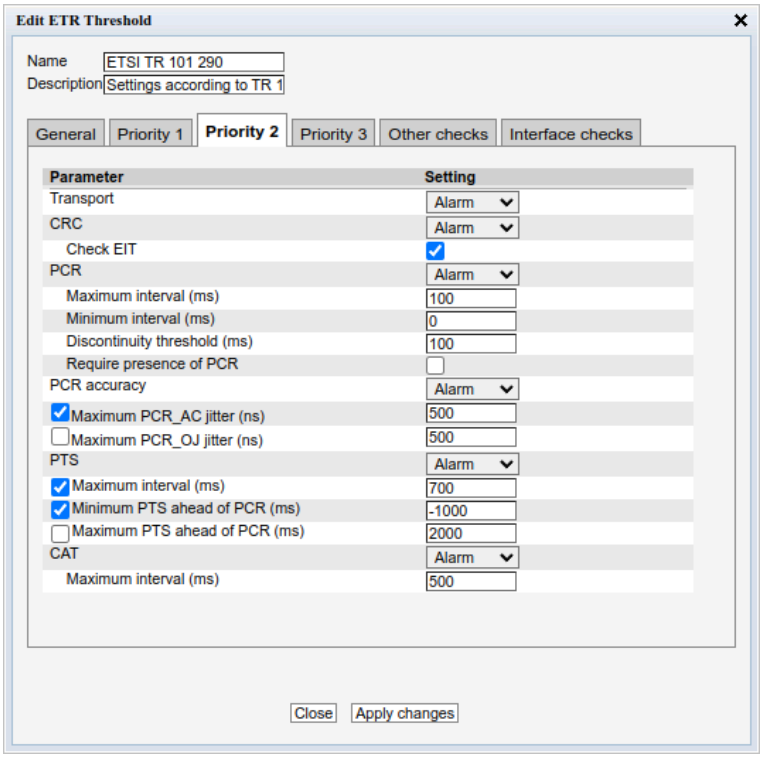
Minimum section gap (ms):	The minimum allowed gap between transmission of two consecutive sections with the same table ID. If the sections are transmitted too rapidly the STB may not be able to process the data in time and various problems can occur. However newer STBs can normally handle lower section 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

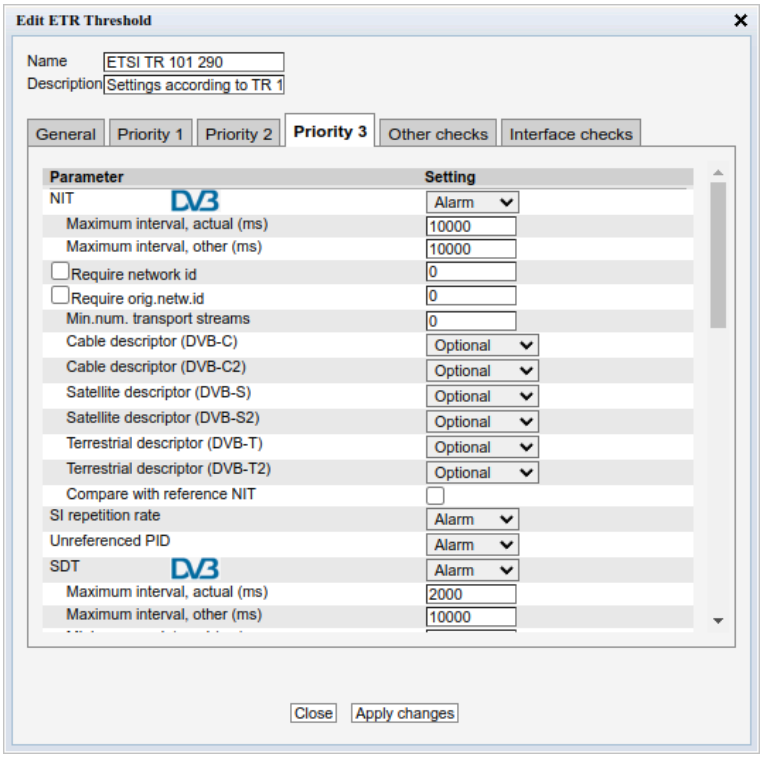
PAT – Allowed Transport Stream IDs:	When this field is left blank all TS IDs are considered valid. If one or more TS IDs are specified (separated by commas or as a range) only these IDs are considered valid, and any other TS ID will trigger an alarm. Example of a valid field: '100-120, 300,320'
Continuity:	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
CRC – Check EIT:	When enabled alarming of CRC errors in the EIT tables will be performed. Default: Enabled
CRC – Check AIT:	When enabled alarming of CRC errors in the AIT tables will be performed. Default: Enabled
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. Checking of this value will be performed if the checkbox is enabled. 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. Checking of this value will be performed if the checkbox is enabled and the stream is received on an ASI or RF interface. 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. Checking of this measurement will be performed for all PTS PIDs if the checkbox is enabled in the ETR Thresholds template. When the checkbox is disabled the measurement will only be checked for the PIDs that have this measurement enabled in the **PID threshold template**. Default threshold according to ETSI TR 101 290: 700 ms

PTS – Minimum PTS ahead of PCR (ms):	The minimum allowed value for the measurement of the signaled PTS versus the current PCR clock. If the PTS value sent refers to a PCR clock time that have already passed the measurement will be negative. Checking of this measurement will be performed for all PTS PIDs if the checkbox is enabled in the ETR Thresholds template. When the checkbox is disabled the measurement will only be checked for the PIDs that have this measurement enabled in the **PID threshold template**. Default: -1000 ms
PTS – Maximum PTS ahead of PCR (ms):	The maximum allowed value for the measurement of the signaled PTS versus the current PCR clock. Checking of this measurement will be performed for all PTS PIDs if the checkbox is enabled in the ETR Thresholds template. When the checkbox is disabled the measurement will only be checked for the PIDs that have this measurement enabled in the **PID threshold template**. Default: 2000 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



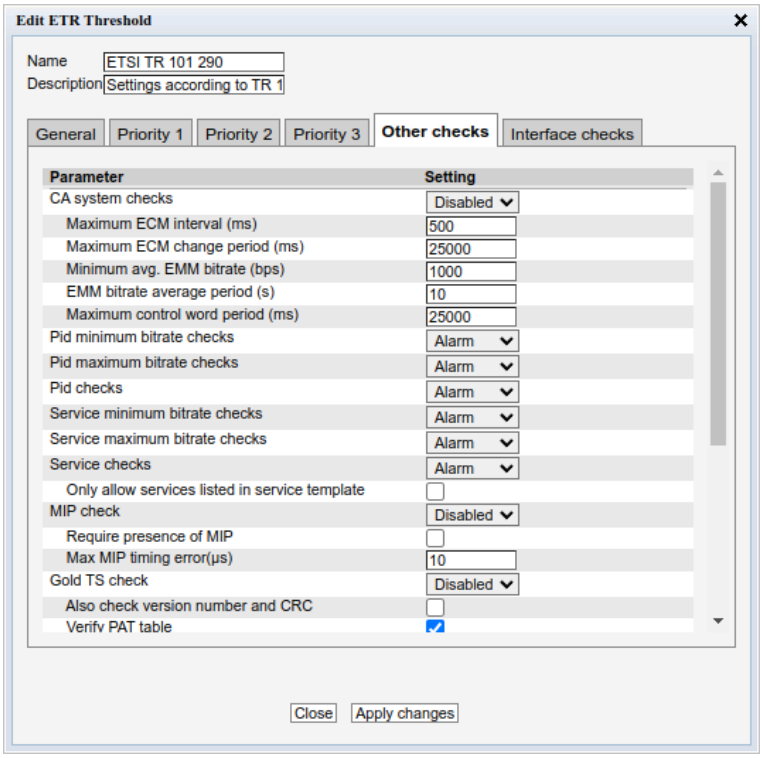
	ETR Thresholds — Priority 3:
NIT:	Enable or disable alarming of Network Information Table errors. Only relevant when DVB mode is selected.
NIT – Maximum interval actual (ms):	The maximum allowed section repetition interval for the NIT actual table. Default according to ETSI TR 101 290: 10 s
NIT – Maximum 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.
VCT – Require TVCT:	Require presence of the Terrestrial Virtual Channel Table.
VCT – 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.
PIM/PNM – Require PIM:	Require presence of the Program Information Message table.
PIM/PNM – Maximum interval PIM (ms):	The maximum allowed section repetition interval for the PIM table. Default: 500ms
PIM/PNM – Require PNM:	Require presence of the Program Name Message table.
PIM/PNM – 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

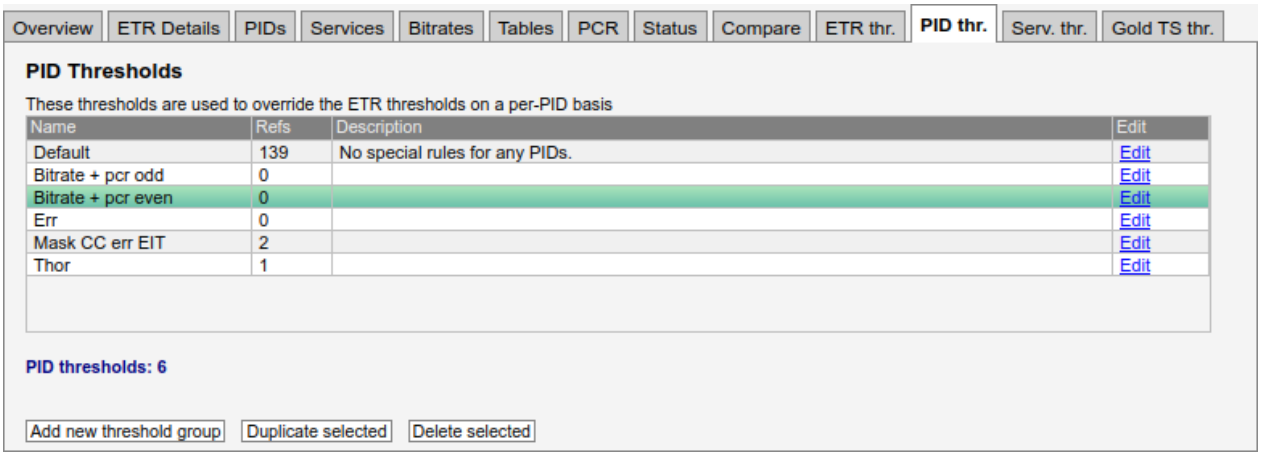


	ETR Thresholds — Other checks:
CA system checks:	Enable or disable alarming of Conditional Access System errors.
CA system checks – Maximum ECM interval (ms):	The maximum allowed ECM repetition interval. Default: 500 ms
CA system checks – Maximum ECM change period (ms):	The maximum time allowed between 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
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.

5.9.12 ETR 290 — PID thresholds

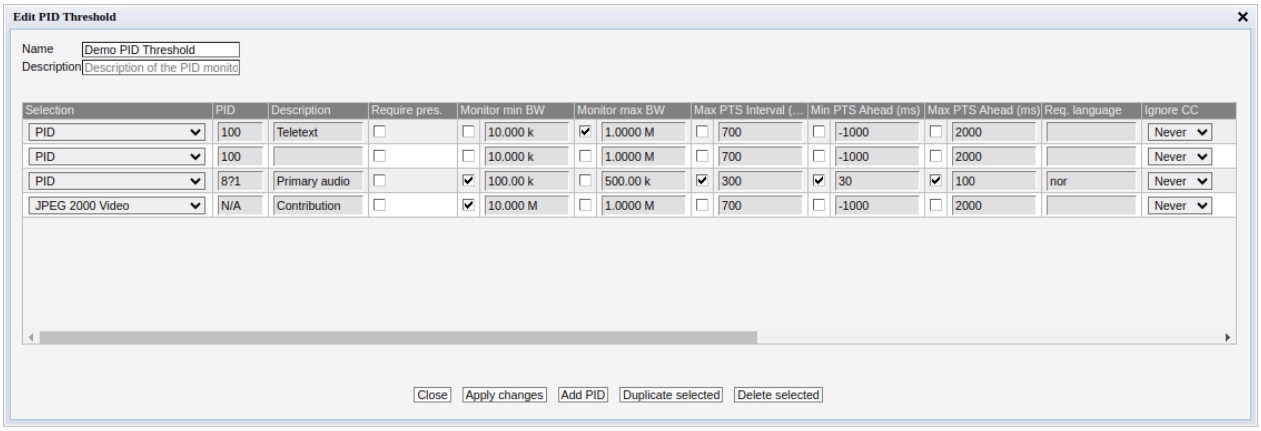


The **PID thresholds** make it possible to define detailed conditions for alarm triggering on a PID or PID type basis. There is one predefined PID threshold template that cannot be edited by the operator: 'Default'. The 'Default' PID threshold template contains no PID definitions and will therefore not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

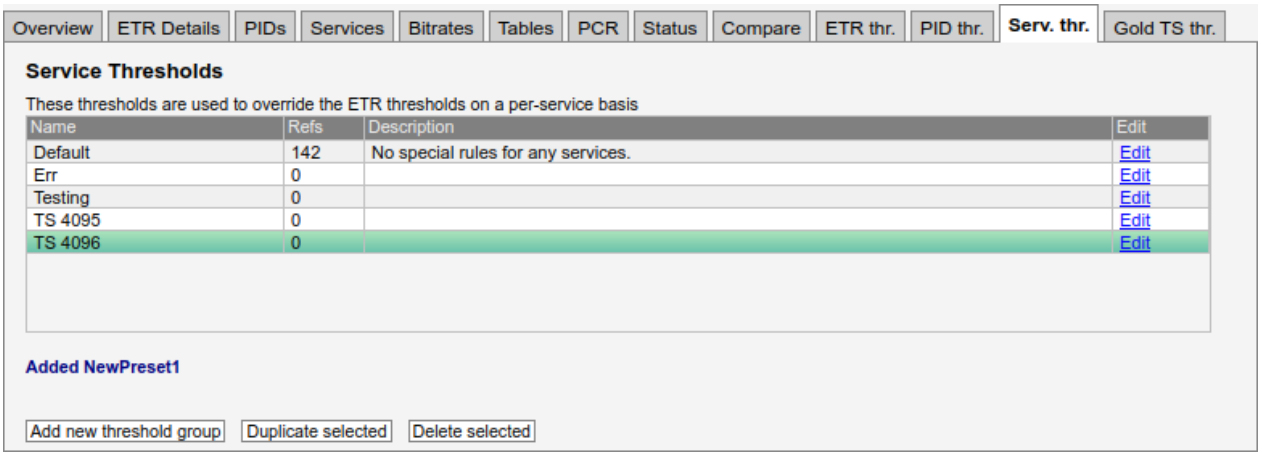
Edit PID Threshold:	
Name:	The name of the PID threshold template
Description:	Text field that should contain a meaningful description of the threshold template

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. A question mark can be used as a wild card to represent one digit. Example: The PID value `8?1` will match 3 digit PID numbers such as 801, 811 and 891. It will not match PID 81 or 8001.
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.
Max PTS interval (ms):	If the checkbox is enabled, the PTS interval measurement will be enabled for this PID and use the configured threshold. This will override the setting in the **ETR thresholds** template. An alarm is raised if the PTS repetition interval exceeds the configured limit.
Min PTS ahead (ms):	If the checkbox is enabled, the measurement of minimum PTS ahead will be enabled for this PID and use the configured threshold. This will override the setting in the **ETR thresholds** template. An alarm is raised if the PTS ahead measurement is lower than the the configured limit. The PTS ahead measurement measures the PTS value relative to the current PCR clock.
Max PTS ahead (ms):	If the checkbox is enabled, the measurement of maximum PTS ahead will be enabled for this PID and use the configured threshold. This will override the setting in the **ETR thresholds** template. An alarm is raised if the PTS ahead measurement is higher than the the configured limit. The PTS ahead measurement measures the PTS value relative to the current PCR clock.
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.

5.9.13 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.

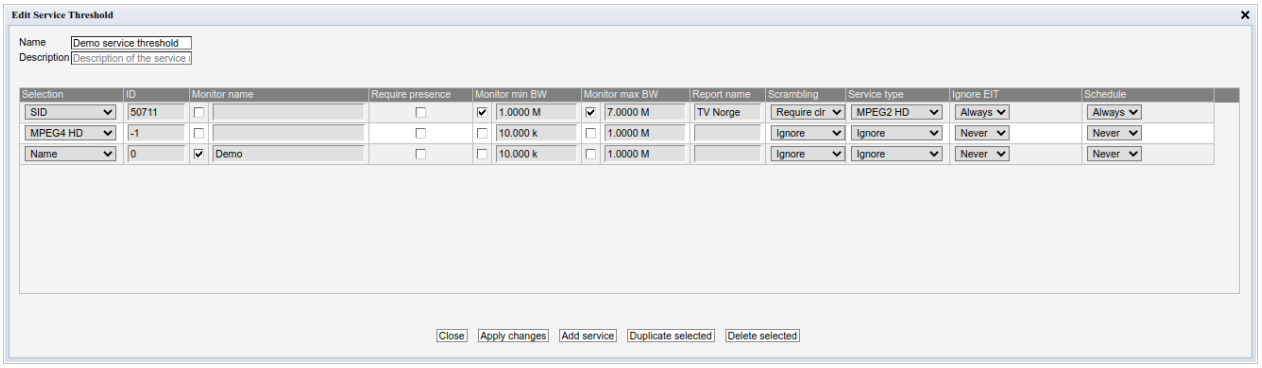
By associating scheduling templates to service threshold templates it is possible to disable alarming at pre-selected time intervals. Scheduling templates are defined in the **Setup — Scheduling** view and will be available from the schedule drop-down menu.

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 minimum bitrate checks**, **Service minimum bitrate checks** and **Service checks** in the ETR threshold template controls whether or not to report alarms based on the service threshold template parameters.



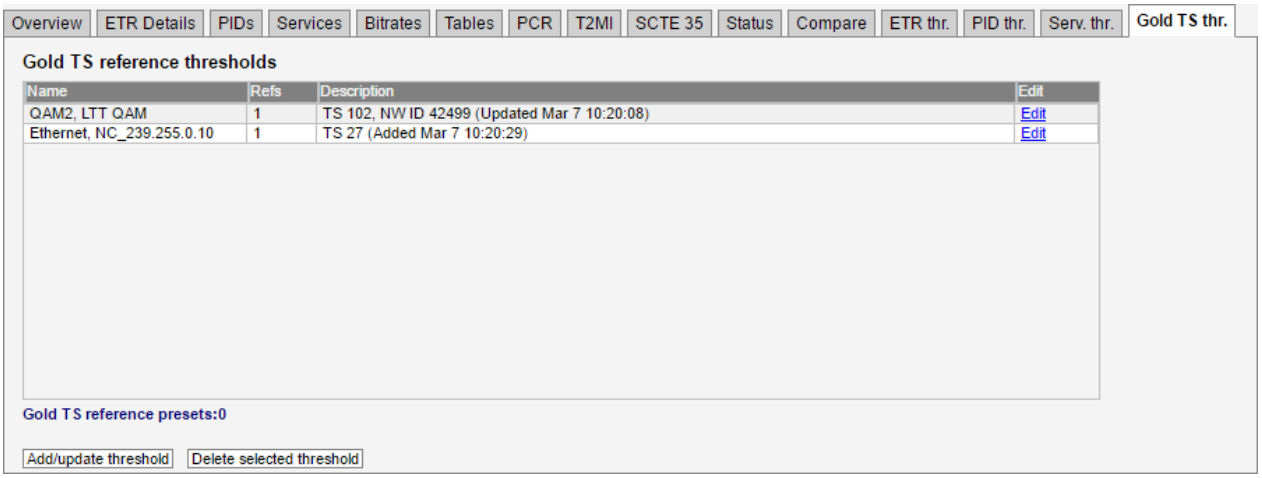
Edit Service Threshold	
Name:	A text string that identifies the service threshold group
Description:	Text field that should contain a meaningful description of the threshold

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 VideoBRIDGE 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 VideoBRIDGE 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.
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.

5.9.14 ETR 290 — Gold TS thresholds



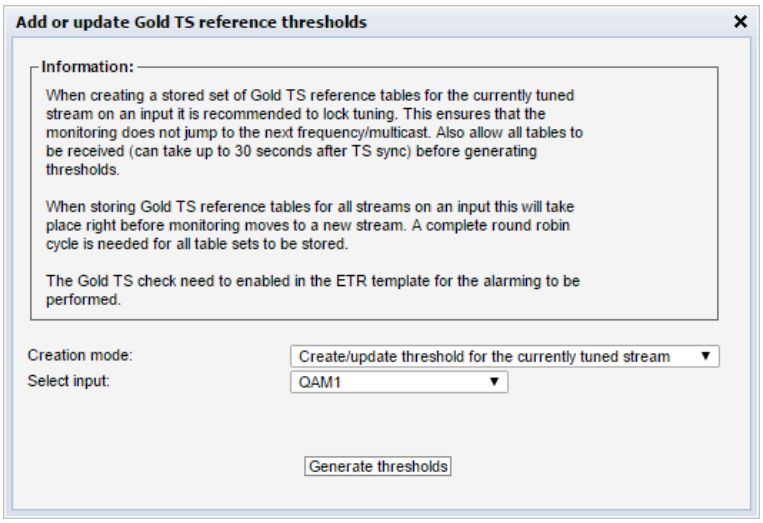
The Gold TS reference feature is used to compare the tables in the transport stream with a set of stored reference tables. This allows the operator to be notified of any changes in the PSI/SI tables such as:

- 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)

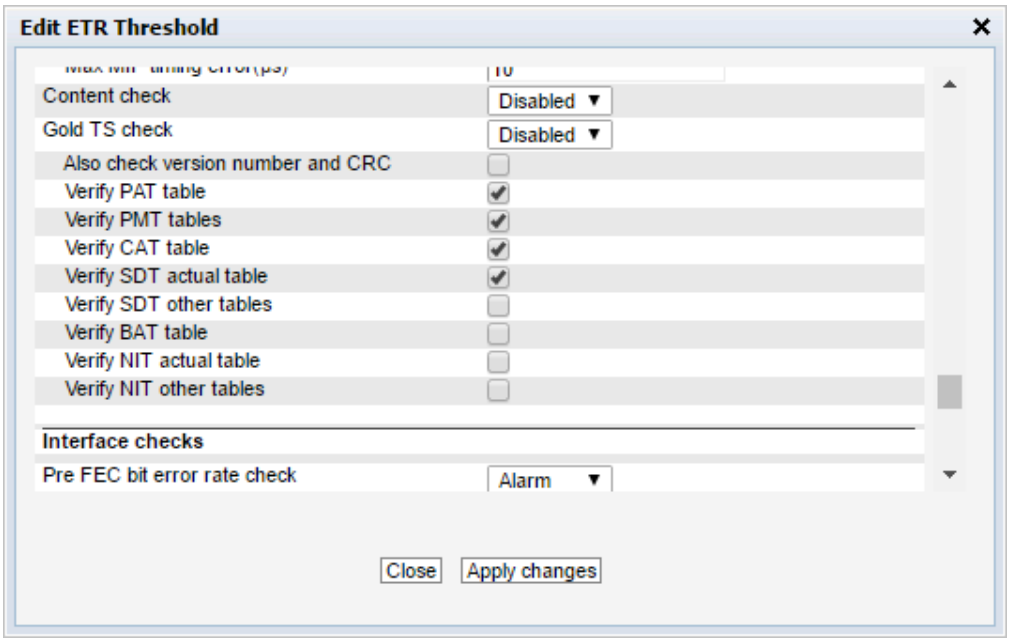
When creating a template for a specific stream the table set is saved immediately. It is therefore recommended that the ETR tuning is locked to this stream to avoid the round-robin operation from tuning to a new frequency just before the table set is stored. It can take 30 seconds after tuning to receive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

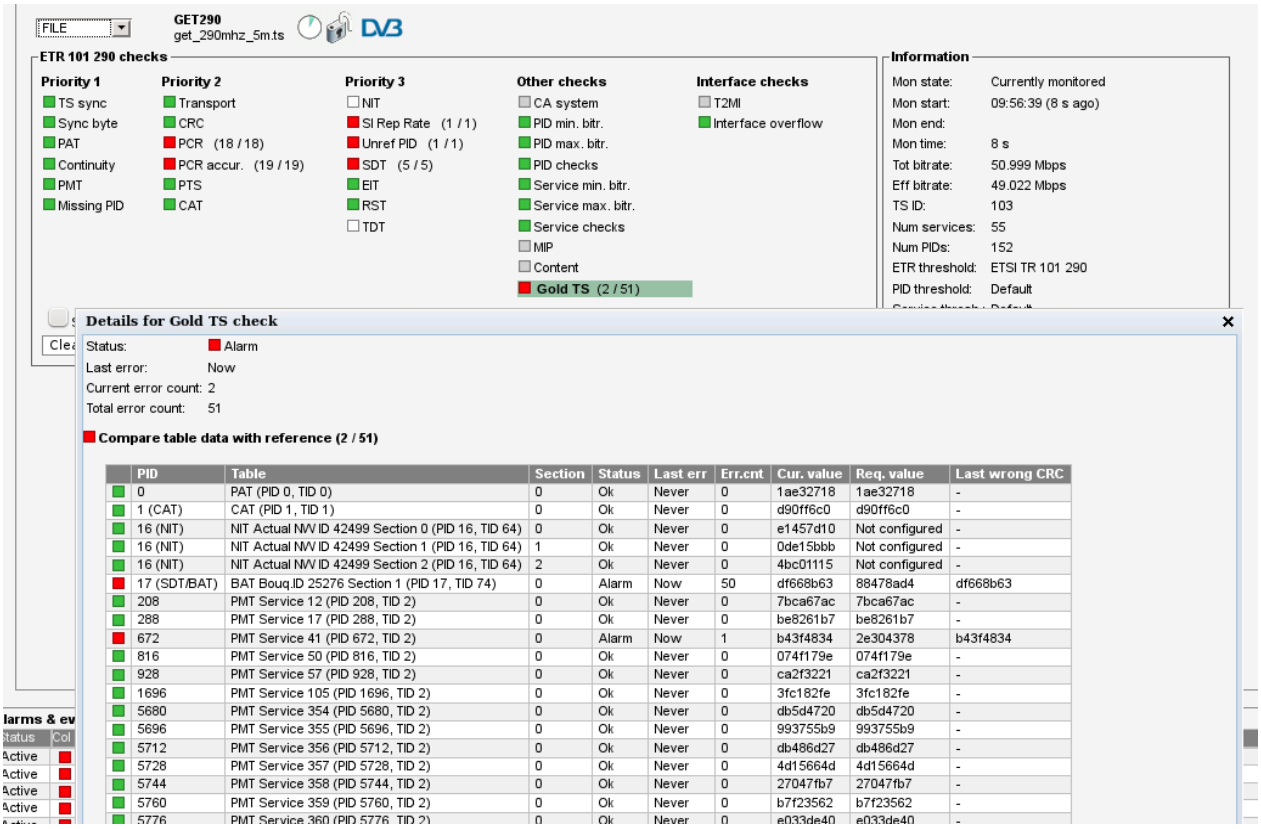
The settings are as follows:

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 Association 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

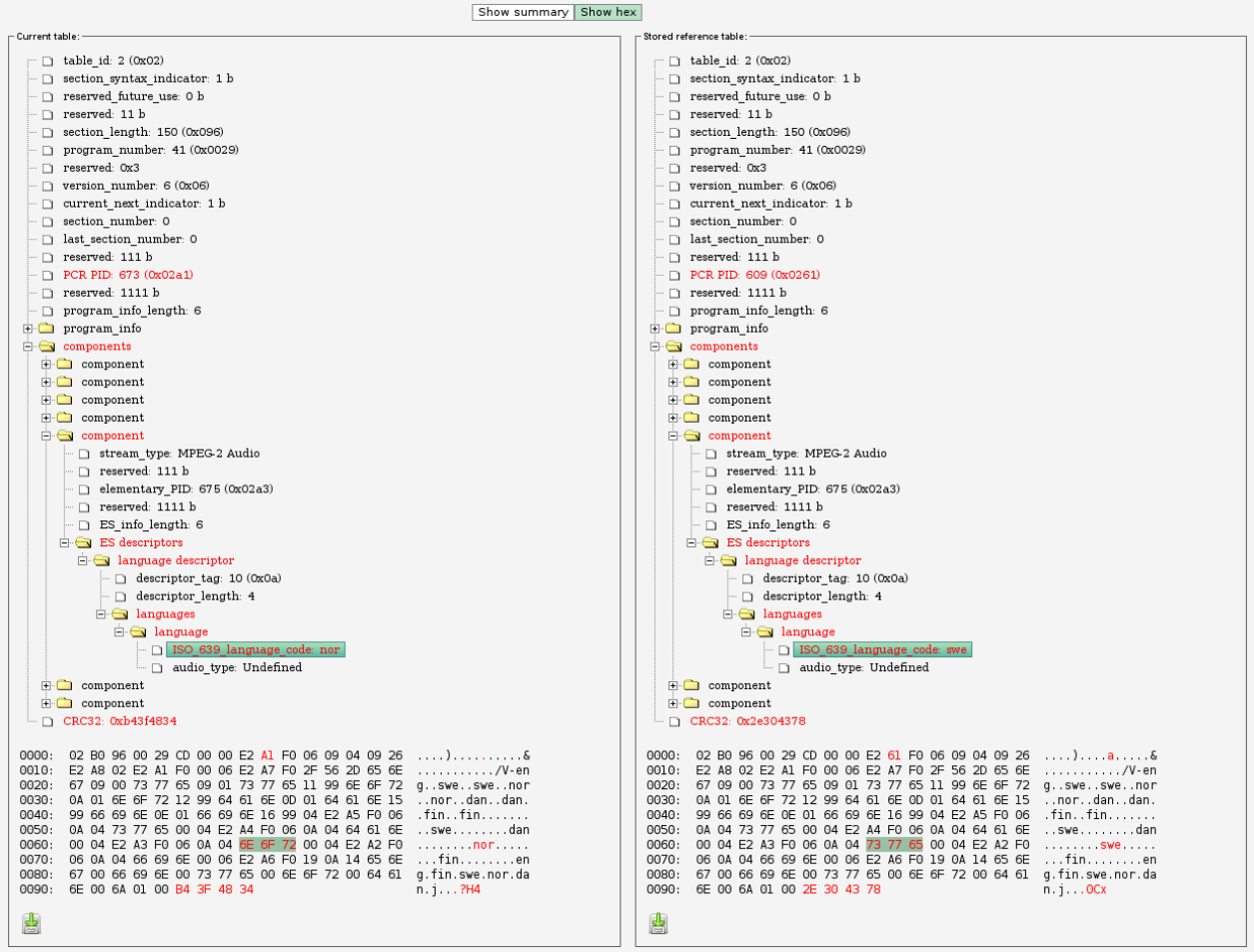
The Gold TS reference checking is performed by the ETR engines and can be performed in round

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.

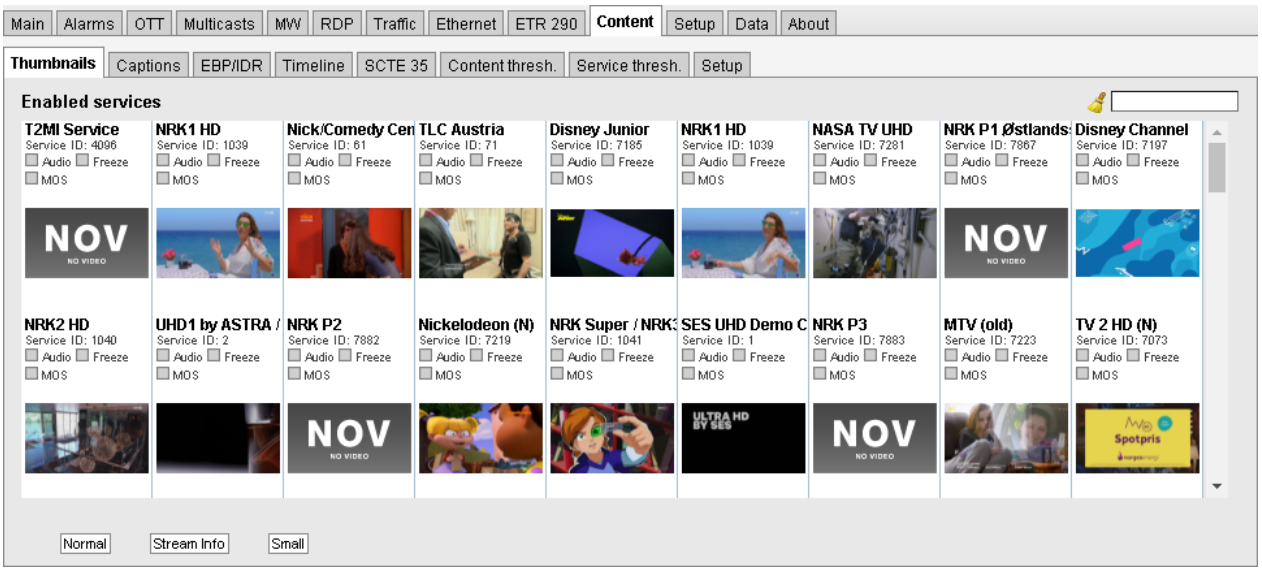
When the ETR engine is tuned to a stream it is possible to compare the tables for this stream with the stored reference tables by clicking on the entry in the list. This opens up a new window where the table data can be compared, both as a tree-breakdown and as a hexadecimal dump:



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 Content

5.10.1 Content — Thumbnails



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

If the **Small** button is clicked, the **Thumbnails** 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:

Thumbnails	
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.

Audio status:	If the probe has been licensed with the Content Extraction and Alarming option, status bulbs are displayed indicating the current audio alarm status for the streams. The audio threshold values are set as part of the content threshold template associated with each multicast or OTT channel (refer to the **Content – Content thresh.** view). The different bulb colors are: **Grey:** audio thresholds are disabled. **Green:** audio thresholds are enabled, and audio is currently normal. **Yellow:** audio thresholds are enabled, and we have detected an abnormal audio situation, but the timeout value has not been exceeded. **Red:** audio thresholds are enabled, and we have detected an abnormal audio situation and the timeout value has been exceeded, thus resulting in an alarm.
Freeze-frame status:	Status bulbs are displayed indicating the current freeze-frame and color-freeze status for the streams. The freeze-frame error timeout values are set as part of the content threshold template associated with each multicast or OTT channel (refer to the **Content – Content thresh.** view). The different bulb colors are: **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.
MOS average status:	If the probe has been licensed with the Content Extraction and Alarming option, status bulbs are displayed indicating the current MOS average alarm status for the streams. The MOS average threshold values are set as part of the content threshold template associated with each multicast or OTT channel (refer to the **Content – Content thresh.** view). The different bulb colors are: **Grey:** MOS average thresholds are disabled. **Green:** MOS average thresholds are enabled, and the MOS average is above the configured threshold. **Red:** MOS average thresholds are enabled, and the MOS average has dropped below the configured threshold, thus resulting in an alarm.

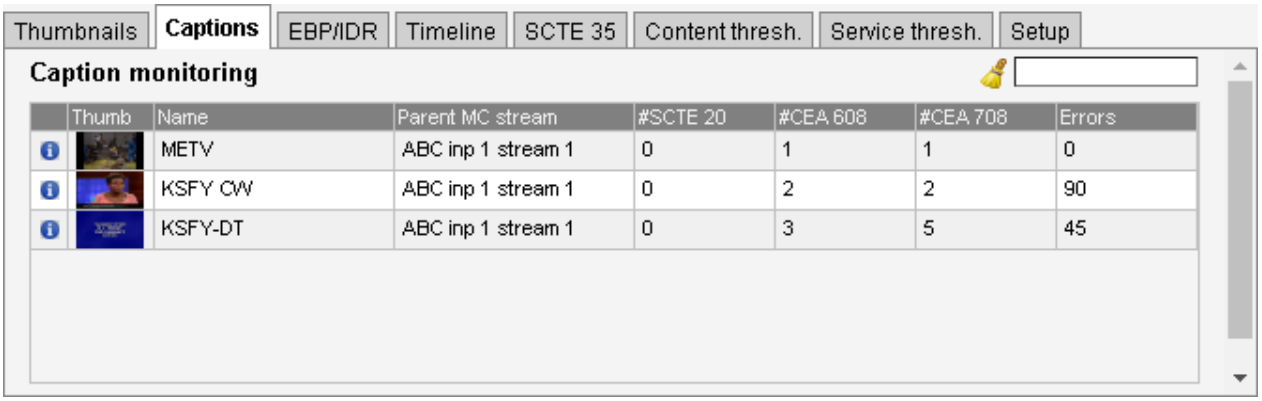
SCTE 35 status:	If the probe has been licensed with the SCTE 35 Signaling Analysis and Logging option, status bulbs are displayed indicating the current SCTE 35 alarm status for the streams. The SCTE 35 alarming threshold values are set as part of the content threshold template associated with each multicast or OTT channel (refer to the **Content – Content thresh.** view). The different bulb colors are: **Grey:** SCTE 35 alarming thresholds are disabled. **Green:** SCTE 35 alarming thresholds are enabled, and no SCTE 35 alarms are active. **Red:** SCTE 35 alarming thresholds are enabled, and one or more SCTE 35 alarms are active. Additionally, if the service is currently in SCTE 35 cue out mode, the words "CUE OUT" are displayed under the thumbnail.
Alignment status:	If the probe has been licensed with the Content Extraction and Alarming option, status bulbs are displayed indicating the current OTT alignment status for the streams. OTT alignment check is defined as part of the content threshold template associated with OTT channel (refer to the **Content – Content thresh.** view). The different bulb colors are: **Grey:** Alignment check is disabled. **Green:** Alignment check is enabled, and the OTT profiles are currently aligned. **Red:** Alignment check is enabled, and the OTT profiles are currently not aligned; an alarm is active.

The **Thumbs Details** pop-up view is accessed by clicking a thumb in the **Thumbnails** 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 freeze-frame or color-freeze alarming (Content Extraction and Alarming option) has been enabled in the Content threshold template. The same pop-up details are displayed as when opened from the **ETR 290 — Services** view.

To display thumbnails for JPEG XS services, the JPEGXS-OPT license is required.

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

5.10.2 Content — Captions (requires CONTENT-OPT)



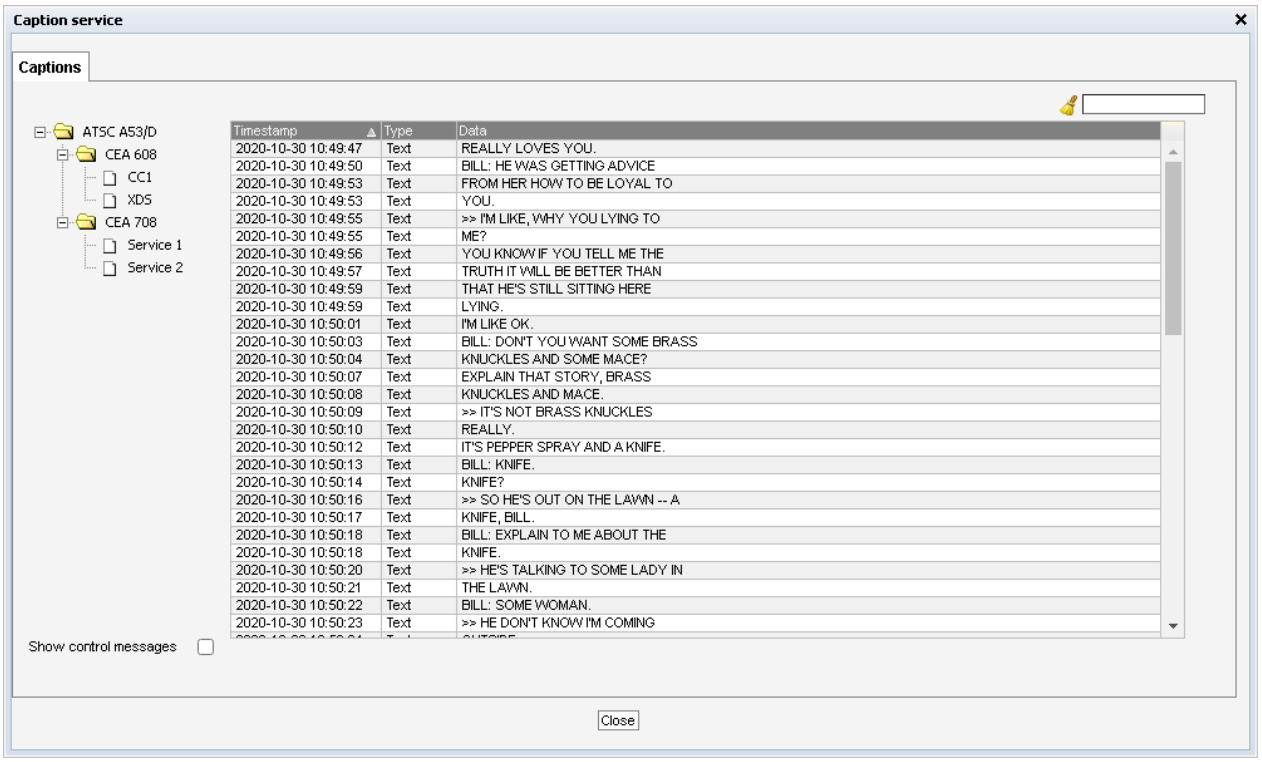
The **Content — Captions** view provides an overview of the closed caption status of each service. The services that the Software Probe extracts captions from are presented in a list of services.

Please note that this view only displays data related to closed captions carried inside the video stream. DVB Subtitling is carried on specialized PIDs and displayed elsewhere.

Thumb:	Thumbnail
Name:	Service name
Parent MC stream:	Name of the multicast stream this service is extracted from.
#SCTE 20:	Number of SCTE 20 caption services detected in this service.
#CEA 608:	Number of non-SCTE 20, CEA 608 caption services detected in this service.
#CEA 708:	Number of CEA 708 caption services detected in this service.
Errors:	Number of caption related errors on this service since joined.

Caption service

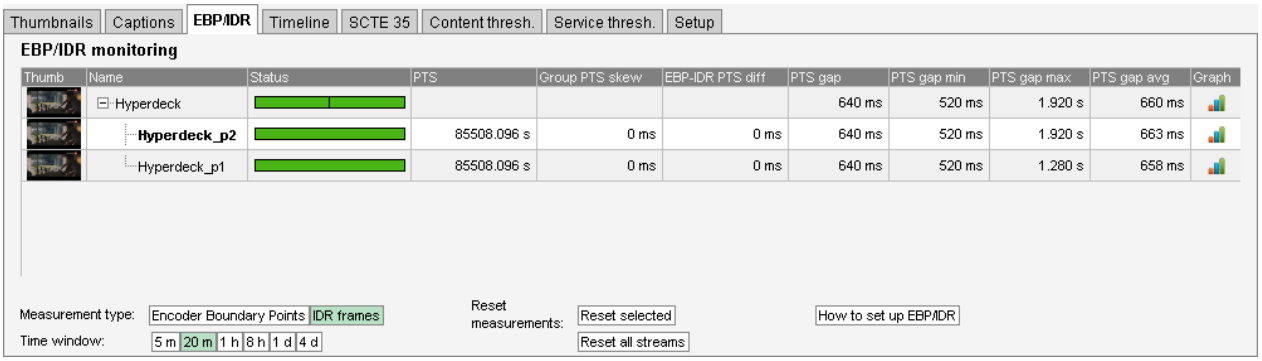
Press the blue information button on a service to open the caption service window. This window gives you access to view all closed caption services, and see the alarms for this service.



The **Caption service — Captions** view in this pop-up consists of a closed caption service format selector, and the list to display the select captions.

By default, only the closed caption text is shown in the list. If you would like to see all control messages as well, check the **Show control messages** checkbox at the bottom left.

5.10.3 Content — EBP/IDR (requires CONTENT-OPT)



The Encoder Boundary Point (EBP) monitoring is designed to monitor Adaptive Transport Streams (ATS) carrying boundary signaling. The VB330-SW presents Presentation Time Stamp (PTS) measurements and calculations for IDR frames, and EBPs following the OpenCable EBP specification[3].

[3]Encoder Boundary Point Specification, Version I01, OC-SP-EBP-I01-130118 `https://www.cablelabs.com/specifications/encoder-boundary-point-specification?v=I01`

Buttons in the GUI control which data is presented in the table. Streams that belong to the same ATS group can be grouped together, and a reference stream can be selected. The VB330-SW will give information about each stream and compare streams within the groups.

The table in the GUI uses a tree structure. Each group will have an entry in the table followed by the streams in the group. Streams without a group will be put under *Not grouped*. The different measurements and calculations, along with all elements of the **Content — EBP** view, are described in the following tables. A setup guide is located at the end of this section. A short guide is also available directly in the GUI by clicking the **How to set up EBP** button.

Thumb:	The thumbnails will not always be generated at the same time for all streams in a group. This means that the thumbnails displayed in the user interface might differ even though the streams are synchronized.
Name:	The name of the stream or group. A group row will have a + or - sign to the left of the name. This can be used to expand and collapse the group. If a name is highlighted in the table it means that it is the reference for **Group PTS skew** calculations for the group members.
Status:	The EBP status of the stream or group. The colors reflect the status of the EBP or IDR frame alarms. A group's status will have one field per member and show the status of all stream members. These are not in order. The colors show the following • **Green**: No active alarms • **Red**: One or more alarms are active • **Grey**: The stream has *No signal*
PTS:	The latest PTS read, for the boundaries (EBP or IDR frame) depending on the *Measurement type* selected.
Group PTS skew	The skew between the stream's and the group reference's boundary PTSs. This value is calculated based on the points that are expected to be synchronized. If a stream has fallen out of sync with the group, the value is updated continuously. The value is calculated by subtracting the reference's PTS from the stream's PTS. A positive value means the PTS of the stream is larger (later in time) than that of the reference. A negative value means smaller (before in time). Typically the streams will share the same PTSs, and the skew is expected to be 0.
EBP-IDR PTS diff	The difference between the PTS of the packet containing the EBP, and the PTS of the IDR frame. As the header indicates, the IDR frame PTS is subtracted from the EBP PTS. A positive value means the PTS of the stream is larger (later in time) than that of the reference. A negative value means smaller (before in time). An ATS is expected to carry an EBP in the IDR frame. In this case they have the same PTS with no difference between the EBP and IDR frame.
PTS gap	The gap between the EBP or IDR frame PTSs of the respective stream.

PTS gap min	The minimum value measured within the selected *Time window*.
PTS gap max	The max value measured within the selected *Time window*.
PTS gap avg	The average calculated from the gaps within the selected *Time window*.
Graph	Column used to open the graph pop-up.

The table below describes the buttons found at the bottom of the page.

Measurement type:	Selects which measurements are displayed in the table. The currently selected measurement type's button is highlighted. Options: **Encoder Boundary Points** or **IDR frames**
Time window:	Selects the time window of the gap statistics. The currently selected time window's button is highlighted. Time units: m = minute, h = hour, d = day. Options: **5m**, **20m**, **1h**, **8h**, **1d** or **4d**
Reset measurements:	These buttons are used to reset the EBP data of the streams. **Reset selected**: reset the EBP data of streams (table rows) currently selected in the table. **Reset all streams**: resets the EBP data of all streams.
How to set up EBP	Opens a pop-up with a short description of how to set up the EBP monitoring.

Setup guide

By default, the EBP and IDR frame PTS monitoring is not enabled. The setup consists of two main steps: create content thresholds, and configure the streams. The monitoring is controlled by the content thresholds. A stream must be assigned a content thresholds template with EBP and/or IDR frame monitoring enabled to appear in the **Content — EBP** view.

Create content thresholds:

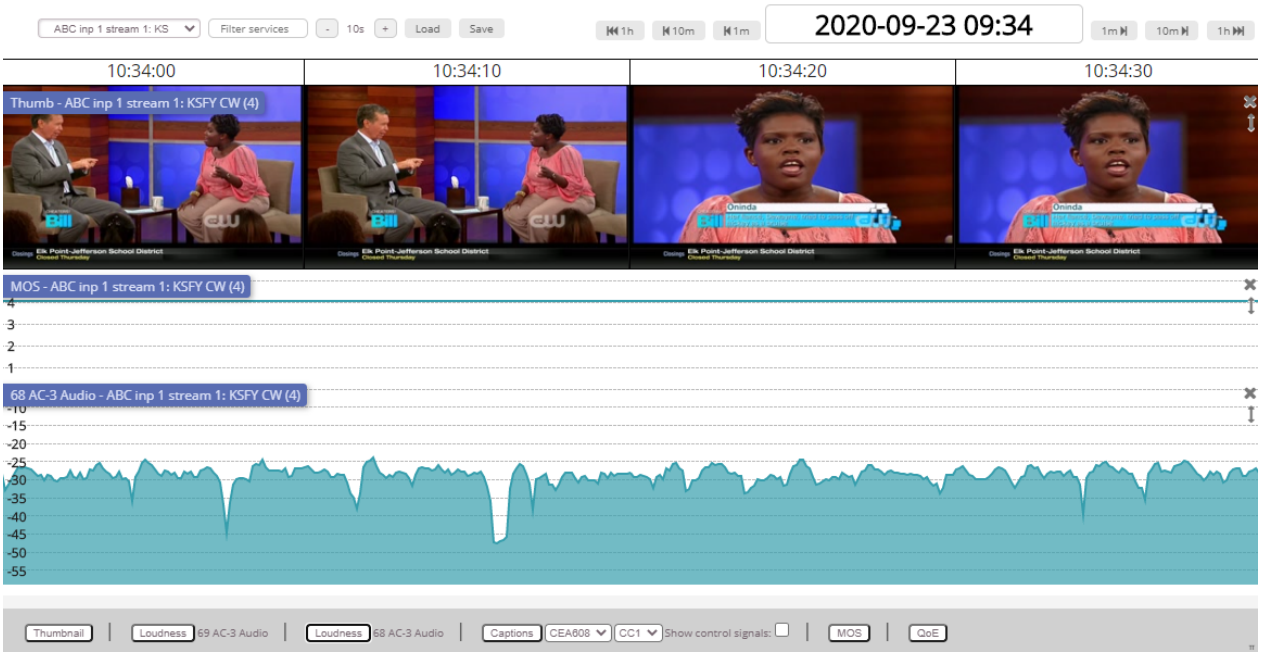
1. Go to the **Content — Content thresh.** view.
2. Create new, or edit existing, thresholds.
   - The EBP related settings are under the EBP header.
   - Hover over the field in the Threshold column for a tool-tip.
3. Enable EBP and/or IDR frame PTS monitoring.
4. Set the thresholds according to your specifications.

Add streams:

1. Go to the **Multicasts — Streams** view.

2. Add the streams you want to monitor.
3. When editing set the following: (remember that multi edit is possible)
   - **Group name** under the **General**.
   - **Group reference** under **Content** for the skew reference.
   - **Content thresholds** under **Content** selects content thresholds.
4. All streams with the same **Group name** are considered a group.
5. A reference is selected automatically if no group member has **Group reference** checked.

5.10.4 Content — Timeline (requires CONTENT-OPT)



The **Timeline** view requires the Content Extraction and Alarming option, and that a disk is mounted for the Timeline storage. If these conditions are met, the Timeline option is enabled.

If no disk is available, but the system has more than 32 Gbyte RAM installed, temporary storage is made available for the Timeline. This temporary storage will reset when the system is rebooted. If no storage is available, this view will display a message saying so.

Depending on how the file systems are mounted, the Timeline may also compete for space with data stored for use with the multi-stream recording feature.

Select **Timeline** from the **Content** tab, and the timeline should load in the main content area.

Choosing what to inspect

To change which stream and service you are looking at, select the desired service from the drop down at the top left. Note that tracks that are already added will stay put to enable comparing services. If you do not want to have the old tracks there, click the small × in the top right of each track. You can filter which streams you see by typing part of the stream or service name into the filter box. The drop down should now only be populated by the matching streams or services. To clear the filter, just click on the × in the right hand part of the filter box.

In the bottom left you can select the different types of data available for the selected service.

To remove a track, press the × located at the top right of the track you want to remove.

Some tracks can be resized by clicking on the vertical arrows located under the close button for the track.

Navigating in time

To navigate in time you have two options. Back and forth in time, and zoom in / out.

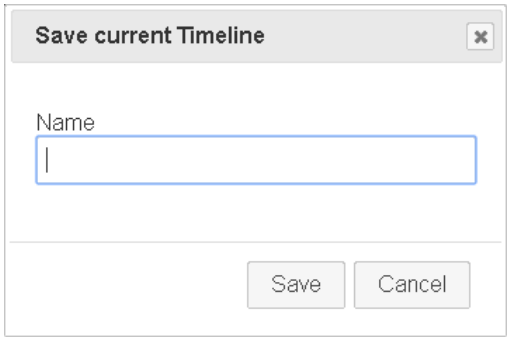
To go back and forth it time you can select the desired time from the time and date picker located at the center top. The time and date picker is most useful for large jumps in time, like if you want to look at data from days/weeks/months back in time. Just select the correct date and time, and the timeline should automatically jump to that point in time.

The buttons to the left and right of the time-picker let you move in small increments in both directions, and are most suited for smaller adjustments in time.

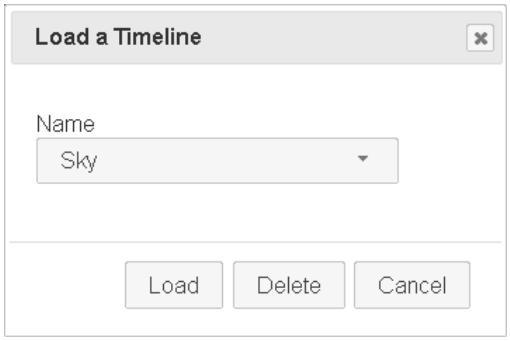
The last way to navigate in time is to drag the timeline in the direction you would want to move it. The timeline should smoothly glide with the dragging motion, and new data should pop up seamlessly.

To zoom in and out, use the + and – buttons located to the right of the filter box. Between the buttons the current zoom level is shown. The zoom level describes how much time is shown in one box.

Persistent layout



When you are happy with the widget layout, you may save the layout by pressing the **Save** button on the top of the screen and giving the layout an unique name. If you later want to update this layout, just save with the same name, and the new layout will override the old.

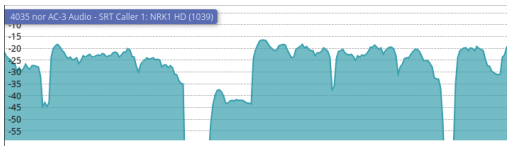


To load a previously saved layout, press the **Load** button on the top of the screen, find the layout you want in the list, and press the **Load** button. You can also delete layouts you no longer need from this view. Select the layout from the list, press the **Delete** button and confirm the deletion.

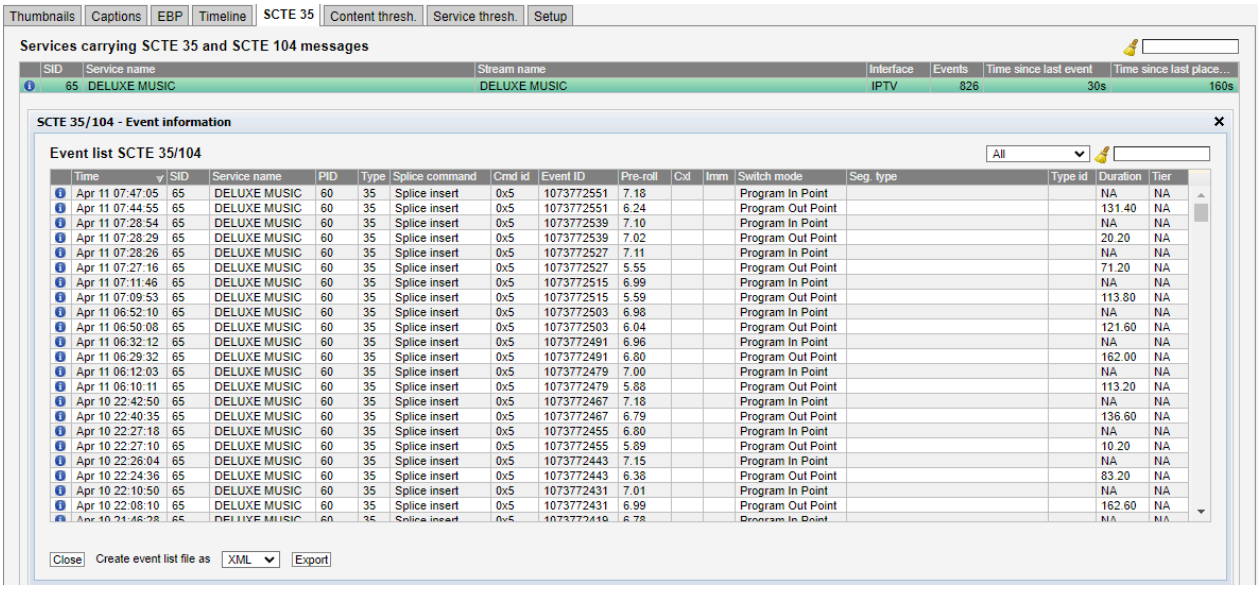
Audio silence in the timeline

Audio loudness analysis on the probe is designed to monitor and analyze the loudness of audio streams continuously, however, in certain situations the probe may become overloaded resulting in an inability to keep up with the volume of incoming audio data configured for analysis. In such situations you may notice missing audio analysis segments in the timeline. You can see an example of such a missing audio segment below:

The graphical representation of silent audio in the timeline is subtly different: notice that the thicker, darker line travels down the Y-axis towards an audio level of negative infinity (instead of abruptly disappearing from the segment). You can also see that upon audio returning from silence to once again being audible, the thick blue line travels up from negative infinity towards its new levels.



5.10.5 Content — 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 104 specifies carriage of these events in uncompressed streams.

The SCTE 35 option enables monitoring of SCTE 35 and SCTE 104 events of all streams and OTT channels monitored by the probe.

Service list parameters	
SID:	The ID of the service for which SCTE 35 or SCTE 104 data has been received.
Service name:	The name of the service for which SCTE 35 or SCTE 104 data has been received.
Stream name:	Name specified by the user when adding a multicast or tuning.
Interface:	The input source of the transport stream.
Events:	The number of SCTE 35 or SCTE 104 events seen for the service.
Time since last event:	The time since the last SCTE 35 event specified in seconds, minutes, hours or days.
Time since last placement:	The time since the last SCTE 35 placement opportunity in seconds, minutes, hours or days.

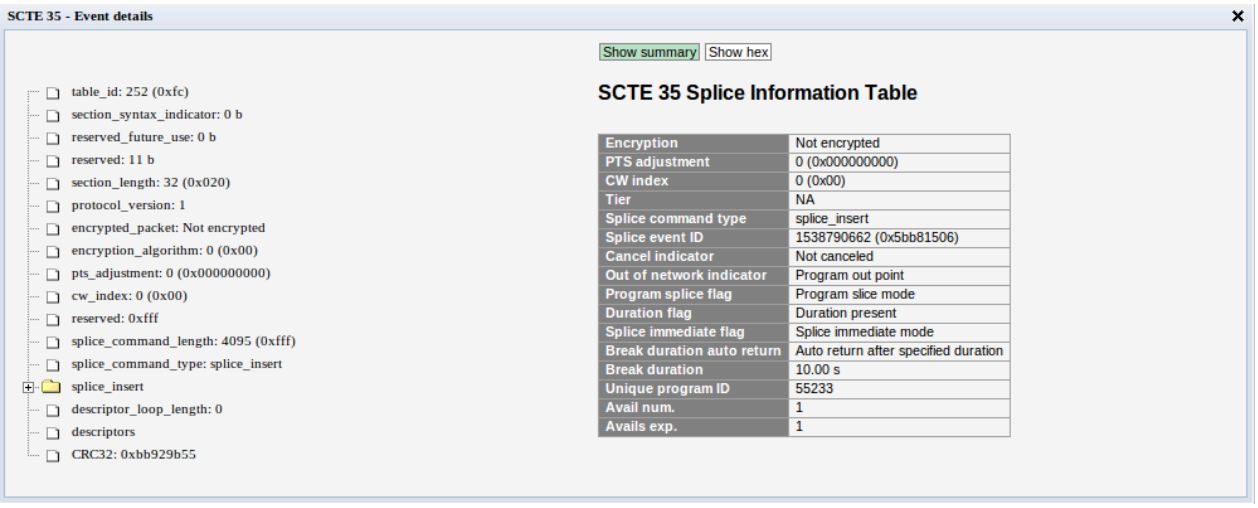
To monitor SCTE 35 and SCTE 104 information, enable the **Monitor SCTE 35** checkbox in

Content — Content thresh. and configure the transport stream or OTT channel to use that content threshold. If it contains SCTE 35 or SCTE 104 information, the 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 or OTT channel.

Event information list parameters:	
Parameter	***Description***
Time:	When the event occurred.
SID:	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 or SCTE 104 information. A service can have multiple SCTE 35 or SCTE 104 PIDs signaled in the PMT table(s).
Type:	Indicates whether the received event was SCTE 35 or SCTE 104.
Splice command:	The type of the splice command.
Cmd id:	The hex value of the command.
Event ID:	Id of the specific event.
Pre-roll:	Number of seconds before a splice the event was received.
Cxl:	Canceled indicator, if set it indicates that this splice message cancels a previously sent splice message.
Imm:	Immediate mode, if set it indicates that this message should take effect immediately.
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). For messages with the splice command type ‘Time signal’ the Switch mode parameter will be empty and the Segment type parameter will contain the details.
Seg. type:	The segmentation type found in the segmentation descriptor (if found).
Type id:	The hex value of the segmentation type parameter.
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.

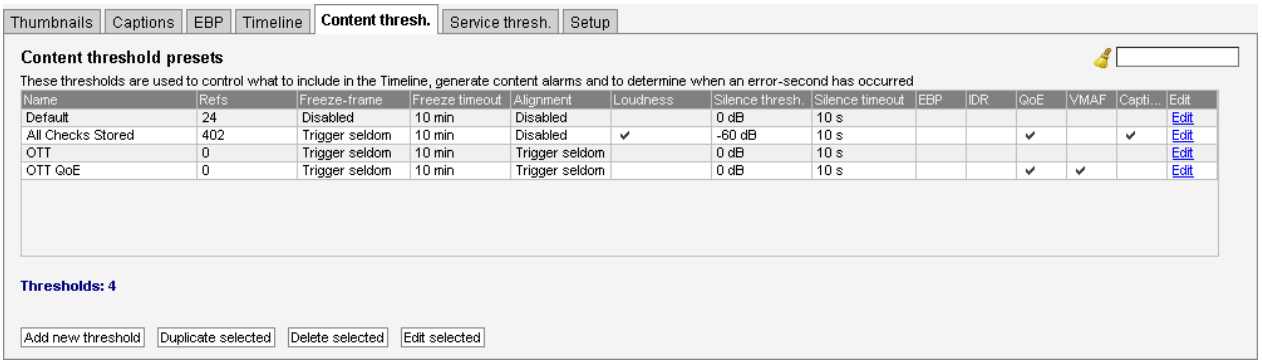
Use the drop-down at the top of the event list dialog to switch between displaying all events (default) or to display only SCTE 35 or only SCTE 104 events.

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 or SCTE 104 events signaled for the specified transport stream or OTT channel. Splice NULL messages are not logged.



Please note that for some OTT manifest formats, the SCTE 35 message is not transmitted in binary form, and the message shown in the **Event details** view is then synthesized from the available input.

5.10.6 Content — Content thresh.



Thresholds are used to determine when to actually raise an alarm upon detection of an error. The Content thresholds are used for generating content alarms as well as for calculating error-seconds. Error seconds and content alarms are issued whenever measurements exceed the defined threshold levels for a parameter. 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 **Content — Content 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** and **OTT — Channels** views. 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.

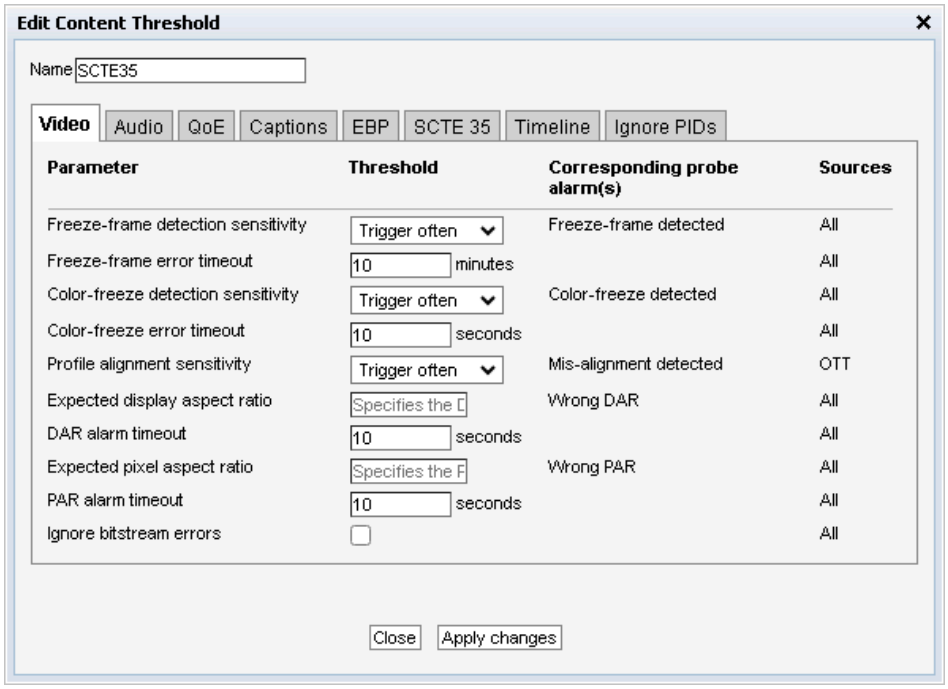
Deleting a threshold template is done by highlighting the threshold template that should be removed and clicking **Delete selected**. It is possible to delete or edit several entries simultaneously. Several

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.

The available thresholds depend on the currently active license. Applying content analysis on many concurrent streams can introduce a performance penalty, please refer to appendix B.5 for more details.

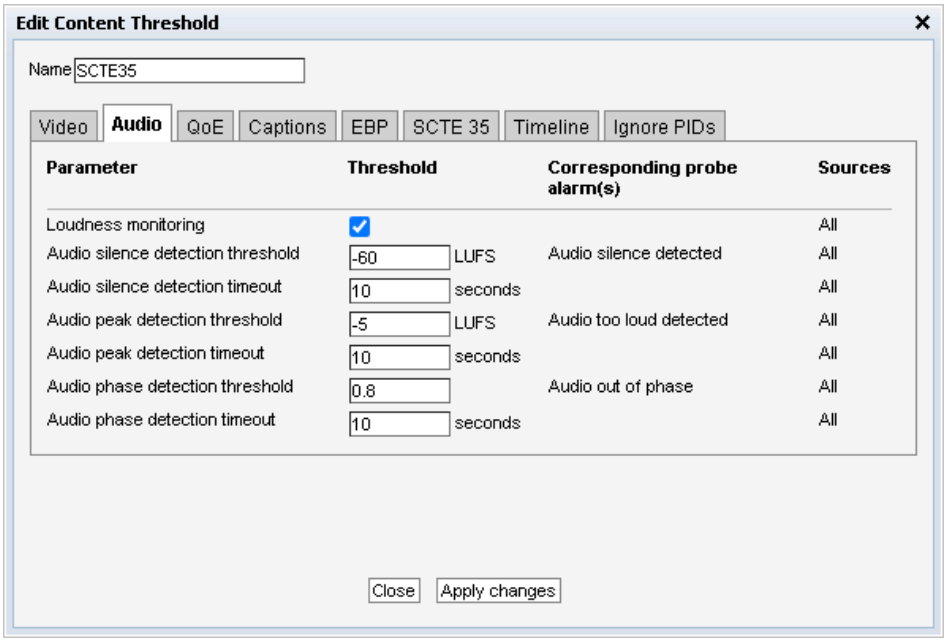
The **Sources** column indicates which of the different threshold settings are supported where.



Video

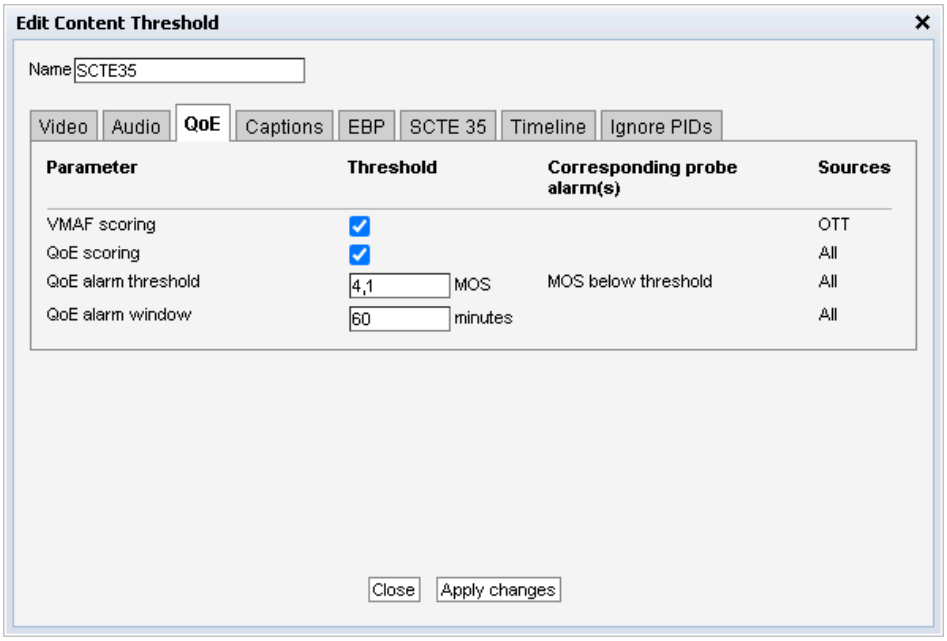
Freeze-frame detection sensitivity:	Picture matching in video streams is not an exact science, as noise can be introduced in many of the stages the stream goes through. This setting makes it possible to define the amount of noise to be allowed when performing freeze-frame detection. When set to **Disabled**, 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.
Freeze-frame error timeout:	The time (in minutes) a freeze-frame error should persist before the probe will raise an alarm
Color-freeze detection sensitivity:	This setting makes is possible to define the amount of noise to be 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.
Color-freeze error timeout:	The time (in seconds) a color-freeze error should persist before the probe will raise an alarm.
Profile alignment sensitivity:	*OTT channels only:* 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 profile alignment detection. When set to **Disabled**, profile alignment detection is disabled. When set to **Trigger seldom**, a large amount of noise is allowed when comparing the frames across profiles for out-of-alignment conditions. **Normal** is the recommended setting, whereas **Trigger often** allows only a small amount of noise, which may result in too many out-of-alignment alarms.

Expected display aspect ratio:	If this field is non-empty, an alarm will be raised if the display aspect ratio for the stream differs from the one entered here. The aspect ratio is entered on the form *n:m* (e.g *16:9* or *4:3*).
DAR alarm timeout:	The minimum number of seconds during which an alarm remains active when the Expected display aspect ratio is not correct.
Expected pixel aspect ratio:	If this field is non-empty, an alarm will be raised if the pixel aspect ratio for the stream differs from the one entered here. The aspect ratio is entered on the form *n:m* (e.g *1:1* or *2:1*).
PAR alarm timeout:	The minimum number of seconds during which an alarm remains active when the Expected pixel aspect ratio is not correct.
Ignore bitstream errors:	In some cases, the video codec reports errors in the bit-stream while still being able to generate thumbnails or partial thumbnails. If the stream shows a "Bitstream Errors" icon, you can try to ignore this by enabling this setting.

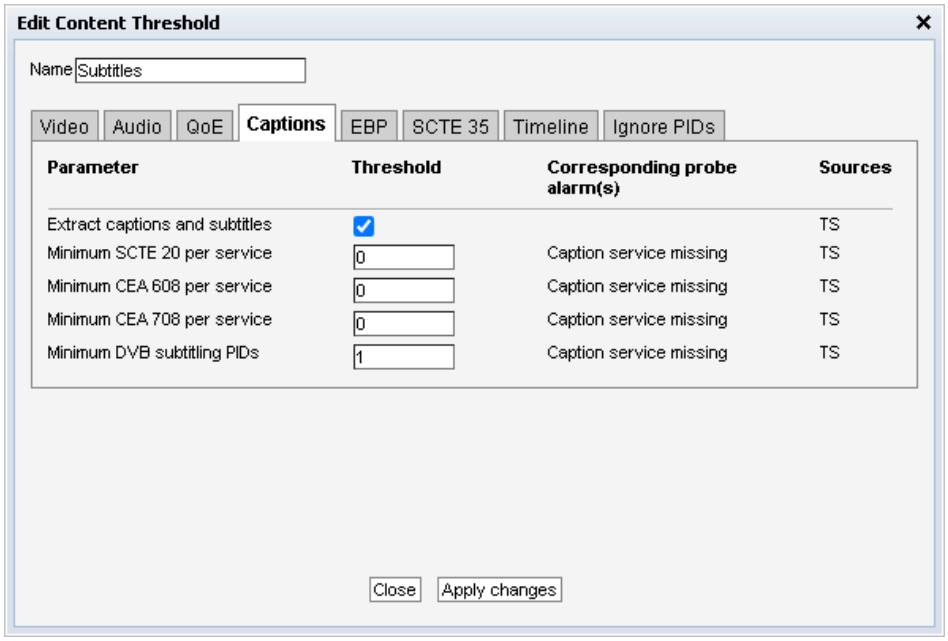


Audio

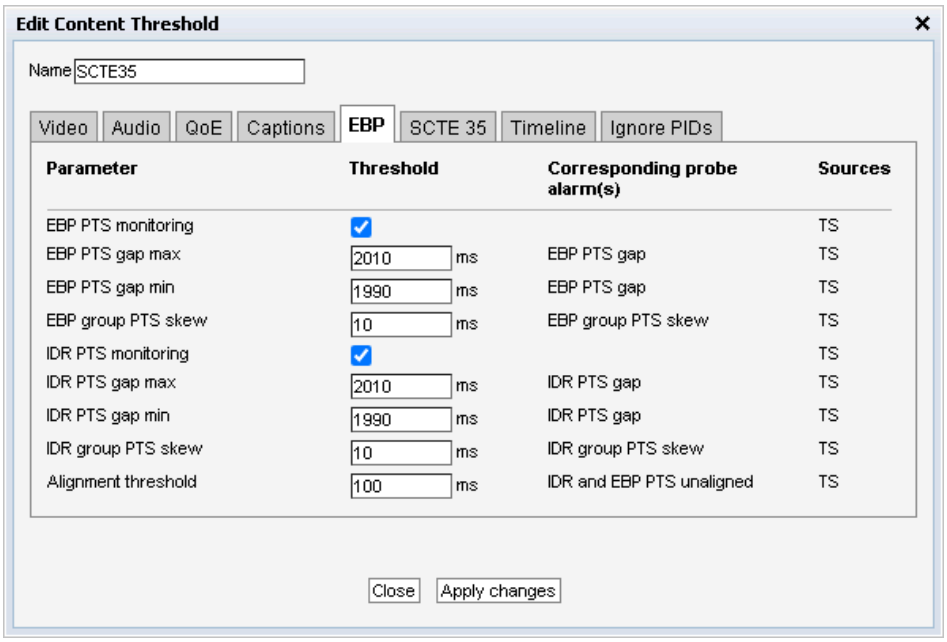
Loudness monitoring:	Enables real-time loudness extraction for the stream. The loudness data can be retrieved through the Eii.
Audio silence detection threshold:	The value in LUFS/LKFS when to trigger the audio silence alarm. Setting this to a value of 0 disables audio silence detection.
Audio silence detection timeout:	The number of seconds that audio has to be below the silence detection threshold before the audio silence alarm is triggered.
Audio peak detection threshold:	The value in LUFS/LKFS when to trigger the audio too loud alarm. Setting this to a value of 0 disables audio peak detection.
Audio peak detection timeout:	The number of seconds that audio has to be above the peak detection threshold before the audio too loud alarm is triggered.
Audio phase detection threshold:	For two channel audio (stereo or dual mono), this defines the threshold for when to report out of phase audio. A value of –1 indicates audio that is completely out of phase, whereas a value of 1 indicates audio that is completely in phase. Setting this to a value of –1 disables audio phase detection.
Audio phase detection timeout:	The number of seconds that audio has to be above the phase detection threshold before the audio out of phase alarm is triggered.



QoE	
VMAF scoring:	*OTT channels only:* When enabled, the VB330-SW will compare the different profiles and create a VMAF score relative to the profile with the highest bitrate.
QoE scoring:	Enables picture analysis and MOS scoring.
QoE alarm threshold:	Set the threshold for average MOS. If QoE scoring is enabled and this value is set to a a value above 1.0, an alarm will be triggered if the MOS average drops below this value. Set to 1.0 to disable the alarm.
QoE alarm window:	The time (in minutes) over which to calculate the MOS average for alarming purposes.

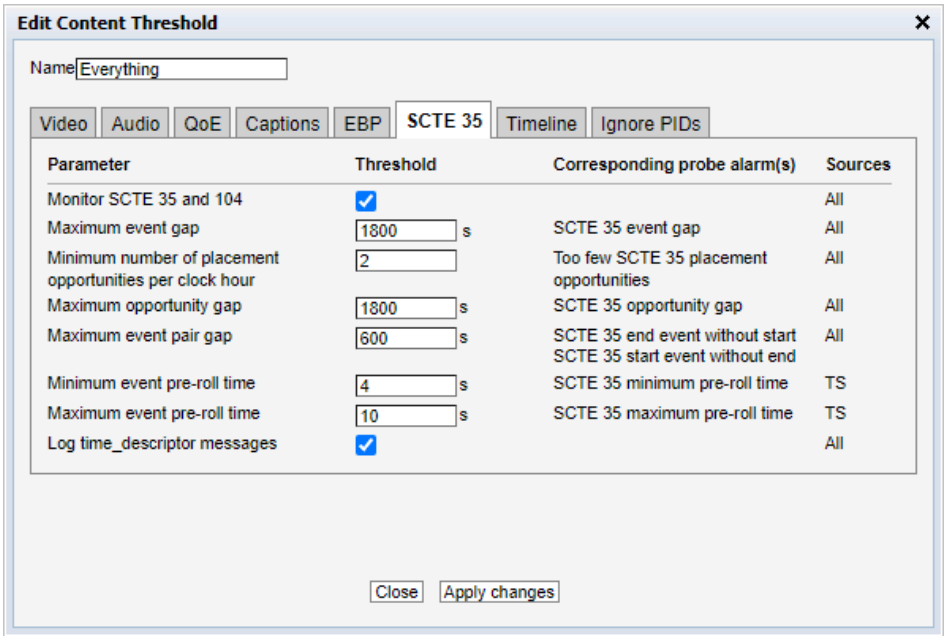


Captions	
Extract captions and subtitles:	Enable extraction of closed captions from the video stream and of DVB subtitles.
Minimum SCTE 20 per service:	The minimum number of SCTE 20 caption services that has to be present in the video stream before an alarm is triggered.
Minimum CEA 608 per service:	The minimum number of non-SCTE 20 CEA 608 caption services that has to be present in the video stream before an alarm is triggered.
Minimum CEA 708 per service:	The minimum number of CEA 708 caption services that has to be present in the video stream before an alarm is triggered.
Minimum DVB subtitling PIDs:	The minimum number of DVB subtitling PIDs that has to be present in the service before an alarm is triggered.



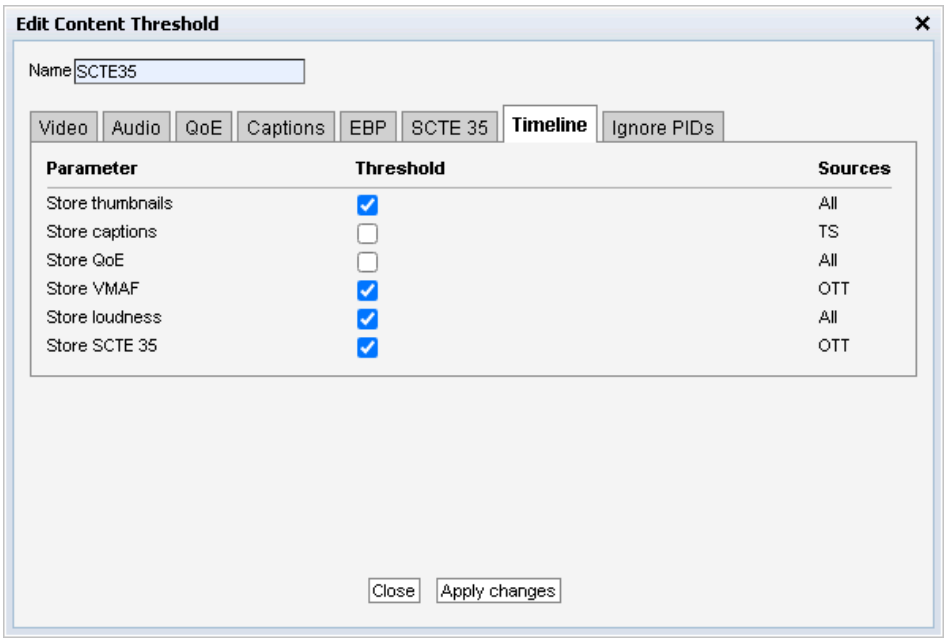
EBP	
EBP PTS monitoring:	When *EBP PTS monitoring* is enabled, the probe will look for EBPs, and the respective PTS, in the stream. The table in the **Content — EBP** view will present the stream's EBP related information. This setting only applies to the table's *Encoder Boundary Points Measurement type*. The stream is only visible in the table when *EBP PTS monitoring* is enabled.
EBP PTS gap max:	The upper EBP PTS gap threshold. Gaps longer than this threshold will raise an alarm. Set this and gap min to -1 to disable the alarm.
EBP PTS gap min:	The lower EBP PTS gap threshold. Gaps shorter than this threshold will raise an alarm. Set this and gap max to -1 to disable the alarm.
EBP group PTS skew:	The absolute value of the group PTS skew allowed before an alarm is raised. The skew is calculated based on the group reference stream. set to -1 to disable alarm
IDR PTS monitoring:	When *IDR PTS monitoring* is enabled, the probe will look for IDR frames, and the respective PTS, in the stream. The table in the **Content — EBP** view will present the stream's IDR frame related information. This setting only applies to the table's *IDR frame Measurement type*. The stream is only visible in the table when *IDR PTS monitoring* is enabled.
IDR PTS gap max:	The upper IDR frame PTS gap threshold. Gaps longer than this threshold will raise an alarm. Set this and gap max to -1 to disable alarm.
IDR PTS gap min:	The lower IDR frame PTS gap threshold. Gaps shorter than this threshold will raise an alarm. Set this and gap max to -1 to disable alarm.

IDR group PTS skew:	The absolute value of the group PTS skew allowed before an alarm is raised. The jitter is calculated based on the group reference stream. set to -1 to disable alarm.
Alignment threshold:	The maximum PTS difference allowed between an EBP and the associated IDR frame. Set to -1 to disable alarm.

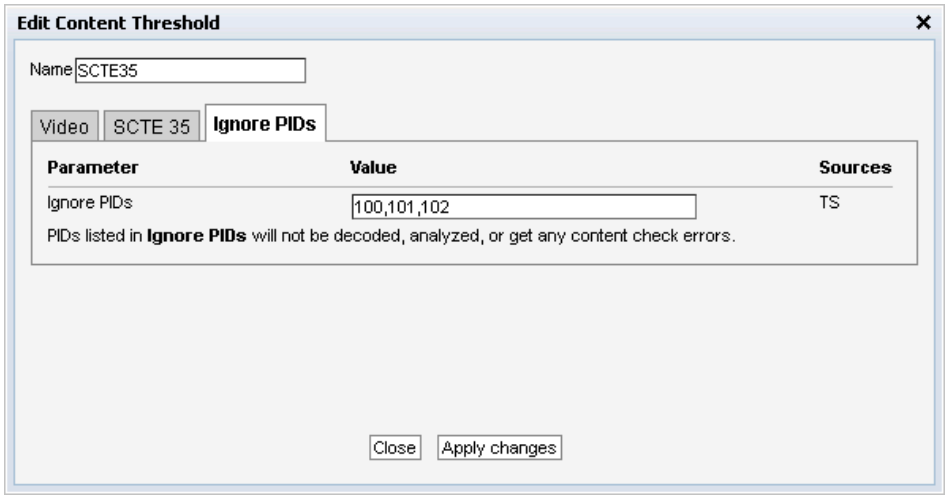


SCTE 35	
Monitor SCTE 35:	If enabled, SCTE 35 and SCTE 104 events are captured and displayed in the **Content – SCTE 35** view
Maximum SCTE 35 event gap:	Specifies the maximum number of seconds allowed between two SCTE 35 or SCTE 104 events before an alarm is raised. Set to –1 to disable the alarm.
Minimum number of placement opportunities per clock hour:	Specifies the minimum number of placement opportunities that must be signaled for a full clock hour. An alarm will be raised at the top of the hour if the previous hour had fewer than this number of opportunities. Set to –1 to disable the alarm.
Maximum SCTE 35 opportunity gap:	Specifies the maximum number of seconds allowed between two SCTE 35 or SCTE 104 placement opportunities before an alarm is raised. Set to –1 to disable the alarm.

Maximum event pair gap:	Specifies the maximum number of seconds allowed between the a SCTE 35 or SCTE 104 start and end segmentation descriptor messages in Time signal events. An alarm will be raised for five seconds when this is detected. Additionally, an alarm will be raised if an end segmentation message was received without the corresponding start message. Set to –1 to disable these alarms.
Minimum event pre-roll time:	Specifies the minimum number of seconds allowed between when the SCTE 35 event is received and when the splice is supposed to happen. An alarm will be raised for five seconds when this is detected. Set to –1 to disable these alarms.
Maximum event pre-roll time:	Specifies the maximum number of seconds allowed between when the SCTE 35 event is received and when the splice is supposed to happen. An alarm will be raised for five seconds when this is detected. Set to –1 to disable these alarms.
Log time_descriptor messages	Determines whether the SCTE 35 or SCTE 104 messages containing nothing else than a time_descriptor should be included in the message log. 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 SCTE 35 or SCTE 104 PID). If the message log is filled up with the time_descriptor messages, disable logging of these messages

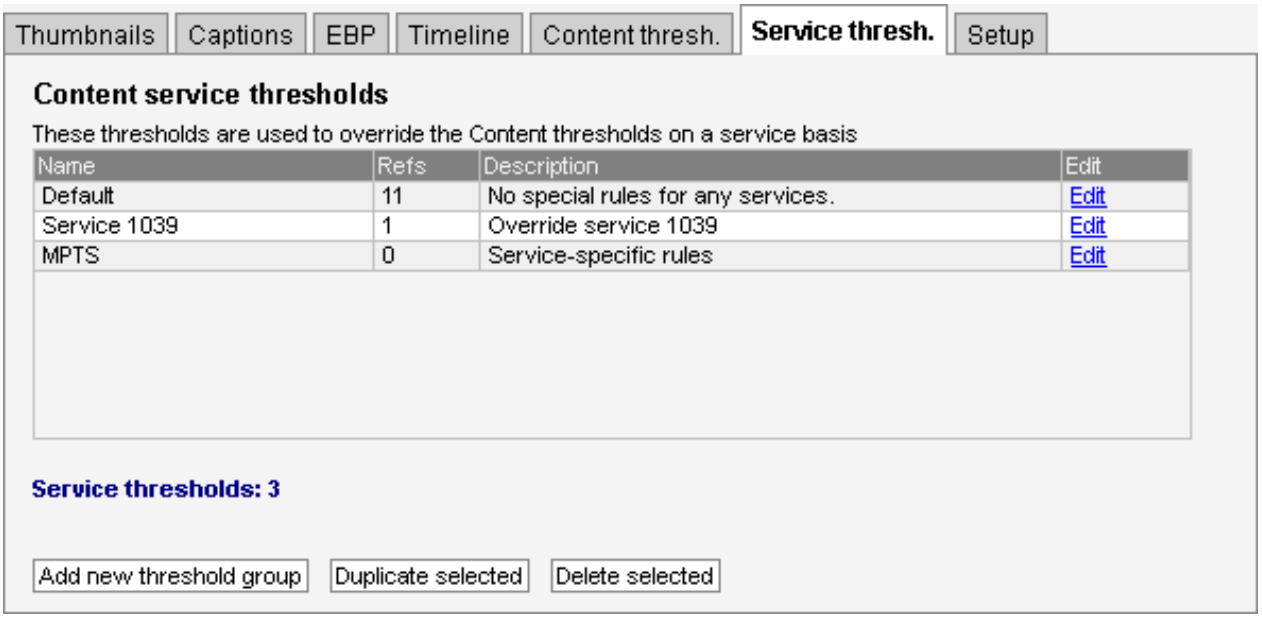


Timeline	
Store thumbnails:	If enabled, thumbnails are stored for display in the **Content — Timeline** view. Note that the **Extract thumbnails** checkbox in the tuning setup must be checked for this to take effect.
Store captions:	If enabled, closed captions are stored for display in the **Content — Timeline** view. Note that the **Extract thumbnails** checkbox in the tuning setup must be checked for this to take effect.
Store QoE:	If enabled, QoE scores are stored for display in the **Content — Timeline** view. Note that the **QoE scoring** checkbox must be checked for this to take effect.
Store VMAF:	If enabled, VMAF scores are stored for display in the **Content — Timeline** view. Note that the **VMAF scoring** checkbox must be checked for this to take effect.
Store loudness:	If enabled, loudness data are stored for display in the **Content — Timeline** view. Note that the **Loudness monitoring** checkbox must be checked for this to take effect.
Store SCTE 35:	If enabled, SCTE 35 events are stored for display in the **Content — Timeline** view. Note that the **Monitor SCTE 35 and 104** checkbox must be checked for this to take effect.



Ignore PIDs	
Ignore PIDs:	*Not applicable to OTT channels:* A comma separated list of PIDs for which the probe should not decode, analyze or report any content check errors. No thumbnails, loudness or captions will be decoded on these PIDs.

5.10.7 Content — Service thresh.



Thresholds are used to determine when to actually raise an alarm upon detection of an error. The **Content — Service thresh.** view makes it possible to define detailed conditions for alarm triggering on a per-service basis. This is particularly useful to specify individual alarm handling rules for services in a multi-program transport stream (MPTS). Note that if there is a stream and service threshold mismatch, the service threshold will apply. This may be the case if QoE or scheduling

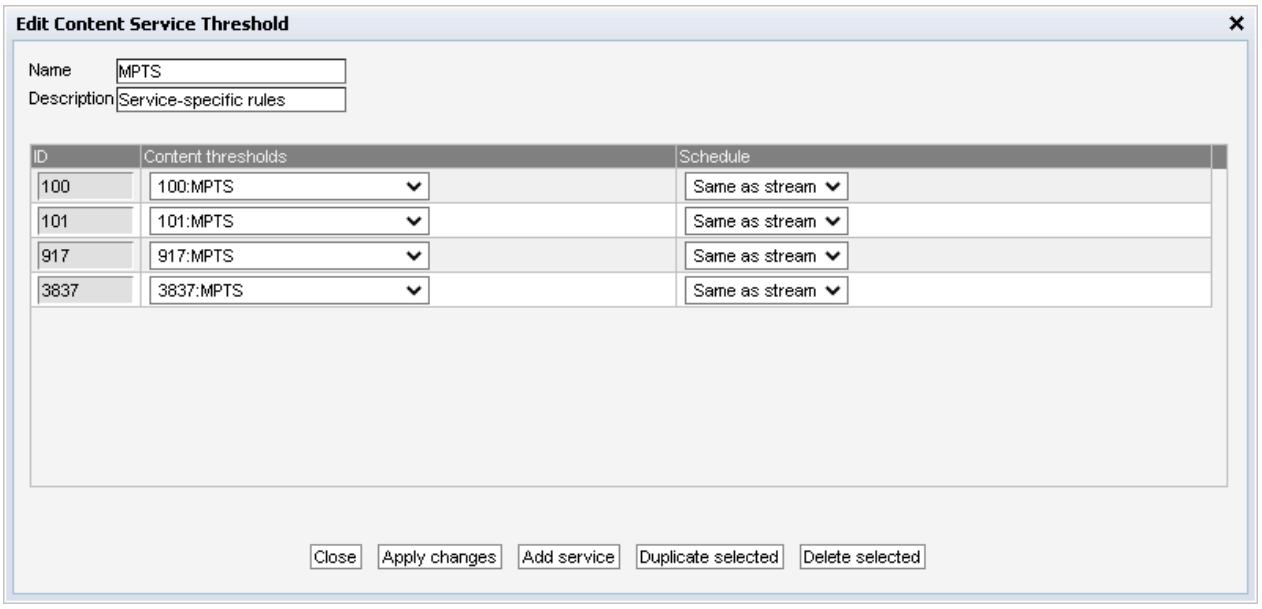
requirements are set differently in the stream threshold template and service threshold template associated with a stream. There is one predefined service threshold template that cannot be edited by the operator: **Default**. The Default service threshold template contains no service definitions and 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.

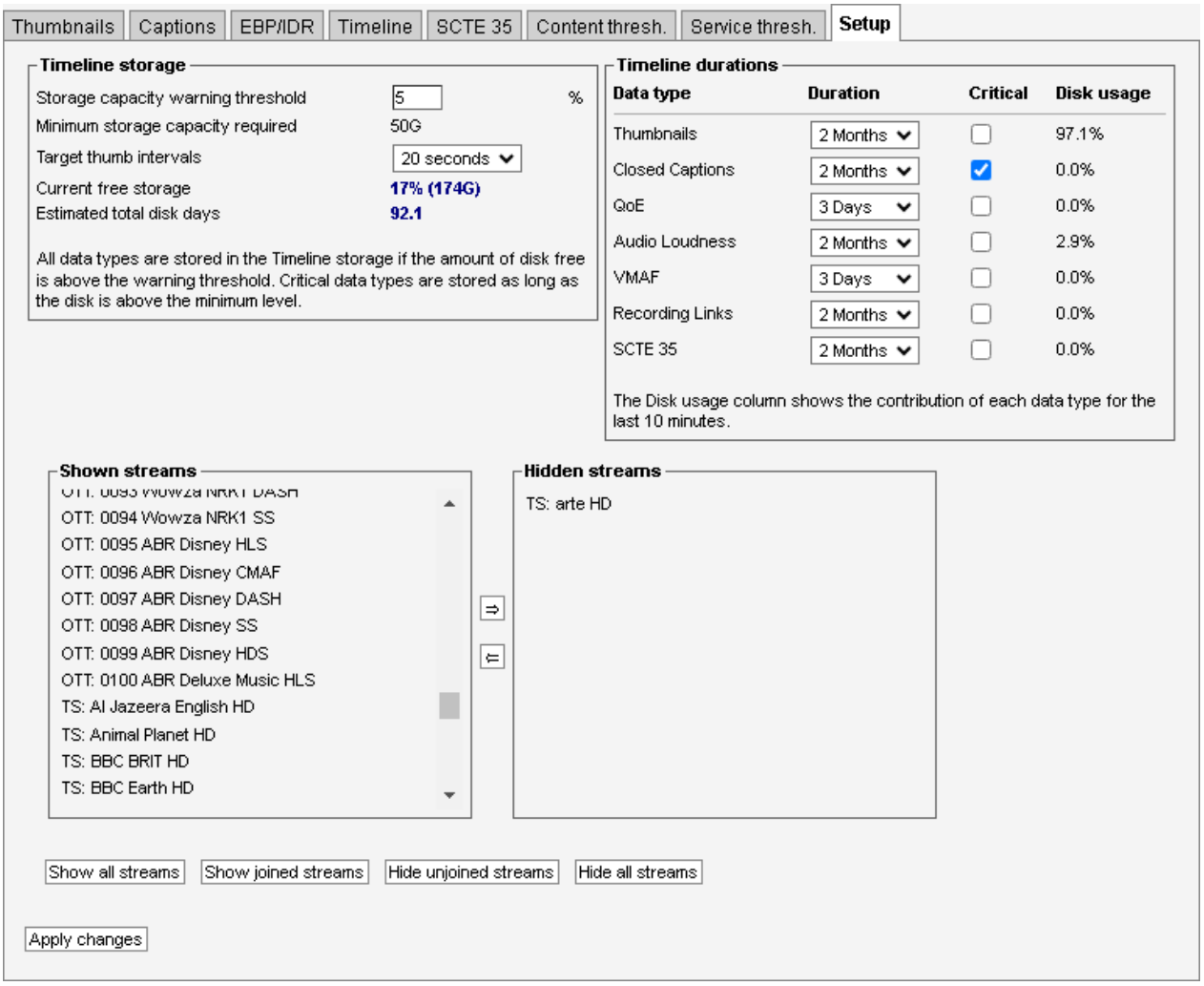
Deleting a service threshold template is done by highlighting the template that should be removed and clicking **Delete selected**. Note that if the deleted threshold template was assigned to a stream being monitored, the new threshold template for that stream will default to the **Default** template.



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	
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.
Content thresholds:	This settings defines the content threshold settings that should be applied to this stream. The entire content threshold setting, with the exception for the 'Ignore PIDs' setting, will be applied to the service. Please refer to chapter 5.10.6 for the specific meaning of the settings. Set this to *Same as stream* to apply the default content thresholds for this service.
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. When *Same as stream* is selected, the requirement defined in the stream threshold will apply. Note that alarm masking only affects alarm lists and SNMP traps; other alarm indications in the GUI will remain visible.

5.10.8 Content — Setup (requires CONTENT-OPT)



The **Content — Setup** view is used to configure storage and display parameters for the Timeline. The individual streams that should be archived and made available in the **Content — Timeline** view are configured using the **Content — Content thresh.** view.

The Timeline view requires a dedicated file system being available for storage. If no disk has been mounted and the system has enough RAM available, a RAM disk filesystem will be created for the Timeline. In this case, Timeline data will be lost when the probe is rebooted, either explicitly, or as a result of a power failure. A message stating that no disk has been mounted for Timeline storage is displayed in this case.

By default, all streams available in the Timeline database are available in the selection drop-down. If services have undergone many renames, the **Shown/hidden streams** view can be used to select which streams should be available.

Use **Show joined streams** to move all streams that are currently joined to the **Shown streams** list. Use **Hide unjoined streams** to move all streams that are currently not joined to the **Hidden streams** list.

Timeline storage	
Storage capacity warning threshold:	This defines the amount of free space that should be available on the file system holding the Timeline database before a warning is issued. Archiving of data types not marked as critical is suspended when the free space goes below this threshold. When you get an alarm saying the disk is getting full, you can change the configuration to keep it for a shorter duration, or add more disk to the server. If the multi-stream recording feature is used and data is stored on the same file system as is used for the Timeline, it is recommended that this value is configured to be lower than the value in the **Record — Setup** view if Timeline data is to take precedence of recordings.
Minimum storage capacity required:	This value is the amount of free space that should be available on the file system holding the Timeline database for any data to be stored in the database. This value is set to five percent or fifty gigabytes, whichever is lowest.
Target thumb intervals:	Allows the interval between updated thumbnails in the timeline to be selected, between 1 and 60 seconds. This is the targeted refresh and will never be faster than the frequency at which full-frame pictures are present in the stream (IPTV) or the segment duration (OTT).
Current free storage:	This shows the currently available free space on the file system holding the Timeline database.
Estimated total disk days:	Number of days of data the disk can hold, according to current settings. This number is based on the disk usage figures in the Timeline durations frame. Depending on how the file systems are mounted, the Timeline may also compete for space with data stored for use with the multi-stream recording feature, in which case the number presented here might not be accurate.

Timeline durations

Duration:	For each supported data type, this selects for how long data is retained in the Timeline database.
Critical:	If a data type is set as critical, it is still stored in the Timeline database if the amount of free space drops below the warning threshold, as long as it is above the minimum storage capacity required value.
Disk usage:	The actual disk usage for each of the available data types over the last 10 minutes. The value is used to calculate the *Estimated total disk days*. When changing a setting affecting disk usage, these figures should begin to settle within 10 minutes.

5.11 Record

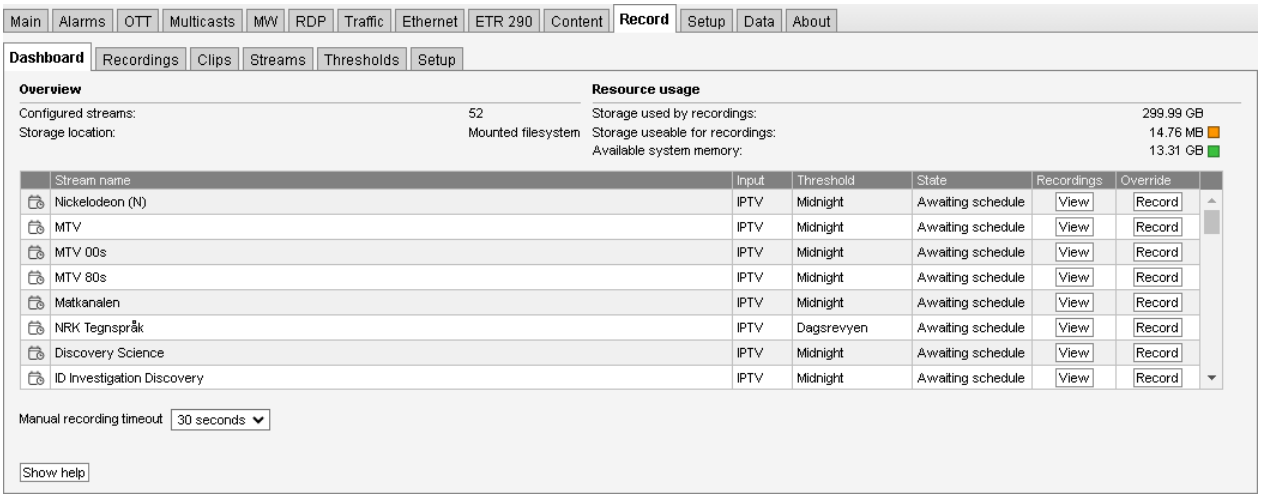
The multi-stream recording feature enables recording streams to file, either directly, on a schedule, or triggered by alarms or events. Streams may be recorded from IPTV interfaces.

By default, the Software Probe can record up to two streams simultaneously. With license upgrades, up to 200 streams can be recorded in parallel at an aggregate bandwidth of 10 Gbit/s.

The multi-stream recording feature is designed and tested to keep up to 100000 recordings stored on a probe at a given time. Exceeding this may cause undefined behavior.

The probe can be instructed to record a stream through the graphical user interface, or the external integration interface. In the graphical user interface there are five sub-views related to the multi-stream recording feature.

5.11.1 Record — Dashboard



The **Record — Dashboard** view contains an overview of recording activity on the probe and a list of streams that are currently configured to be recorded, or where recording was started manually.

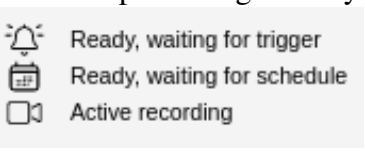
The overview consists of key attributes outlining the state of the probe when it comes to recording.

Overview	
Configured streams:	This attribute sums up how many streams that are configured to be recorded, using a Threshold. The streams may be configured to start recording according to a schedule and / or triggered by an event or alarm.
Storage location:	This attribute describes where recordings are stored. Recordings may be stored in: • Root filesystem: The recordings are are stored in the same location as the system files. If the disk space occupied by the recordings grow beyond the set safety margins for unknown reasons then it could affect the probe upgrade process. • RAM disk filesystem: Recordings are stored in a filesystem located in volatile memory. The data will be lost when the probe is rebooted, either explicitly, or as a result of a power failure. • Mounted filesystem: Recordings are stored in a filesystem mounted to the record directory (or its parent directory). The recorded files will not be conflicting with system files, but may still compete for space with data stored for use with the Timeline feature etc.
Storage used by recordings:	The current amount of disk space used by recordings.
Storage usable for recording:	The amount of space that can be used for further recordings, taking into account the current settings for maximum disk usage for recordings, and the actual free space on the partition recordings are stored on.
Available system memory:	The available of free memory.

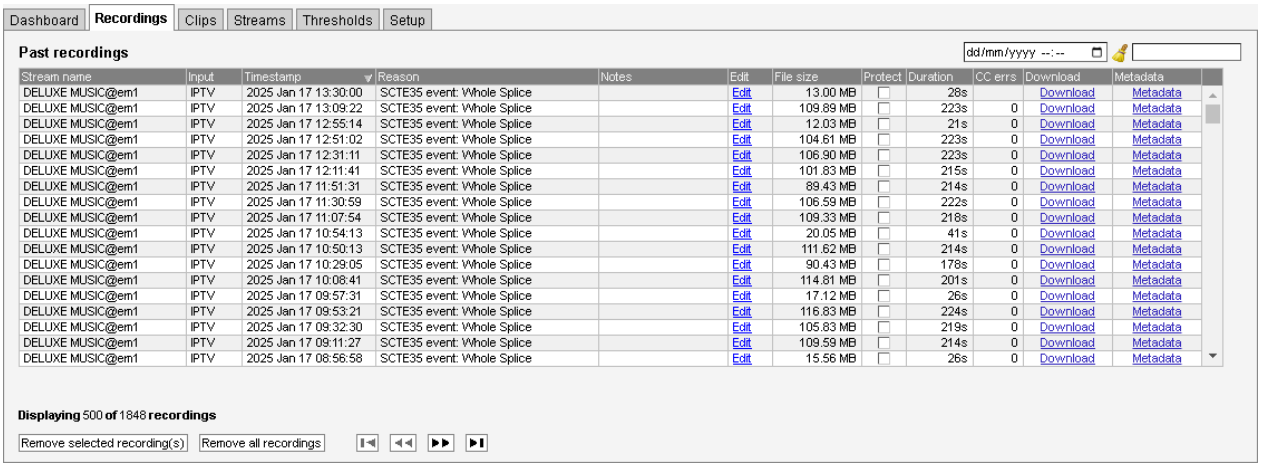
Bulbs are shown colored based on the amount of available disk space and memory to be used for recording in the system. The disk space bulb is green if there are lots of usable space, orange if there is still usable space, but it is low, and red if there are no more space for further recordings. The memory bulb is green if there is enough memory available for the configured recordings, and red if there is not. System alarms are raised if there is not enough memory or disk available.

A list of currently configured streams are also present in this view. The following columns are present in the list:

Dashboard recording list columns

Icon:	An icon representing the way the stream is configured is present. 
Stream name:	The name of the stream that is recorded. This name is configured in the stream source (e.g. **multicast** view).
Input:	Input type of the stream. Currently only IPTV is supported.
Threshold:	The recording threshold assigned to this stream.
State:	Displays the status of the stream: • Awaiting schedule: The stream is configured for scheduled recording, and is waiting for the scheduled starting time. • Awaiting trigger: The stream is configured for triggered recording, and is waiting for the triggered action to occur. • Awaiting both: The stream is waiting for both of the above. • Recording: The stream is currently recording.
Recordings:	This button takes the user to the **recordings** view with the stream name entered as a filter. Thus earlier recordings for the stream will be listed.
Override:	Allows the user to override the current state by using the button: • Record: Immediately start a manual recording for the stream. The length of this manual recording is determined by the **Manual recording timeout** option below the list. • Stop: The stream is currently being recorded. Click the stop button to end the recording immediately. • Grayed out record: The stream currently has no signal and cannot be recorded at this time.

5.11.2 Record — Recordings



The **Recordings** view presents past and currently active recordings to the user in a list.

Each recording is represented by a separate row in the list with the following properties:

Recordings list columns	
Stream name:	Name of the input stream that was recorded.
Input:	Input source of the stream recorded. Currently only IPTV streams are supported.
Timestamp:	The timestamp of the start of the recording. If the recording was result of a trigger the timestamp refers to the instant the trigger was triggered. The recording will likely contain data from before this instant that was stored in the pre record buffer.
Reason:	The reason this recording was performed. • Manual recording: This recording was started manually from the user interface or Eii. • Scheduled recording: This recording was started at scheduled time. • Triggered recording: The recording was initiated as a response to a trigger event happening. The name of the event is inserted in the reason field. • Multiple: This recording was started because of one of the reasons above. Additionally, while the recording was in progress one or more of the events above occurred which caused the recording to be extended.
Notes:	First line of the operator supplied notes. Clicking on this column opens a popup where the complete notes can be viewed and edited.
Edit:	Clicking this will open a popup where the complete notes can be viewed and edited.
File size:	The size of the recorded transport stream file on disk.

Protect:	If this check box is checked the recording will not be automatically deleted when running out of disk space. Also deleting a recording from the user interface while the recording is protected may be impossible.
Duration:	The duration (in seconds) of the recording, from the time it is started (triggered, manually started or scheduled), to it is stopped. This duration does not contain the duration of the recording that originates from the pre-trigger buffer.
CC errs:	The number of CC errors for the specified recording. This number is calculated when the recording is finished, and the column is blank while the recording is active.
Download:	Link to the file containing the recorded stream data. To download partial recordings, use the **Record — Clips** view.
Metadata:	Link to a file containing metadata for the recording in JSON-format.

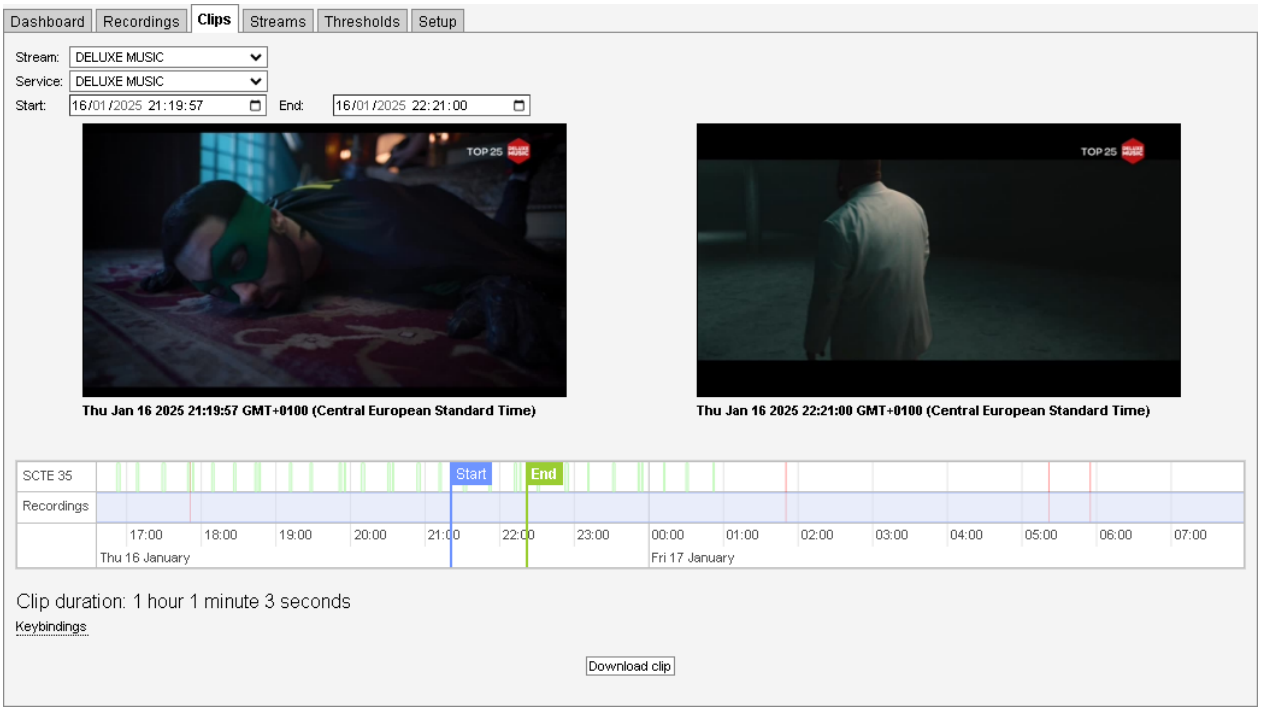
Selecting recordings in this list and clicking on the **Remove selected file(s)** button will delete the recordings from the probe's disk. The list of recordings supports bulk selection in an identical way to the **Record — Configuration** view, which may ease in deleting multiple recordings. Depending on whether or not deleting protected recordings is enabled in the **Record — Setup** view, protected recordings may or may not be deleted when included in the selection. Pressing the **Remove all recordings** button will either remove all unprotected recordings, of if configured as described above, all recordings. This deletion can take some time, and the disk space will be made available again after a couple of minutes.

For performance reasons the length of the past recordings list that is accessible to the web browser at a given time is limited to 500 recordings. The **Displaying x of y recordings** text at the bottom of the past **Record — Recordings** view shows how many recordings are visible, and available respectively. It is possible to use the filter fields in the top right corner of the view to filter by stream name and timestamp. When a date and time is entered in the time picker the recordings that happens before that time will be retrieved from the server. Any sorting done in the list will only take the data that is currently displayed into account. This means that if the user sorts by timestamp it will not see the oldest recording if it is not retrieved from the probe.

By default the list of past recordings are sorted by timestamp, showing the most recent recordings at the top. It is possible to click at the list headers to sort by other properties.

⏮Newest	Show the newest recordings
◀◀Newer	Change timestamp to show newer recordings
▶▶Older	Change timestamp to show older recordings
▶⏭Oldest	Show the oldest recordings

5.11.3 Record — Clips



The **Clips** view makes makes it possible to download selected parts of the recordings shown in the **Record — Recordings** view. This is especially useful when using the continuous recording feature, as the **Clips** view allows downloading clips that span several files.

To change which stream and service you are looking at, select the desired stream and service from the drop down at the top left. To navigate in time you have three options. You can use the date/time selectors at the top of the window, move the **Start** and **End** markers manually in the bottom timeline, or double click the **Recordings** line to move the active marker there. The active marker is colored green. To change which marker is active, press the Space bar.

You can zoom in and out of the timeline using the scroll wheel and drag the timeline left and right to find the location you need to access. It is also possible to navigate the timeline using the keyboard, hover the **Keybindings** label to see all available keyboard shortcuts.

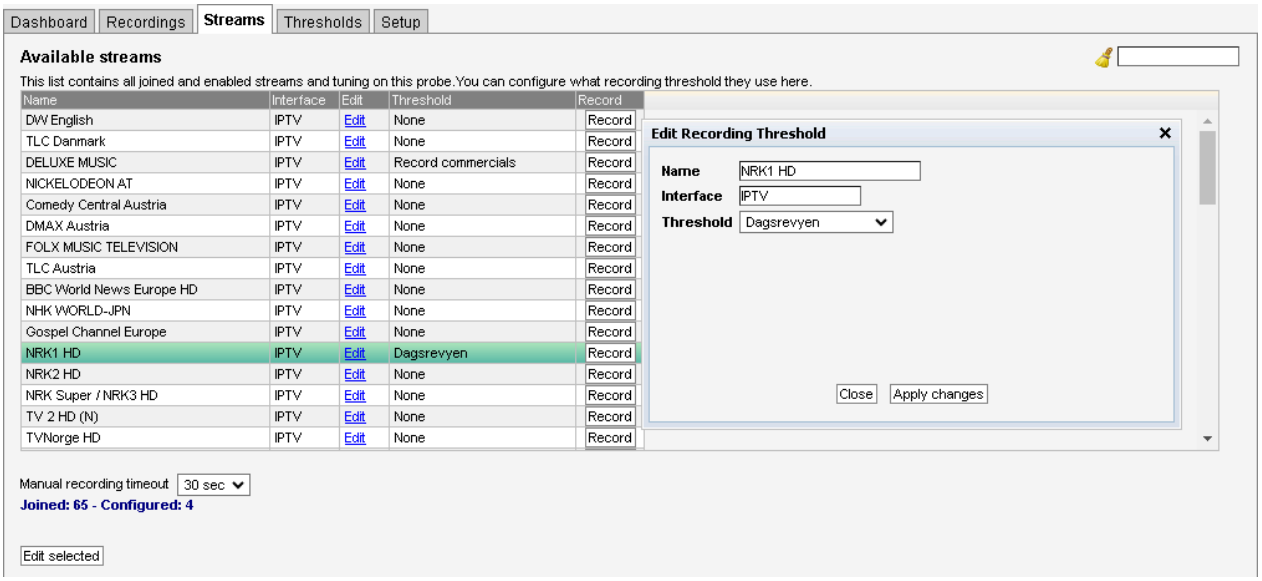
When selecting a time, the Clips feature will find the first key frame after this time. The frame shown on the left is the **Start** frame and will be the start of the export. The frame shown on the right is the **End** frame and is the first frame *not to be included* in the exported clip.

The **Clip duration** is automatically adjusted to display the selected time period. Be aware that selecting a long period of time can produce very large clip downloads.

If available, SCTE 35 events are displayed in the SCTE 35 event graph. If zoomed in, the event type is displayed, with more information available by hovering the event with the mouse pointer. Click the SCTE 35 event to snap the **Start** and **End** markers to download the selected event only.

CC error events are shown as red lines in the timeline; if a clip containing CC errors is selected, the total number of CC errors will be displayed adjacent to the Clip duration.

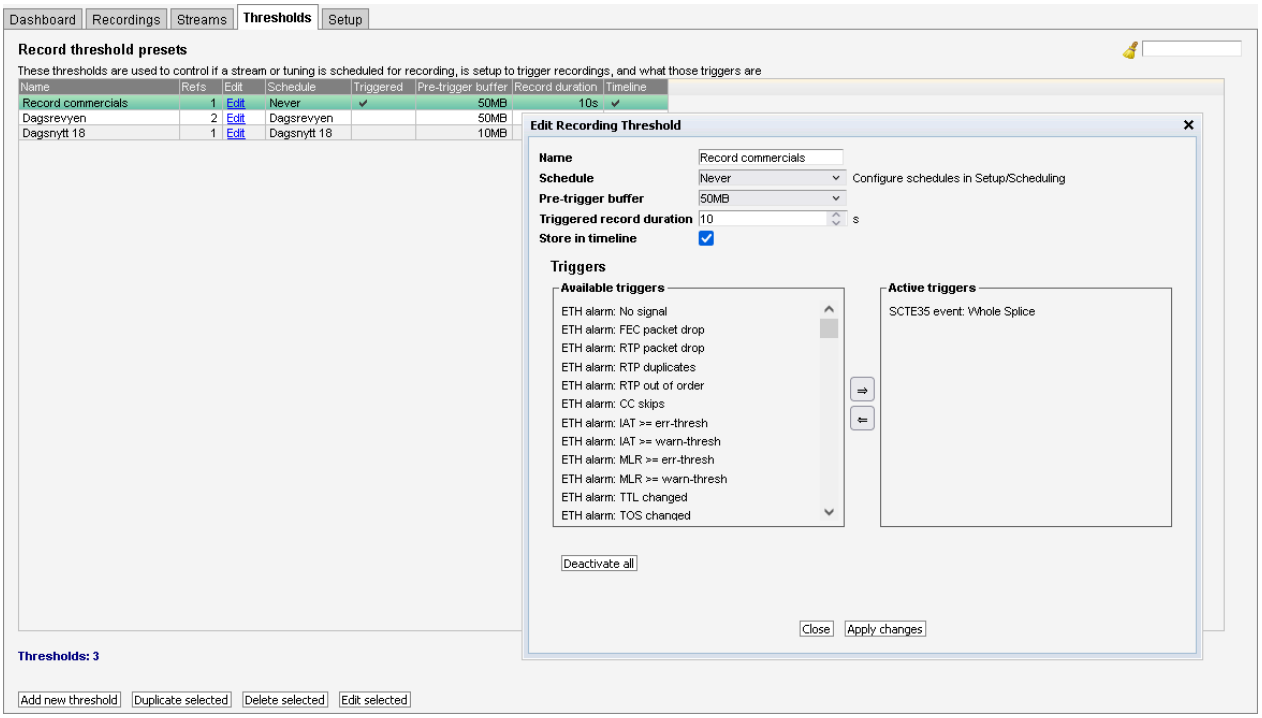
5.11.4 Record — Streams



The **Record — Streams** view allows the user to assign thresholds to streams. To assign a threshold, click the **Edit** link for a stream, or select one or more streams and click on the **Edit selected** button.

The list of streams in the **Record — Streams** view also presents the user with a **Record**-button which can be used to initiate a manual recording of the stream regardless of whether a threshold is assigned to it or not. The length of this manual recording is determined by the **Manual recording timeout** option below the list.

5.11.5 Record — Thresholds



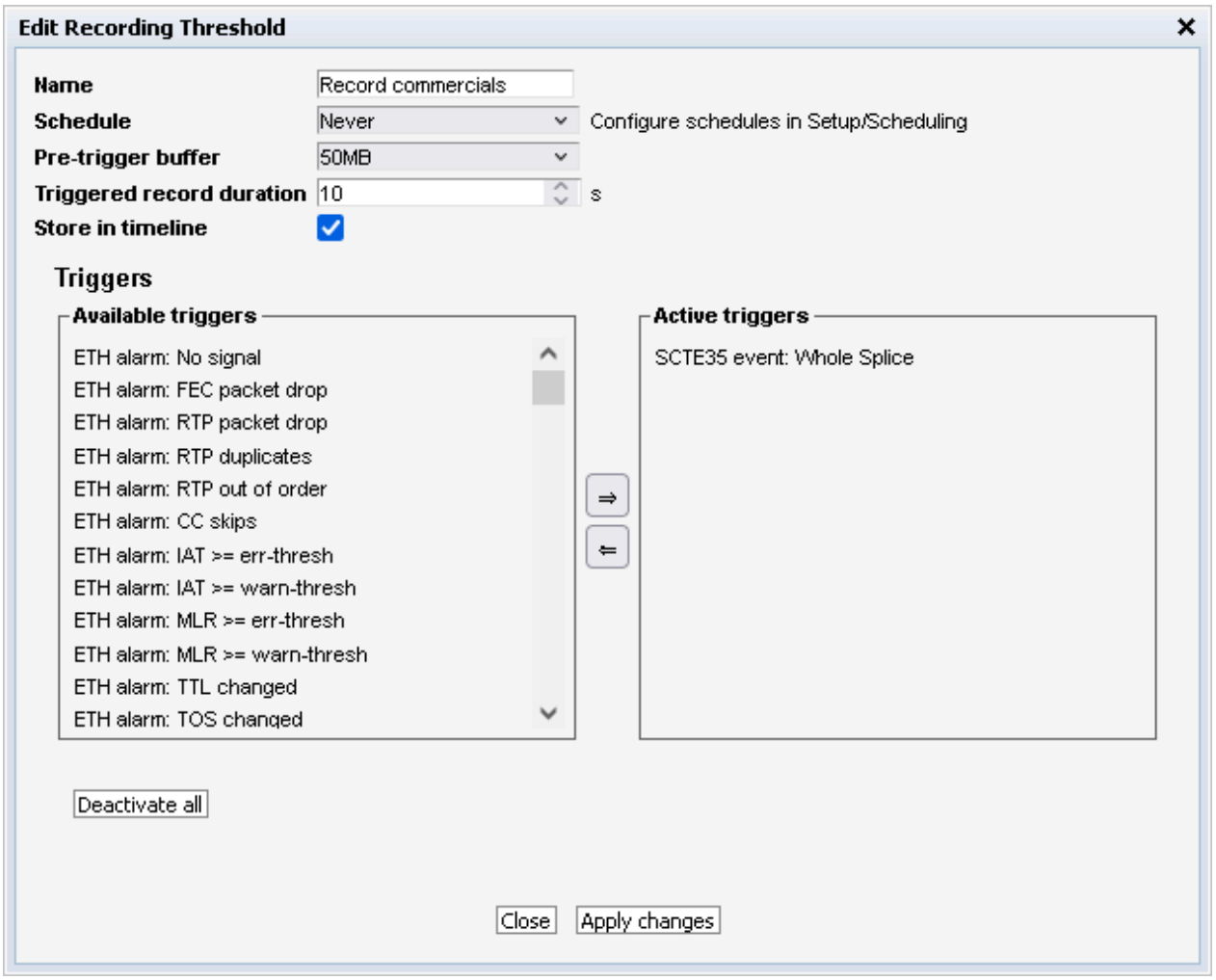
The multi-stream recording feature is configured by assigning thresholds to streams. Thresholds can be created, edited and removed in the in the **Record — Thresholds** view. The thresholds can then be assigned to streams in the **Record — Streams** view.

Thresholds are sets of settings that, once applied to a stream, instructs the probe on how and when to record that stream. The **Record — Thresholds** view displays a list of currently existing thresholds. Adding, deleting and editing existing thresholds can be performed from by clicking the appropriate buttons.

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 recording 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 selected** 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.

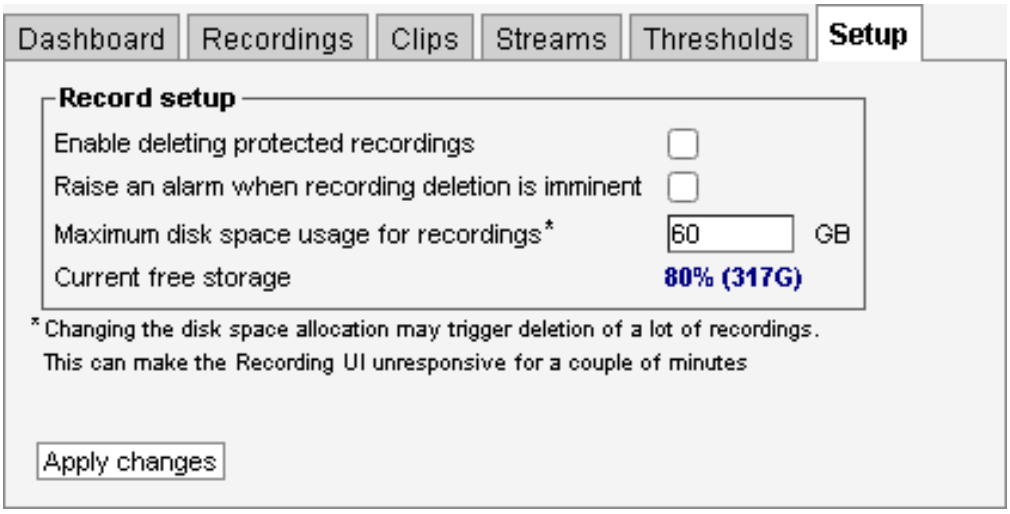
In the threshold presets list the 'Refs' column displays how many streams are associated with each stream threshold template.



Threshold settings	
Name:	The name that identifies this threshold
Schedule:	If set to a value other than **Never**, the streams this threshold is assigned to will be recorded according to the given schedule. By using the special schedule **Always**, a stream can be configured for continuous recording. Such a stream will be recorded in chunks of one clock hour each, which can be managed using the **Record — Clips** view. Schedules can be created or modified in the **Setup — Scheduling** view. These schedules are shared with the alarm functionality.

Pre-trigger buffer:	The size of the pre-trigger buffer (in Megabytes). Each stream assigned to this threshold will buffer the selected amount of data, which will become the start of the recording when the trigger occurs. A sensible amount should be selected with regards to the streams bitrate to ensure the triggering event is located inside the buffer. This setting is ignored for scheduled recordings.
Triggered record duration:	The duration (in seconds) to record for after a trigger has occurred. This setting is ignored for scheduled recordings.
Store in timeline:	If enabled, a link to the recordings are stored for display in the **Content — Timeline** view. Note that this link will only be valid as long as the recording is stored, and the Timeline will stop displaying it after it has been deleted from disk.
Triggers:	If the recording should be triggered by an alarm or stream event, the operator must add the appropriate trigger(s) to the **Active triggers** list. This is done by selecting the triggers from the list of **Available triggers**, followed by pressing the button with the arrow pointing to the right. To remove triggers from the threshold, the reverse applies, in that one should select the trigger from the **Active triggers** list and followed by pressing the arrow pointing to the left. All triggers can also be removed by pressing the **Deactivate all** button. When triggering on an alarm, that alarm must be activated for the corresponding stream in its thresholds configuration. Similarly, when triggering on an SCTE 35 event, SCTE 35 extraction must be configured in the associated content thresholds.

5.11.6 Record — Setup



The **Record — Setup** view presents recording related settings.

Record setup	
Enable deleting protected recordings:	If this checkbox is unchecked protected recordings cannot be deleted while they are protected from the user interface. This is especially useful for bulk editing, where selecting and deleting all recordings in a view may be desirable, but still without deleting protected recordings.
Raise an alarm when recording deletion is imminent:	If this checkbox is checked, an alarm will be raised when the usable disk space for recordings is nearing 0, meaning that deletion of the oldest recordings is imminent.
Maximum disk space usage for recordings:	This setting lets the user specify how many gigabytes of disk can be used for recordings. The record feature will start removing (non protected) recordings when this much disk space is used by recordings, or if the disk gets full because of other files being stored on the same partition. When the useable disk space drops below 1% of this setting, the probe will raise a warning to indicate that non protected recordings will soon start to be deleted. If the usable disk space drops to zero, no new recordings will be allowed to start.
Current free storage:	This shows the currently available free space on the file system holding the recordings.

5.11.7 Automatic deletion of recordings

In order to avoid running out of disk space the probe will delete the oldest unprotected recordings when the usable disk space for recordings drops to zero, this can be caused either by the free space on the partition having become low, or if the size of the recordings stored has reached the threshold. The threshold for deleting recordings is configurable from the **Record — Setup** view.

If for some reason the amount of usable disk space gets too low recording will eventually stop before the recordings filesystem is filled completely.

5.12 Redundancy (requires IP-SWITCH-OPT)

The IP redundancy switching feature enables the VB330-SW to function as a control unit for an external redundancy switching device. The VB330-SW integrates easily by specifying a few parameters. Then the VB330-SW can be configured to send switching commands based on the alarm settings. The actual distribution and switching will be done by the external device. IP redundancy switching is currently supported on the DMG 4000.

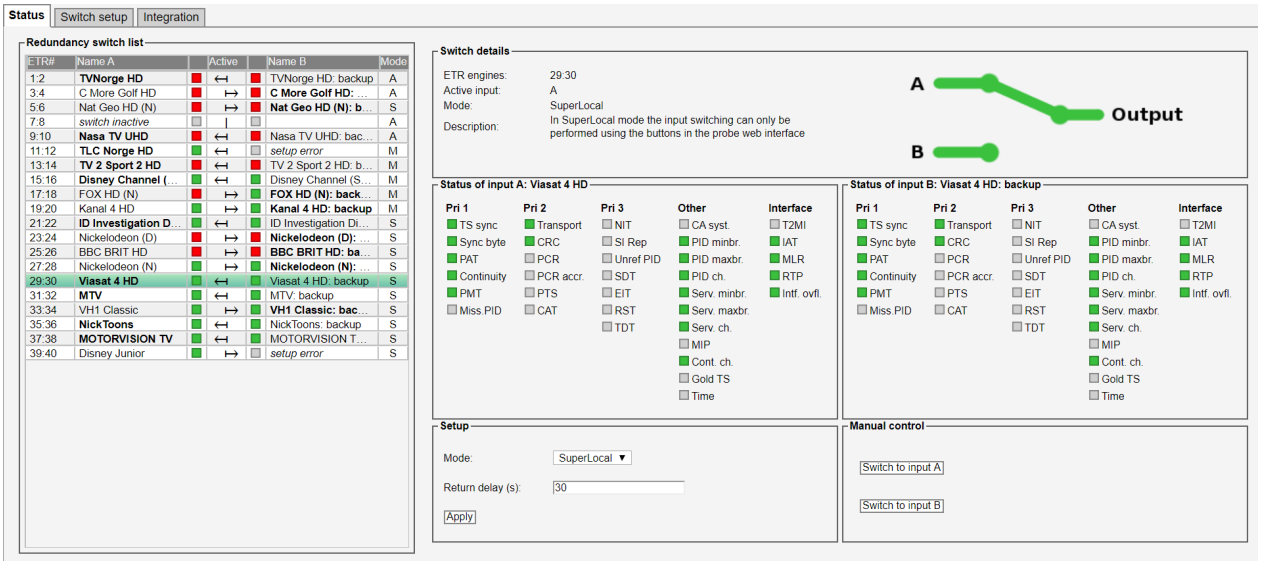
Each redundancy switch is coupled with two specific ETR engines. The pairs are 1 and 2, 3 and 4 etc. The number of ETR engines depends on the ETR290-OPT of the VB330-SW. More information about the ETR290-OPT is found in section 5.9. The number of switches available will adjust automatically to the number of ETR engines.

The multicasts must be assigned to the ETR engines using the **Multicasts — Streams** view. A step by step description of how to do this can be found in section 5.12.5.

A single multicast must be monitored per engine for the switching to work as intended. Round-robin monitoring (multiple multicasts monitored sequentially on the same ETR engine) is NOT supported for redundancy switching.

The redundancy switch status and settings are available using the Eii. Setup changes through the Eii is also possible. See section 5.14.5 for more information about the Eii.

5.12.1 Redundancy — Status



The **Status** view displays the status of the redundancy switches. The Redundancy switch list on the left side gives an overview of all the switches.

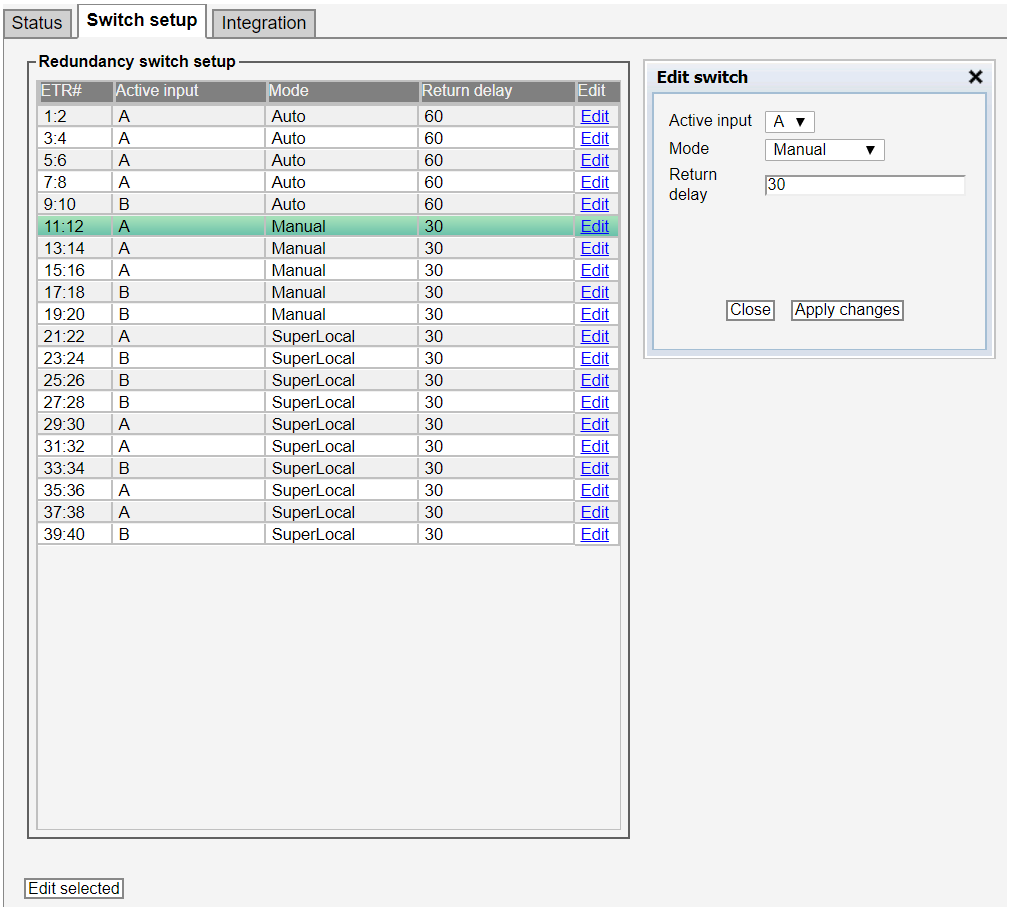
Redundancy switch list	
ETR#:	The ETR engines coupled with the switch. <input A>:<input B>
Name A:	Displays the name of the stream on input A (odd numbered ETR engine). To the right of the name is a bulb showing the ETR290 alarm status. The field also provides the following information: • **Bold** text indicates that the stream is the currently selected as the output. • Displaying *"switch inactive"* together with an empty Name B field means that one or both of the ETR engines are not in use. • *"setup error"* is displayed if there is a setup error. Opening the respective switch information will give more details.
Active:	The arrow indicates which input is currently selected as the output.
Name B:	Displays the name of the stream on input B (even numbered ETR engine). To the left of the name is a bulb showing the ETR290 alarm status. The field also provides the following information: • **Bold** text indicates that the stream is the currently selected as the output. • An empty field together with Name A displaying *"switch inactive"* means that one or both of the ETR engines are not in use. • *"setup error"* is displayed if there is a setup error. Opening the respective switch information will give more details.
Mode:	The operation mode, described in section 5.12.4, set for the switch A = Auto, M = Manual, S = SuperLocal

To the right of the Redundancy switch list, more detailed information about a switch is displayed. This is information about the redundancy switch currently selected in the switch list. A switch can be selected by clicking the respective list entry. The following information is displayed:

Switch information frames	
Switch details:	**ETR engines**: The ETR engines coupled with the switch. <input A>:<input B> **Active input**: The input selected to be output from the switch. **Mode**: The operation mode, described in section 5.12.4, set for the switch **Description**: A description of the switch's current operation. After a switch, the return delay countdown will be shown here. The switch details frame includes a figure with a visual representation of the switch's status.
Status of input A:	The header text is followed by the name of the stream. The frame shows the full ETR290 alarm status of the stream on input A of the selected switch. The content of this frame is described in section 5.9.2.
Status of input B:	This shows the same information as **Status for input A**, but for input B.

Setup:	Allows for quick access to the currently selected switch's setup. The setup parameters are described in section 5.12.2.
Manual control:	Buttons in this frame are used to select which input should be the output from the switch. These are only available in modes Manual and SuperLocal.

5.12.2 Redundancy — Switch setup

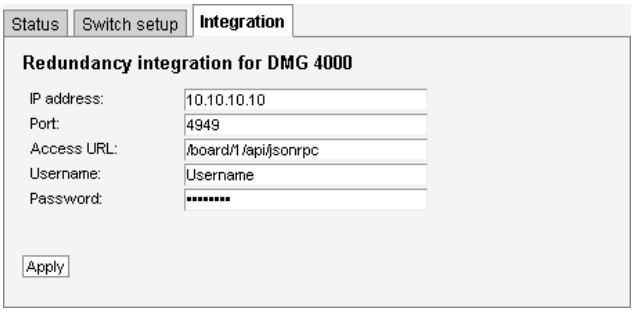


The **Switch setup** view shows the current setup of all the switches. Using this view is the most effective way to edit the setups of the redundancy switches. Multi-edit functionality makes it possible to edit several setups simultaneously. Highlight the setup list entries that should be edited and click the **Edit selected** button. The link in the Edit column can be used to edit the setup on that specific row.

Any setting can be set from the setup page regardless of current mode etc. The probe does not have a way to read the status from the external device. The **Setup** view can be used to manually sync the VB330-SW probe's switch settings to the settings of the external device.

Switch setup list	
ETR#:	The ETR engines coupled with the switch. <input A>:<input B>
Active input:	The input selected to be the output from the switch.
Mode:	The operation mode, described in section 5.12.4, set for the switch.
Return delay:	The return delay specifies a time period following an automatic switch where a new switch cannot be triggered. This only applies if the **Mode** is set to Auto.
Edit:	Click this column to edit the switch's setup parameters.

5.12.3 Redundancy — Integration



The **Integration** view is used to set the parameters needed to integrate with the external switching device. IP redundancy switching is currently supported on the DMG 4000. The following parameters are supported:

Integration parameters	
IP address:	IP address used to reach the external switching device.
Port:	Port used to connect to the external device.
Access URL:	Path to control API.
Username:	Username used to authenticate against the external device.
Password:	Password used to authenticate against the external device.

5.12.4 Redundancy switch operation modes

The redundancy switches have three different modes of operation: Auto, Manual and SuperLocal. The mode can be set for each switch independently. The modes are described below:

Modes

Auto:	Switching between the inputs is done automatically based on the user defined alarm setup. A switch is triggered when the active stream has an active alarm while the inactive stream is alarm free. The return delay specifies a period of time following an automatic switch where a new automatic switch cannot be triggered.
Manual:	An action from the user is required to switch. The switching can be performed using the Manual control buttons in **Redundancy — Status**, editing the setup in **Redundancy — Switch setup** or through the Eii.
SuperLocal:	The redundancy switches can only be controlled through the web GUI. Control through Eii is disabled. Use this mode to disable externally triggered switches.

5.12.5 Setup guide

Coupling multicasts to a redundancy switch

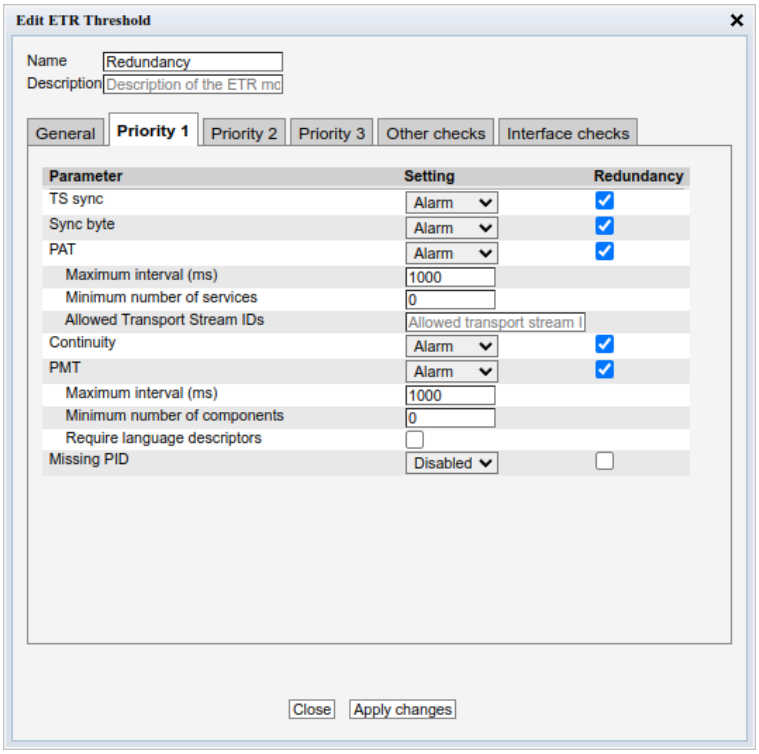
As mentioned at the start of the Redundancy section, each switch is coupled with a specific pair of ETR engines. The number of the ETR engines coupled with a switch are two consecutive numbers starting with the odd number (i.e. 1 and 2, 3 and 4, ...).

The multicasts are assigned to ETR engines using the **Multicasts — Streams** view. Figures and a full description of this view can be found in section 5.4.8.

1. Go to the **Multicasts — Streams** view.
2. Open the edit popup of the multicast you want to couple with a redundancy switch.
3. Join the multicast:
   Under **General**, check **Join stream**.
4. Enable ETR monitoring:
   Under **ETR**, check **Enable ETR**.
5. Assign the multicast to the ETR engine of the switch you want it to be coupled with:
   Under **ETR**, set **Selected ETR engine** to the number of the ETR engine. Only a single multicast can been assigned to ETR engines used for redundancy switching.
6. If the switch will use the Auto mode, set the ETR thresholds:
   Under **ETR**, select the ETR thresholds using the **ETR thresholds** drop-down. How to set up the ETR thresholds for redundancy switching is described in the next section (ETR thresholds for automatic switching).
7. The multicasts will be listed in the **Redundancy — Status** view's Redundancy switch list. If the name of the multicast is not in the list, make sure that the options mentioned in points 3–5 are set correctly. Redundancy switch list error texts are described in chapter 5.12.1.

ETR thresholds for automatic switching

Switches that operate in Auto mode will switch automatically based on the ETR alarm state of the input streams. The ETR thresholds are used to configure which alarms that will be reported, and the limits (i.e. thresholds) for when they will be triggered. A detailed description of the ETR thresholds is given in section 5.9.11. When the IP-SWITCH-OPT is installed, the ETR thresholds will also have a redundancy checkbox for each alarm. The ETR thresholds edit popup with redundancy can be seen below.



An automatic switch can be triggered by an alarm when the alarm is enabled and has the Redundancy checkbox checked in the ETR threshold. If an alarm should be reported, but not trigger a switch, it should then be enabled with the drop-down menu and not have the Redundancy checkbox checked.

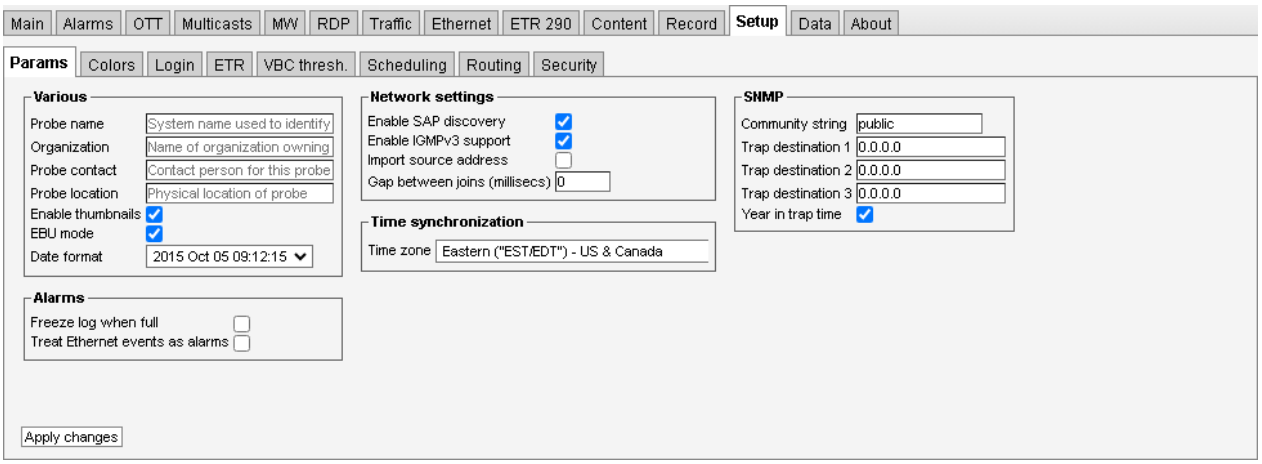
Setting up ETR thresholds:

1. Go to the **ETR 290 — ETR thr.** view.
2. Create a new threshold or open an existing one for editing.
   This will open the pop-up seen above.
3. Enable the alarms that should be reported for the stream:
   Select **Alarm** in the **Setting** column of the alarms.
4. Allow automatic switching on alarms:
   Check the checkbox in the **Redundancy** column of the alarms.

5. To assign the ETR thresholds to multicasts, follow the steps describing how to couple multicasts to redundancy switches in the previous section.

5.13 Setup

5.13.1 Setup — Params



The **Setup — Params** view is used to configure basic parameters for the 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 activating the license on-line, see G Appendix: On-line License Activation 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 activating 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 activating the license on-line.

Enable thumbnails:	Enable or disable thumbnail generation globally. When enabled, thumbnails are only decoded automatically if the **Extract thumbnails** option has been enabled in the associated OTT or multicast setup. If freeze-frame or color-freeze alarming has been enabled in the Content threshold template, the video frames are investigated regardless of this setting. 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.
EBU mode:	Selects the unit to use for loudness monitoring. In EBU mode, LUFS is used, otherwise LKFS is used.
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.

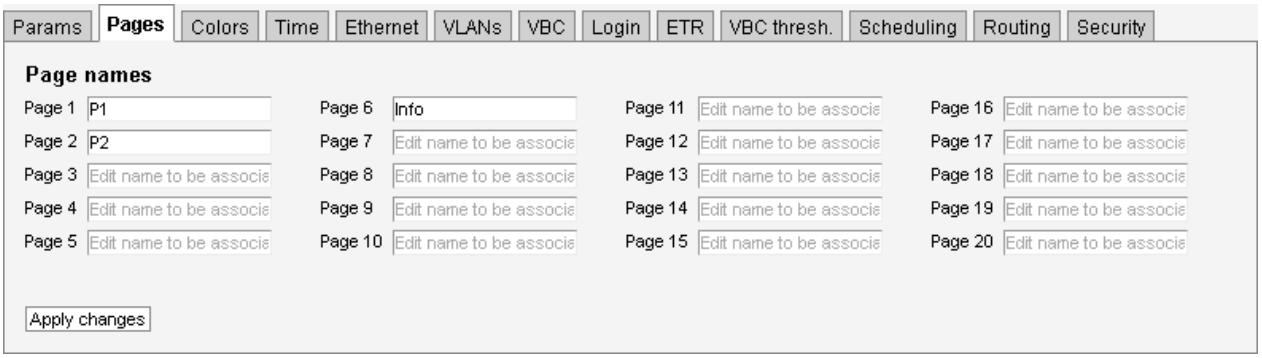
Alarms	
Freeze log when full:	When enabled the alarm list will freeze when full (an event will show that it is full). When the list is full new alarms are ignored until **Clear alarms** is pressed. This can sometimes be useful if a unit is placed unattended.
Treat Ethernet events as alarms:	When enabled each event is treated as an alarm that is active for ten 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 Software Probe makes streams announced using the Session Announcement Protocol available through the **Multicasts — SAP** view.
Enable IGMPv3 support:	Required for probe to support the IGMP v3 protocol. Should always be enabled in networks that support IGMP v3.
Import source address:	When enabled, the detected source address is added to the configuration when importing streams from **Traffic — Detect** or **Traffic — Multicast scan**. This instructs the probe to request the stream as a source specific multicast.
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 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 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 all three destinations to 0.0.0.0 to disable SNMP trap transmission. This will also disable storing of traps accessible through SNMP queries.
Year in trap time:	If enabled, dates in SNMP traps include the year number.

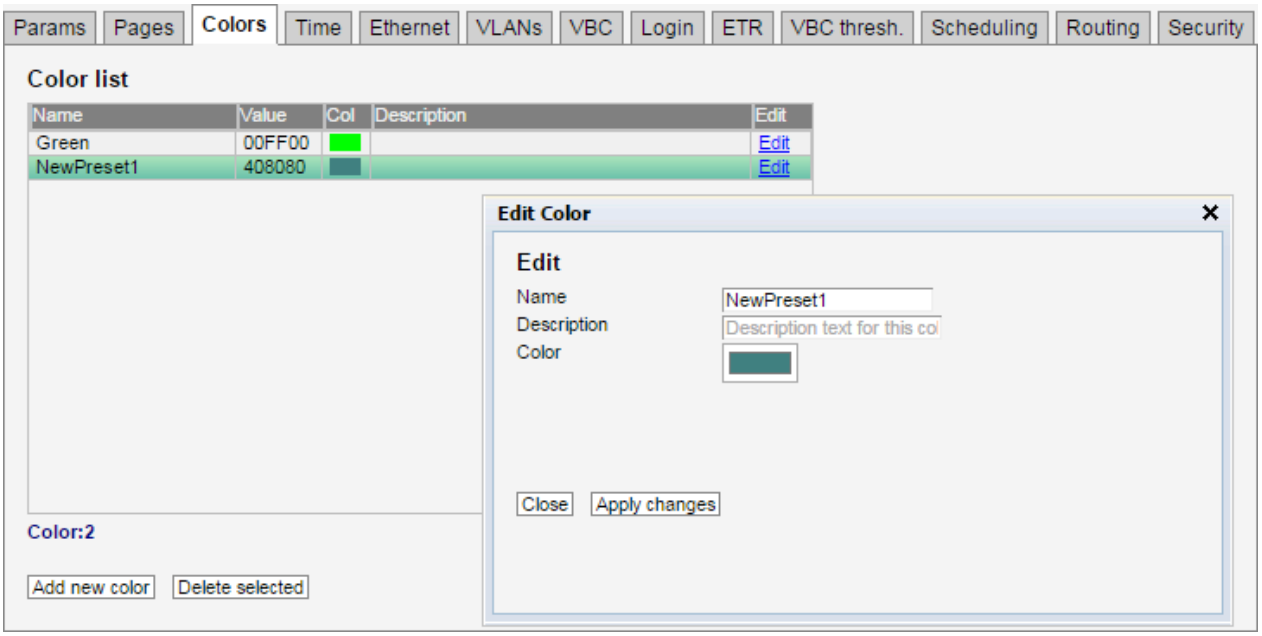
5.13.2 Setup — Pages



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.

The page names for OTT channels are configured using the **OTT — Settings** view.

5.13.3 Setup — Colors

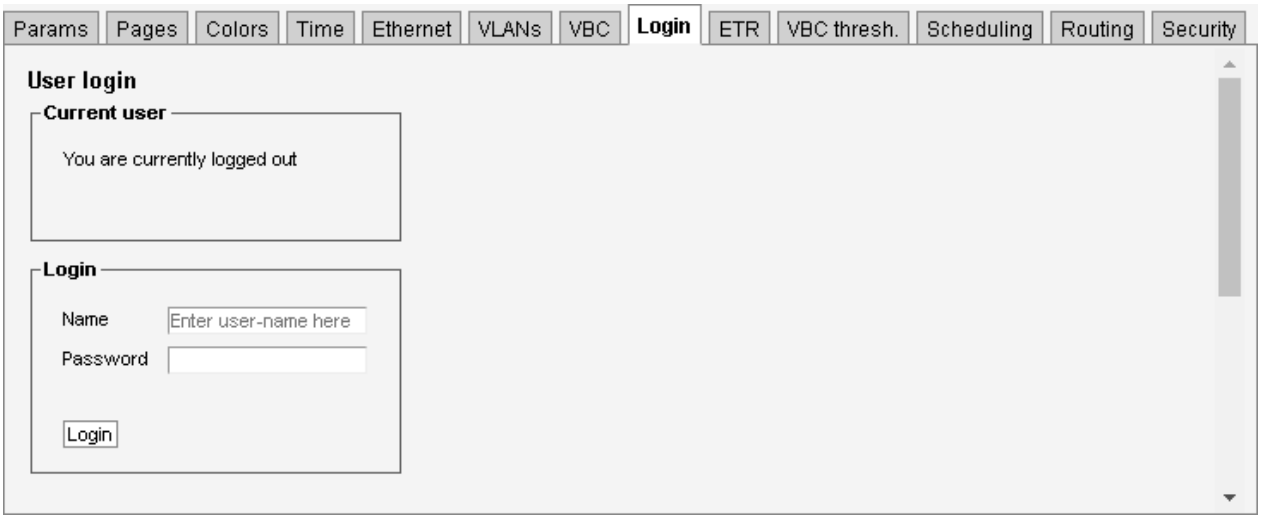


The **Setup — Colors** view allows the user to define colors that should be recognized if a color-freeze condition should occur. A mono-colored freeze frame condition may in some cases indicate what equipment is failing, resulting in the color-freeze.

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.

5.13.4 Setup — Login



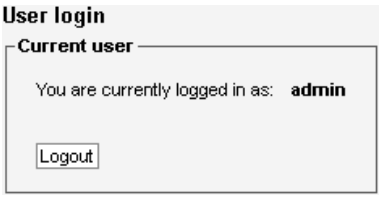
By default, there is no access control and all users have access to all features. When access control is activated, anyone with access to the VB330-SW will first be presented with the login view, requiring the user to log in before being able to access the user interface.

Only the **admin** user can change the access control settings. If access control is disabled, you need to log in using this view before accessing any of the settings in **Setup — Security**.

To restrict access, the **Setup — Security — Authentication** view can be used to set up log-in that restricts all access to the user interface.

Use system firewall to allow or deny certain addresses, please refer to the operating system instructions[4] for more details.

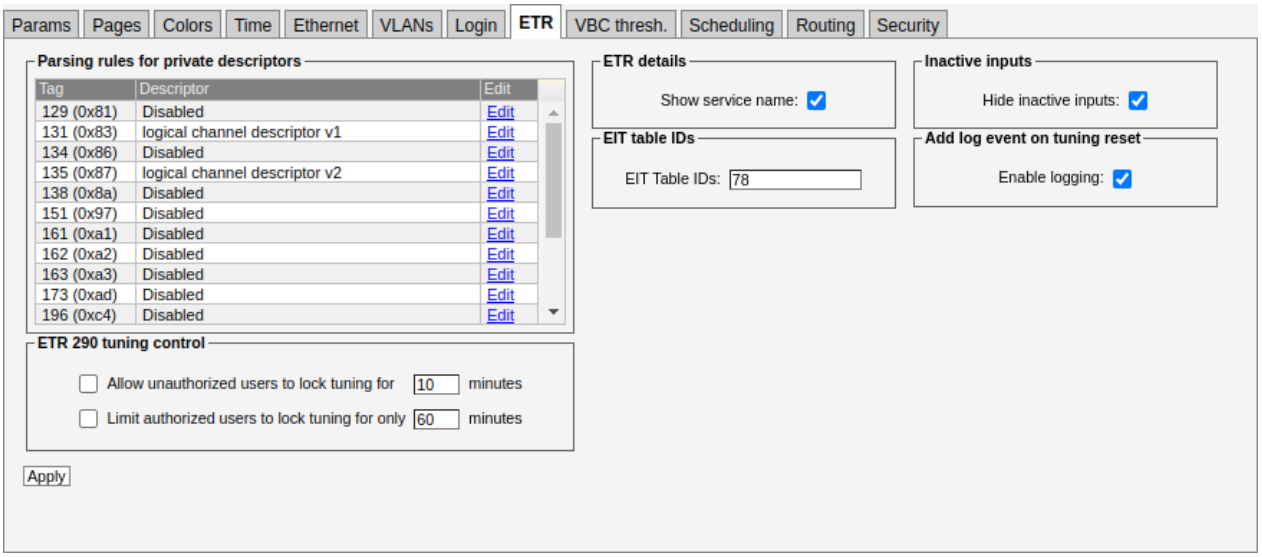
[4] https://ubuntu.com/server/docs/how-to



Log-in is performed by providing the correct username and password. The default user name and password to is **admin** and **elvis**. The operator may define a new password that should be easy to remember. The password for the "admin" user is configured in the **Setup — Security — Password** view.

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

5.13.5 Setup — ETR



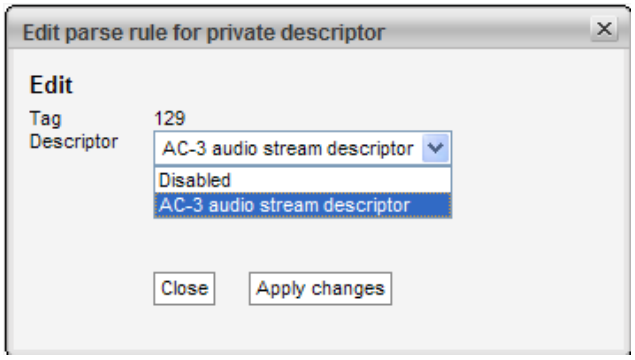
The **Setup — ETR** view allows the user to select miscellaneous ETR handling modes.

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', 'Extended video descriptor' or 'logical channel descriptor v1'
134 (0x86):	'Disabled' or 'caption service descriptor'
135 (0x87):	'Disabled', 'logical channel descriptor v2' or 'content advisory descriptor'
138 (0x8a):	'Disabled' or 'cue identifier descriptor'
151 (0x97):	'Disabled' or 'SCTE_adaptation_field_data_descriptor'

161 (0xa1):	'Disabled', 'service location descriptor' or 'etv_bif_platform_descriptor'
162 (0xa2):	'Disabled' or 'etv_integrated_signaling_descriptor'
163 (0xa3):	'Disabled' or 'Component name descriptor'
173 (0xad):	'Disabled' or 'ATSC private information descriptor'
196 (0xc4):	'Disabled' or 'Anc data descriptor'
201 (0xc9):	'Disabled' or 'download_content_descriptor'
206 (0xce):	'Disabled' or 'extended_broadcaster_descriptor'
215 (0xd7):	'Disabled' or 'SI_parameter_descriptor'
231 (0xe7):	'Disabled' or 'private cable delivery system descriptor'
233 (0xe9):	'Disabled' or 'EBP descriptor'
239 (0xef):	'Disabled' or 'evertz_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** sub-views. 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.

Add log event on tuning reset

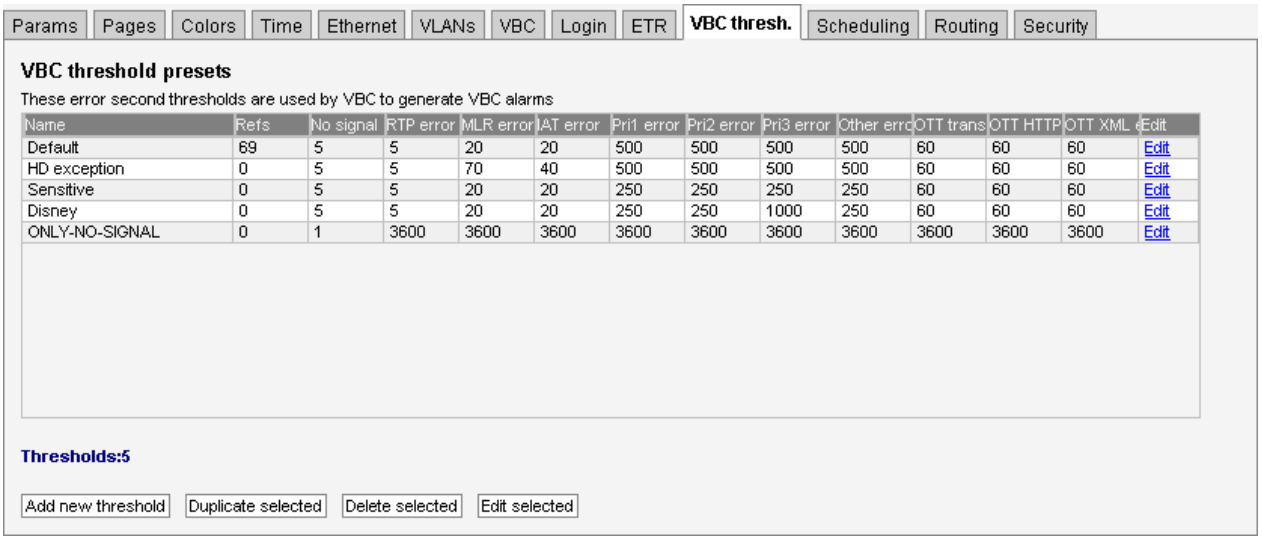
When the **Enable logging** checkbox is enabled, the probe will log events that cause monitoring of a ETR monitored stream to be reset, or when ETR measurements are cleared:

- Tuning reset from the GUI
- Min/max measurements for a stream reset from the GUI
- Min/max measurements for a specific measurement for a stream reset from the GUI
- Tuning reset from the Eii interface
- Min/max measurements for a stream reset from the Eii interface

- Min/max measurements for a specific measurement for a stream reset from the Eii interface
- Monitoring of a stream was restarted due to a configuration change (templates changed etc.)
- Monitoring of the stream was started due to round robin tuning between frequencies or multicasts

The events logged are shown in the **Alarms — Event log** view.

5.13.6 Setup — VBC thresh.



The VBC error second thresholds are used by the VideoBRIDGE 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 VideoBRIDGE 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.

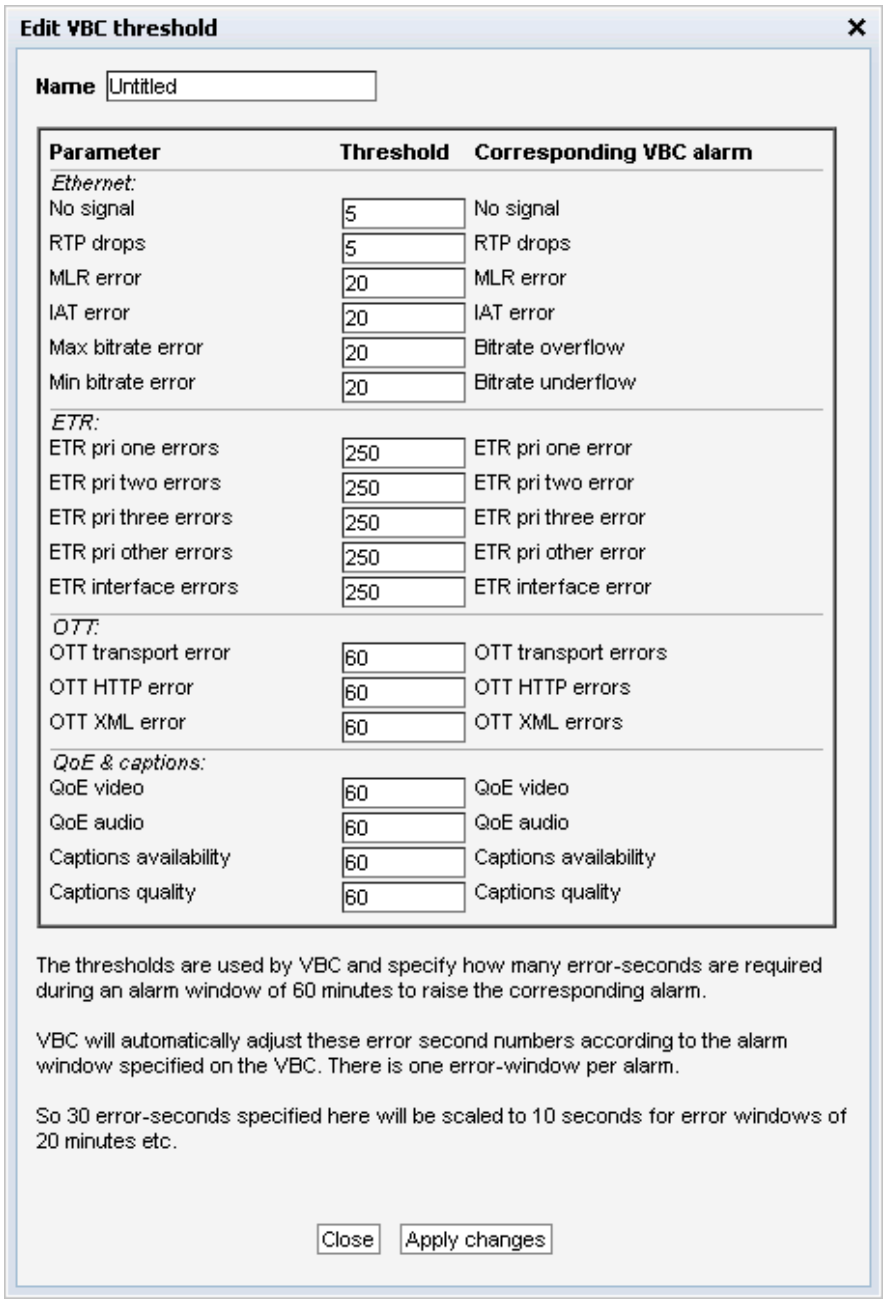
The VBC error second thresholds are specified as the number of seconds affected by an error situation. These thresholds refer to a monitoring window of one hour, meaning that if the number of error seconds summed over any one-hour period exceeds the associated error second threshold an alarm will be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

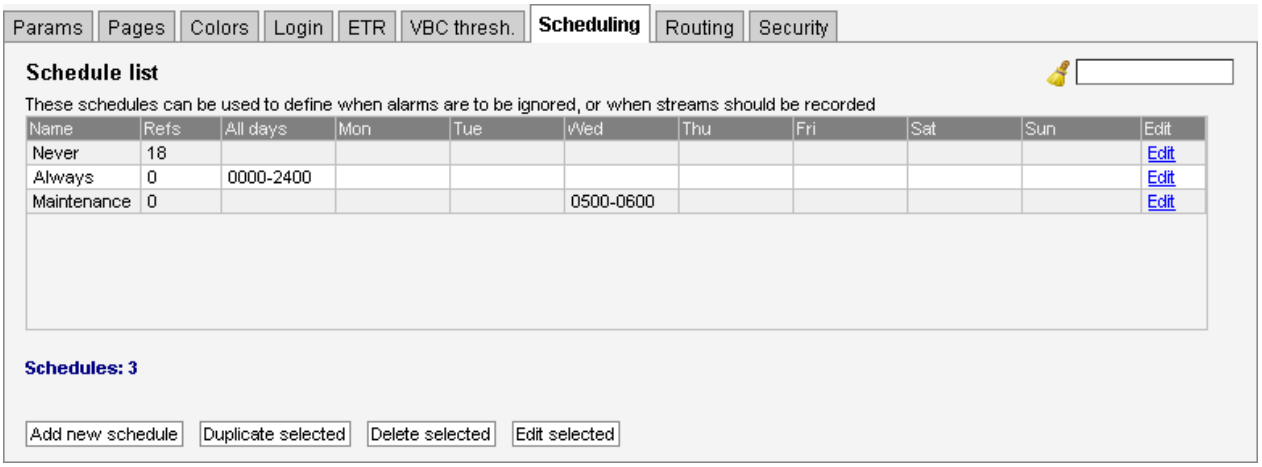
By clicking the **Add new threshold** button the user will enter a VBC thresholds edit view enabling definition of a new threshold template. It is possible to copy or delete an existing threshold template by clicking the **Duplicate selected** or **Delete selected** button respectively. To edit a highlighted 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 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
QoE video:	Number of seconds with QoE video-related alarms, such as freeze-frame and MOS below average
QoE audio:	Number of seconds with QoE audio-related alarms, such as audio silence or out of phase
SCTE 35:	Number of seconds with SCTE 35-related alarms, such as event gap or number of placement opportunities
EBP / IDR:	Number of seconds with EBP/IDR-related alarms, such as EBP PTS gap outside of threshold or EBP and IDR PTS unaligned
Captions availability:	Number of seconds with captions availability alarms
Captions quality:	Number of seconds with captions quality alarms

5.13.7 Setup — Scheduling



The **Setup — Scheduling** view enables definition of schedules. These schedules can be used to mask alarms during selected time intervals, e.g. due to maintenance. To mask ETR 290 alarms, schedules can be assigned to a PID threshold or service threshold. To mask content alarms, schedules can be assigned to a multicast or OTT channel, or to a specific service using a content service threshold.

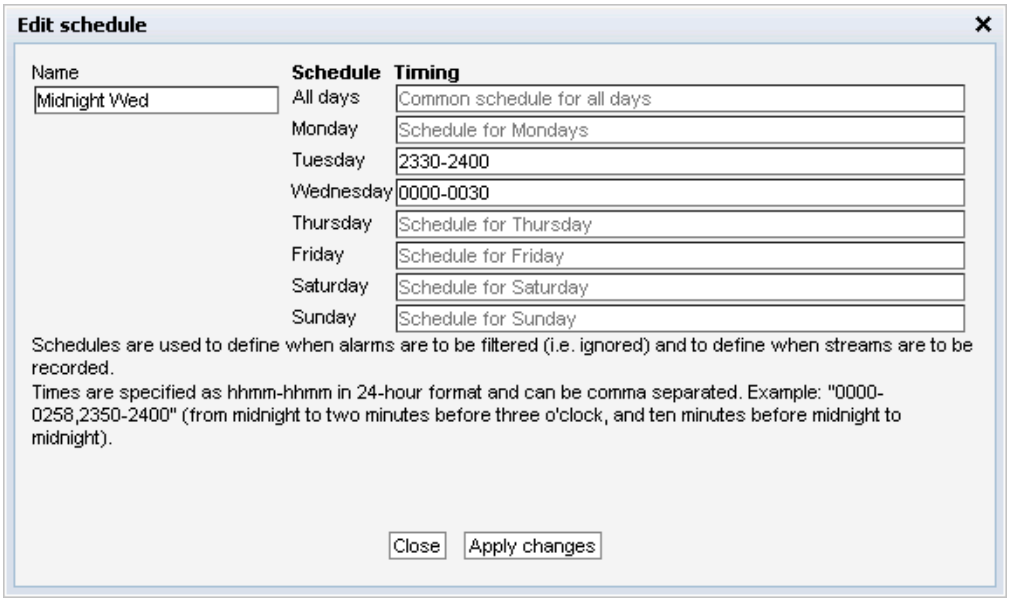
Schedules can also be used in recording templates, where they define the times during which the selected service should be recorded.

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 the places mentioned above.

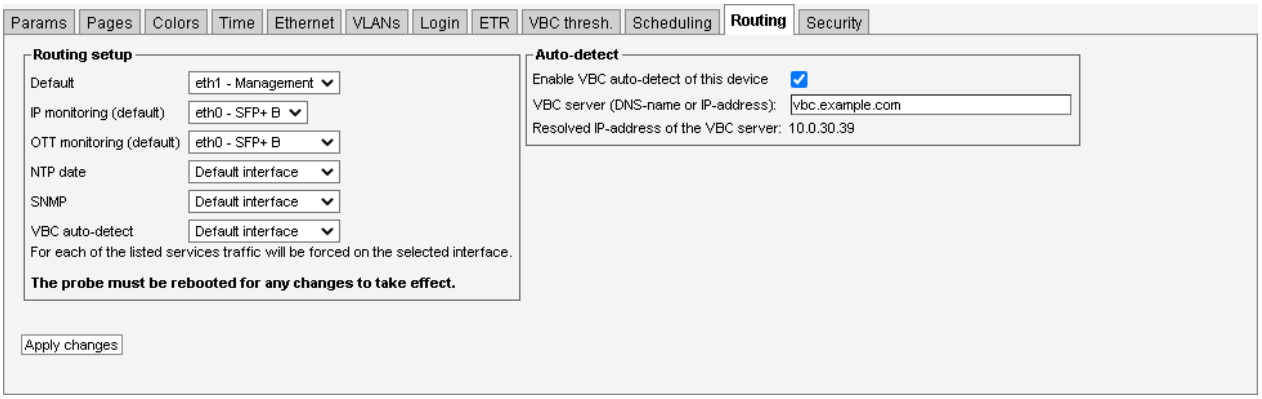
The search field in the upper right corner of the view allows the user to type a text string and the schedule list is updated to display only scheduling templates matching the specified text.

The predefined scheduling templates **Never** and **Always** result in alarms being masked never or always, respectively. When used for recording, the **Never** template disables all time-based recording. The **Always** template cannot be assigned to recording thresholds. 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 the schedule starts 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 **Record — Thresholds — Edit**, **Multicasts — Streams — Edit — Content**, **OTT — Channels — Edit**, **ETR 290 — PID thresh. — Edit**, **ETR 290 — Service thresh. — Edit** and **Content — Service thresh. — Edit** views.



5.13.8 Setup — Routing



The **Setup — Routing** view allows configuring the default interface for out-going probe traffic, the default monitoring interface and VBC detection. System networking configuration is configured using the system network configuration, please refer to D **Appendix: Network configuration** for details.

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 VideoBRIDGE Controller can automatically detect the 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 Software Probes for auto-detection to work.

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

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 **Auto-detect** column.

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

Auto-detect	
Enable VBC auto-detect of this device	Check this box to enable auto-detect
VBC server	Enter the host name name or IP address of the VBC
Resolved IP address	The IP address associated with the DNS name will be displayed here. If host name lookup fails, it is necessary to type the VBC server's IP address instead. Host name lookup is only performed if auto-detect is enabled.

5.13.9 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 Software Probe.

To access this view, you have to be logged in. If probe access control has been disabled, you will need to visit **Setup — Login** first. The default user name and password to enter this view is **admin** and **elvis**. The password is changed in the **Setup — Security — Password** sub-view.

To change the parameters in this view, you need to access the VB330-SW user interface directly, they are not available when logged in through the VBC.

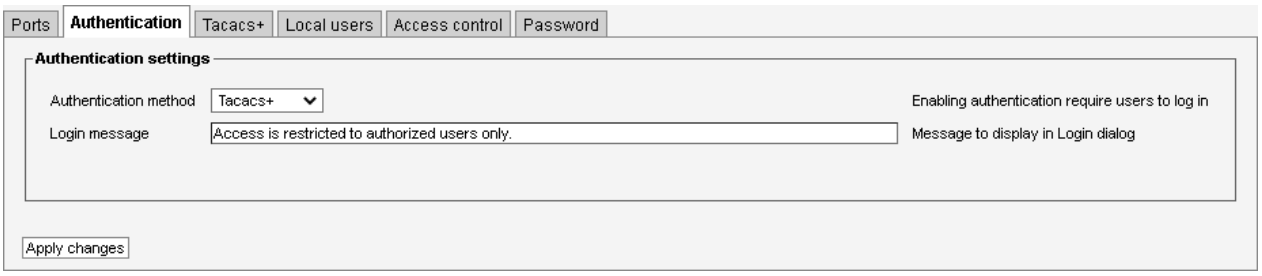
5.13.9.1 Setup — Security — Ports

The **Setup – Security — Ports** view makes it possible to enable and disable a number of protocol ports used by the VB330-SW. 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**.

License activation proxy	
Proxy URL	When using on-line activation, the Software Probe needs to be able to connect to the license activation server. If the 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 Software Probe will try to use the proxy installed on the VBC host, as configured in the **Setup — Routing** view; see G Appendix: On-line License Activation for more details

5.13.9.2 Setup — Security — Authentication



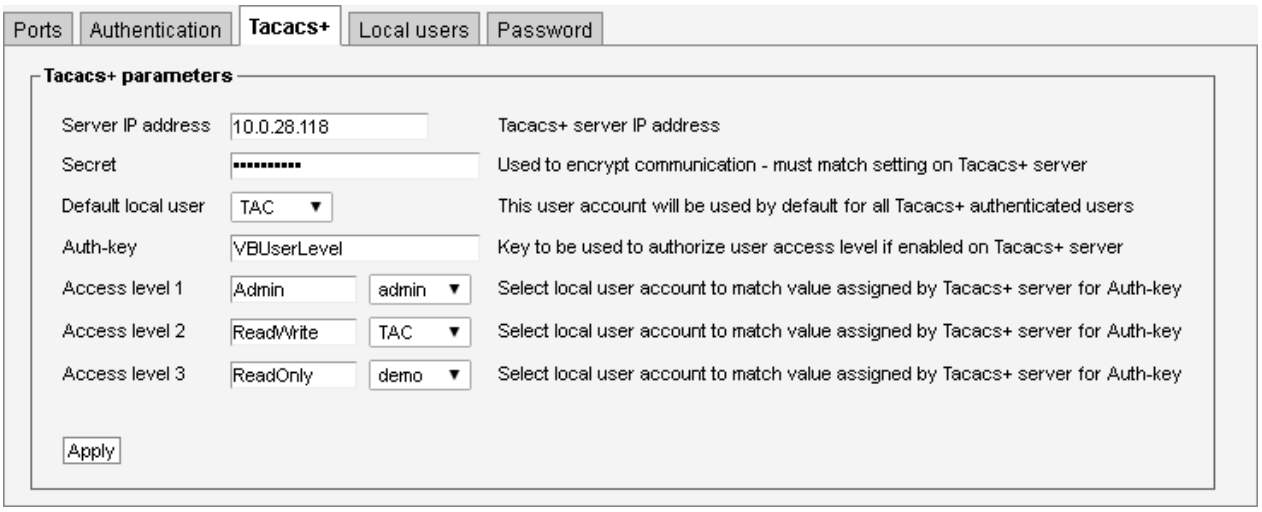
The **Setup — Security — Authentication** view makes it possible to restrict access to the VB330-SW user interface by requiring the user to log in first.

Authentication method	
Disabled	VB330-SW authentication is disabled, and no login is required when accessing the VB330-SW from a web browser. The Software Probe is seamlessly accessible from the VideoBRIDGE Controller. This is the default setting.
Tacacs+	VB330-SW authentication is enabled. When accessing the VB330-SW with a web browser, users needs to authenticate themselves with a username and password. These need to match the pre-defined **admin** user, a user available on the Tacacs+ server configured through the **Setup — Security — Tacacs+** view, or any of the users configured in the **Setup — Security — Local users** view.
Local users	VB330-SW authentication is enabled. When accessing the VB330-SW with a web browser, users needs to authenticate themselves with a username and password. These need to match either the pre-defined **admin** user, or any of the users configured in the **Setup — Security — Local users** view.

If authentication has been enabled when accessing the VB330-SW through the VideoBRIDGE Controller, the local VB330-SW user will be “admin”, but with restrictions imposed by the user account. If the password has been changed from the default, the same password needs to be configured in the **Edit device** popup in the VBC **Equipment** view.

The message entered in the **Login message** text field will be displayed to the user in the **Login** view before logging in.

5.13.9.3 Setup — Security — Tacacs+



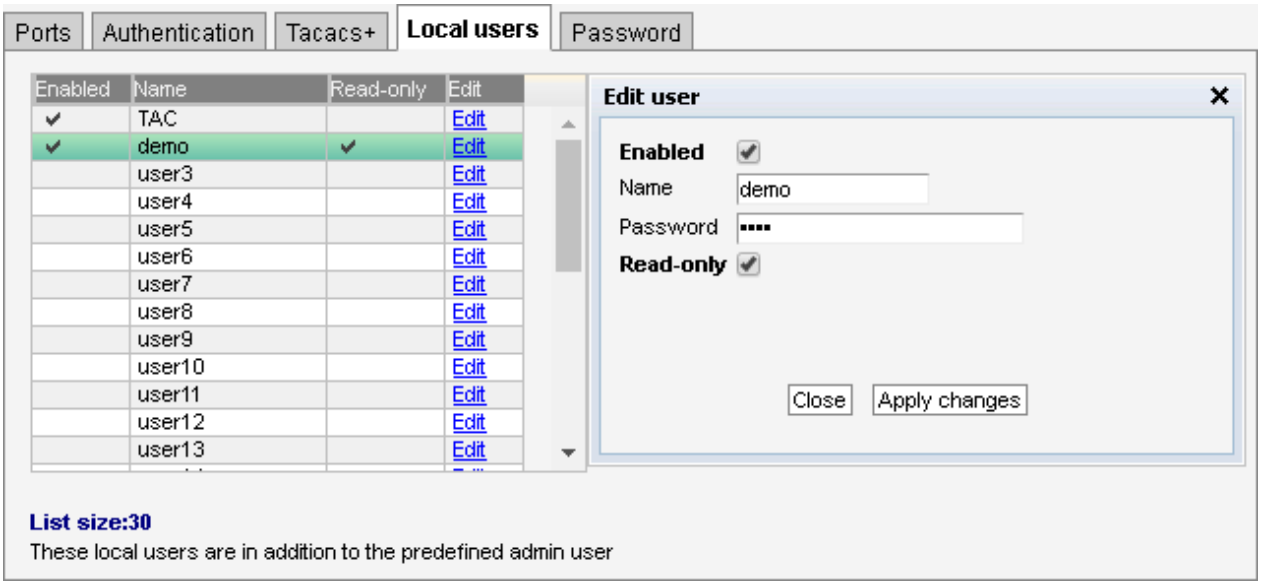
This view is used to configure a Tacacs+ server for user authentication. For this to be used, Tacacs+ authentication must be selected in the **Setup — Security — Authentication** view.

To use Tacacs+ authentication, the IP address of the Tacacs+ server must be specified, along with the secret key used to encrypt the communication between the Tacacs+ server and the VB330-SW server. The same key must also be specified as part of the Tacacs+ server configuration.

We recommend using HTTPS when using authentication, as this combines authentication with encryption. Using authentication with HTTP is not considered very secure since it is possible to sniff the un-encrypted communication and possible reverse engineer the scrambling of login details.

Tacacs+ parameters	
Server IP address	IP address of the Tacacs+ server used for authentication.
Secret	Configures a fixed string used to encrypt the communication with the server.
Default local user	Defines the local user ID that should be used on successful Tacacs+ authentication.
Auth-key	Defines which key in the Tacacs+ authentication response to use to determine the user access level. The value of this key is compared to the **Access level** below.
Access level 1–3	Up to three different Tacacs+ access levels can be configured to map to different local user accounts, allowing different authenticated users to have different access levels. The value configured here is matched with the value of the **Auth-key** configured above.

5.13.9.4 Setup — Security — Local users



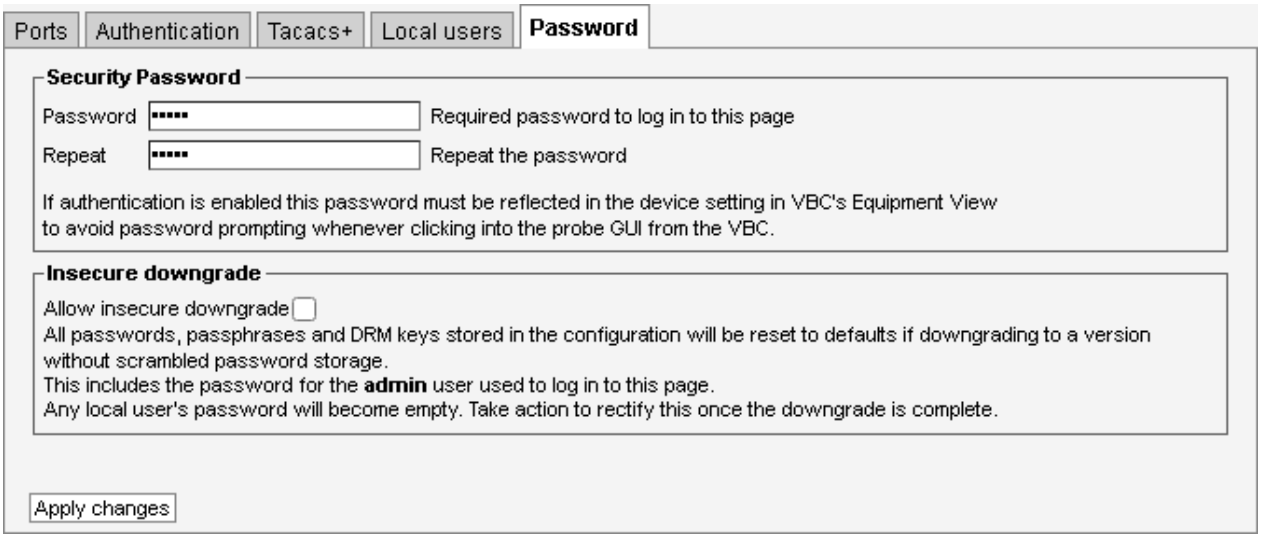
This view is used to configure local users that are allowed to access the VB330-SW user interface. For these to be used, Local users authentication must be selected in the **Setup — Security — Authentication** view. The VB330-SW supports up to 30 local users.

In addition to the users defined here, the predefined “admin” user can also log in. The password for the “admin” user is configured in the **Setup — Security — Password** view. Note that the login requirements towards the **Security** tab is independent of the general authentication and always requires the login of the admin user.

It is not possible to see which user is actually logged in to the VB330-SW, as this information is not kept or used by the probe.

Edit user	
Enabled	If this is checked, the user is allowed to log in.
Name	User-name of the account used to log in.
Password	Password of the account used to log in.
Read-only	If this is checked, the user only has read-only access to the user interface. When read-only access is activated a **READ-ONLY access** message is displayed under the alarm list. To change any parameters, the user needs to log out and then log in as another user.

5.13.9.5 Setup — Security — Password



The **Setup — Security — Password** view is used to change the password used to access all of the **Setup — Security** section. The password is changed by entering a new password and clicking the **Apply changes** button. If authentication has been enabled in the **Setup — Security — Authentication** view, the password defined here can be used with the special username “admin”.

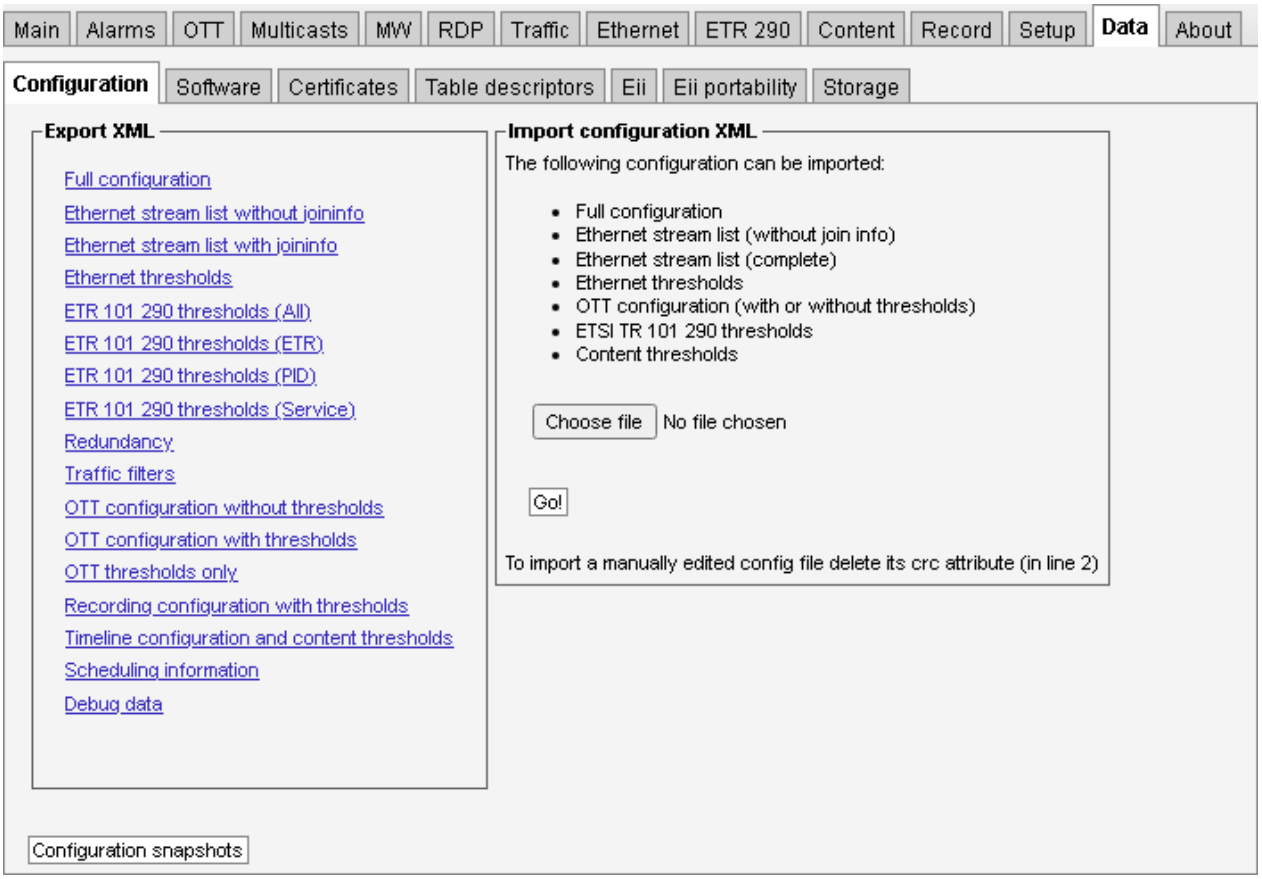
The password defined here controls access to the VB330-SW user interface. The administrative interface uses the system accounts, please refer to chapter 3.4 for details.

The method for storing passwords in the configuration file changed in version 6.5, making it incompatible with previous versions. The **Allow insecure downgrade** checkbox allows downgrades to a version that is unable to read the passwords from the configuration. Please note that the **admin** user password will be reset to the default, and that you will lose all passwords defined for local users, DRM passphrases and keys configured for OTT channels and SRT passphrases and stream IDs configured for multicasts.

It is possible to downgrade without losing passwords. Versions 6.3.0–12 and 6.4.0–5 and later can read the new password storage, converting to the old format. If you need to downgrade further, make sure the configuration is re-saved in the old format before proceeding, by making an inconsequential change to the configuration before applying another downgrade. You could, for instance, change the **Probe name** in the **Setup — Params** view and press **Apply changes** to save the configuration to disk.

5.14 Data

5.14.1 Data — Configuration



Full and partial configuration of the 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 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 VB7880 Advanced Content Extractor.

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

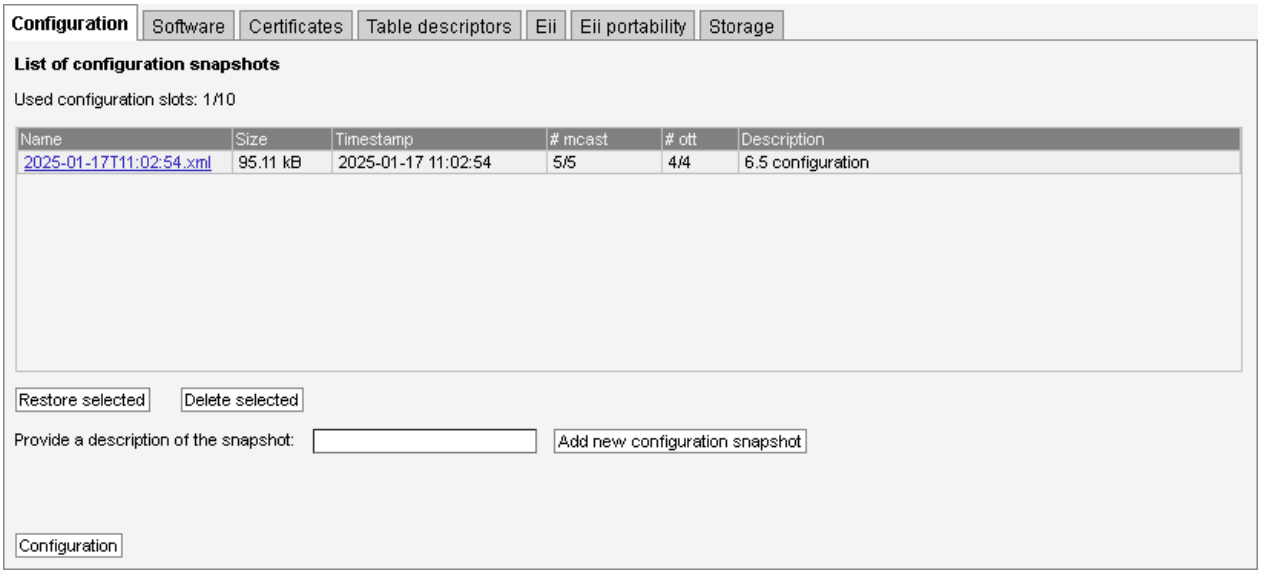
To import documents that have been manually edited the CRC attribute at the very top of the document must be deleted (i.e. delete `crc="..."` from the file). This will bypass the checksum verification mechanism.

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 Software Probe and restoring it on another will make the two 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 Software Probe misbehavior is reported. This file should be sent along with a description of the misbehavior.

5.14.1.1 Configuration snapshots

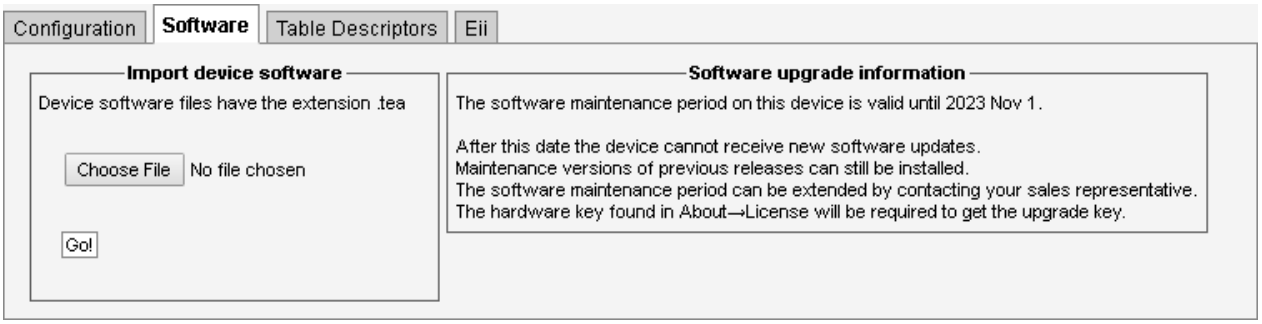


Configuration snapshots allow you to save up to 10 named probe configurations directly on the probe. Each snapshot represents a **Full configuration** XML document and can be used to restore the probe to a previous state, similar to uploading a configuration XML.

Access the **Configuration snapshot** view by clicking the **Configuration snapshots** button below the XML export options in the **Data — Configuration** view. From here you can restore any existing snapshot by selecting it and clicking the **Restore selected** button, and create new snapshots by providing a name and clicking the **Add new configuration snapshot** button. If all snapshot slots are used, you can delete an existing snapshot by selecting it and clicking the **Delete selected** button.

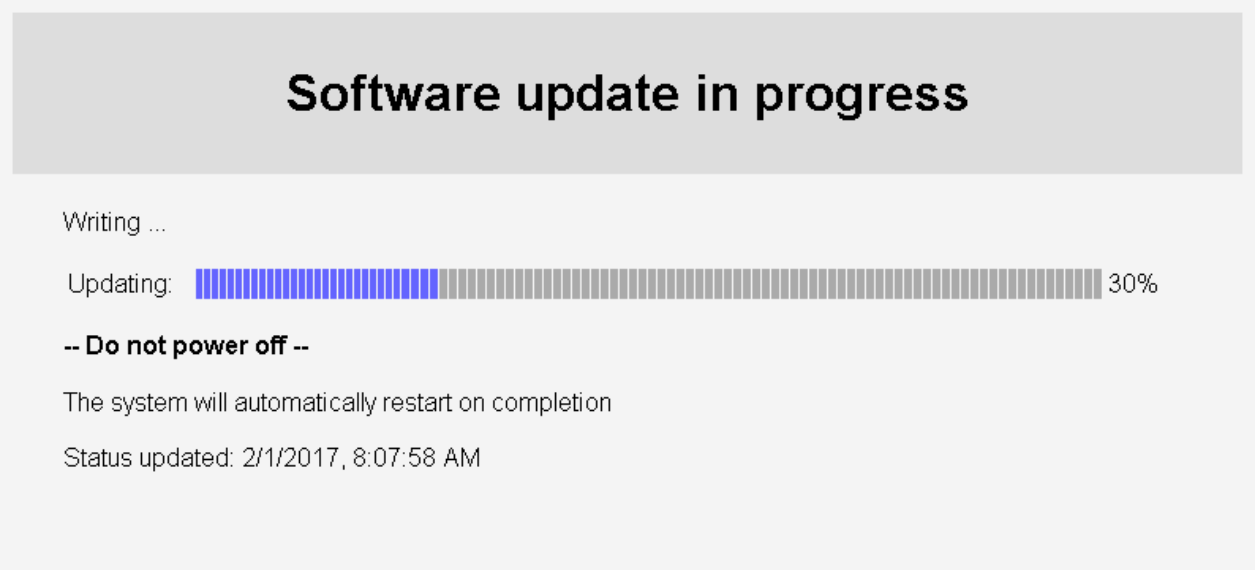
Click the **Configuration** button to return to the **Data — Configuration** view.

5.14.2 Data — Software



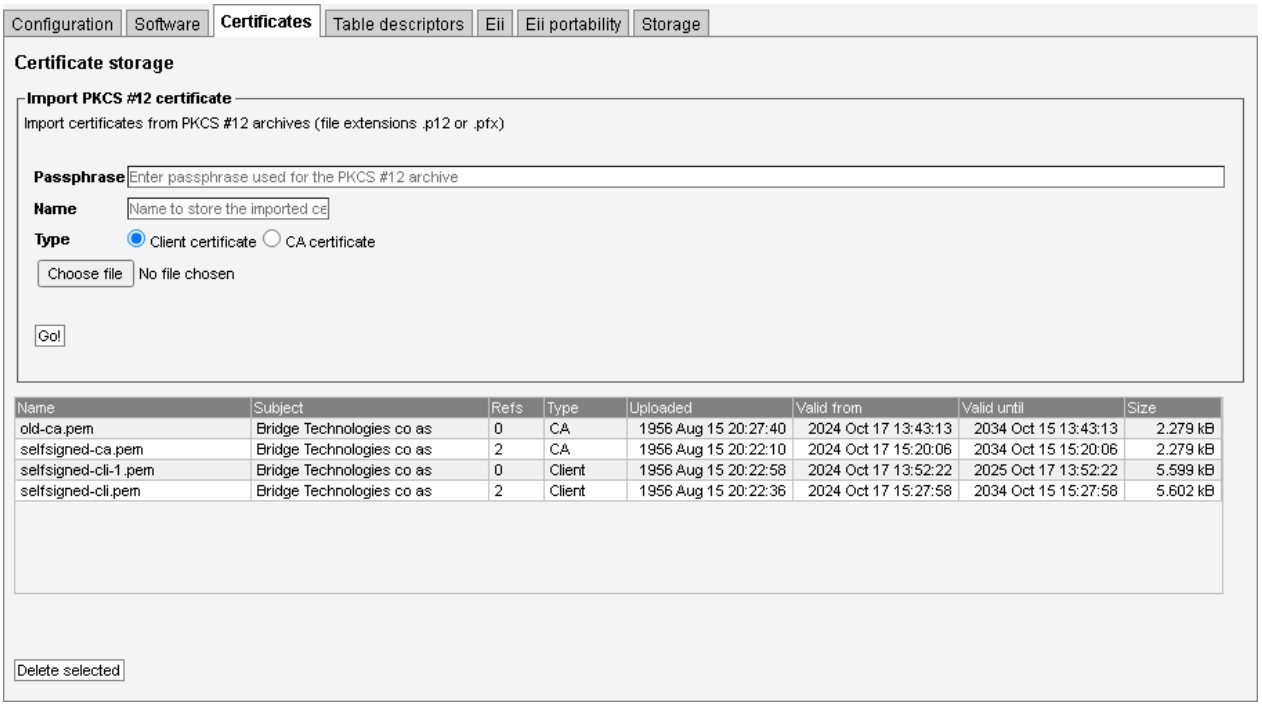
The software section allows the Software Probe to be upgraded to a newer software version. Select the **.tea** file from the local PC and click **Go!** to copy the software to the VB330-SW. When the upload is complete, clicking the **Update software** button will begin the upgrade procedure.

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.

5.14.3 Data — Certificates (requires OTT-OPT)



This view makes it possible to upload client certificates for mTLS authentication and CA certificates for TLS host verification.

Use **Import PKCS #12 certificate** to upload a certificate. Certificates must be available as a PKCS #12 archive (these files usually have a **p12** or **pfx** file extension). Enter the passphrase used for the PKCS #12 archive, enter a name under which to store the certificate, and select whether the certificate is a client certificate or a CA certificate. Click the **Browse** button to select the file that contains the certificate and then click the **Go!** button and the certificate will be imported.

All imported certificates are displayed in the certificate list in the bottom half of the screen. To remove certificates from the certificate store, select the certificate or certificates to remove and click the **Delete selected** button.

5.14.4 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).

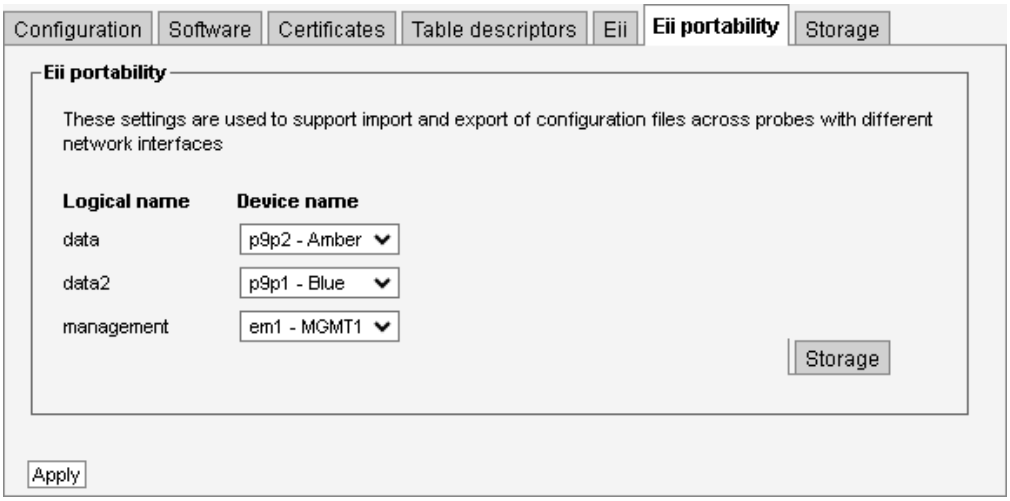
Contact Sencore for more information about private descriptors.

5.14.5 Data — Eii

The **External integration interface** (Eii) allows inclusion of Sencore VideoBRIDGE 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.

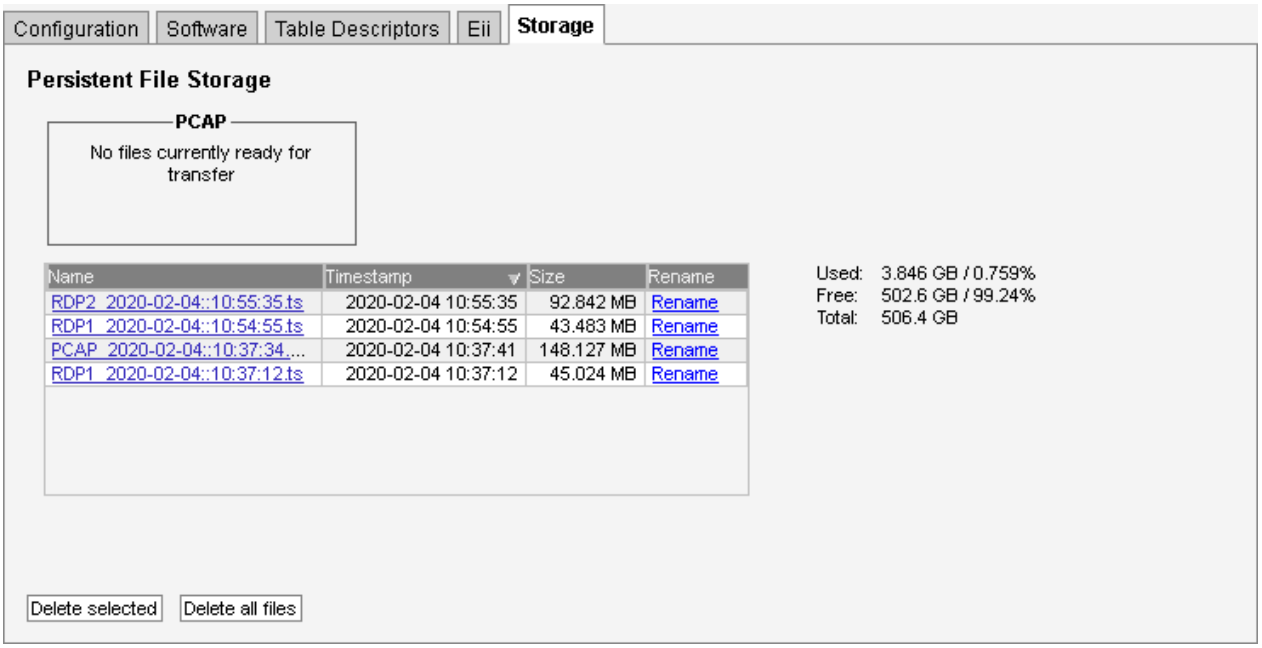
Please refer to the document **Eii External Integration Interface** for detailed information about Eii.

5.14.6 Data — Eii Portability



This view makes it possible to map the logical network interface names **data**, **data2** and **management** to the physical network interfaces available on the VB330-SW. These mappings are used when importing and exporting configuration files between probes of different types and when using the **setrdp** Eii interface.

5.14.7 Data — Storage (requires DATA-LOG-OPT)



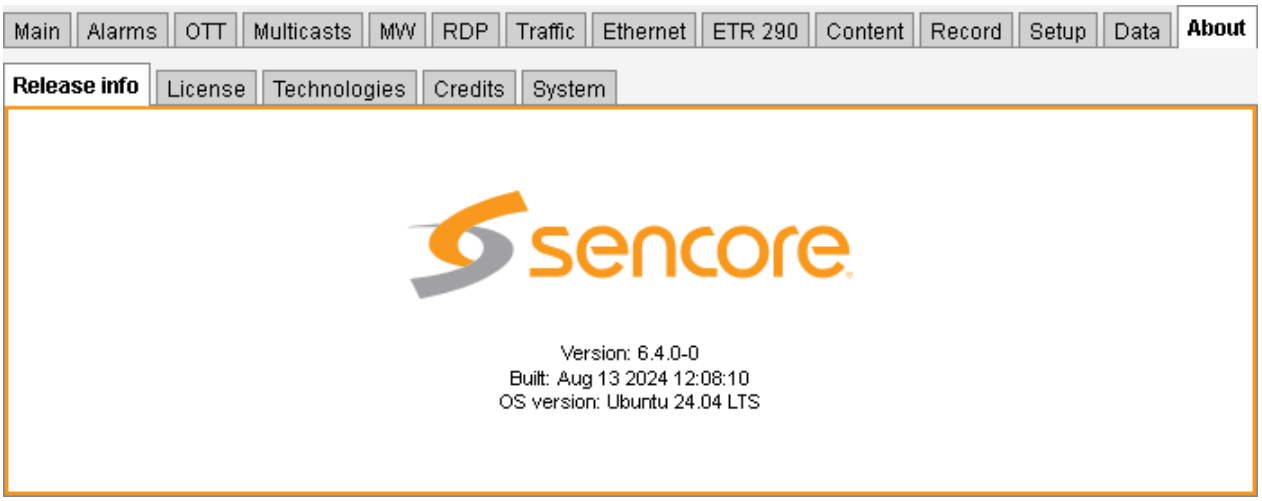
The DATA-LOG option allows the internal hard drive to be used for storing recordings. RDP recordings made from the **RDP — Control** view are automatically stored and can be retrieved from here.

PCAP recordings made from the **Ethernet — PCAP** view can also be stored for later retrieval. When a PCAP recording is available, clicking the **Transfer files** button copies it to the persistent storage area.

The probe will generate system information messages when the storage has less than 10 % free memory. When the storage is full, a system error is generated. These are configured in the **Alarms — Alarm setup** view.

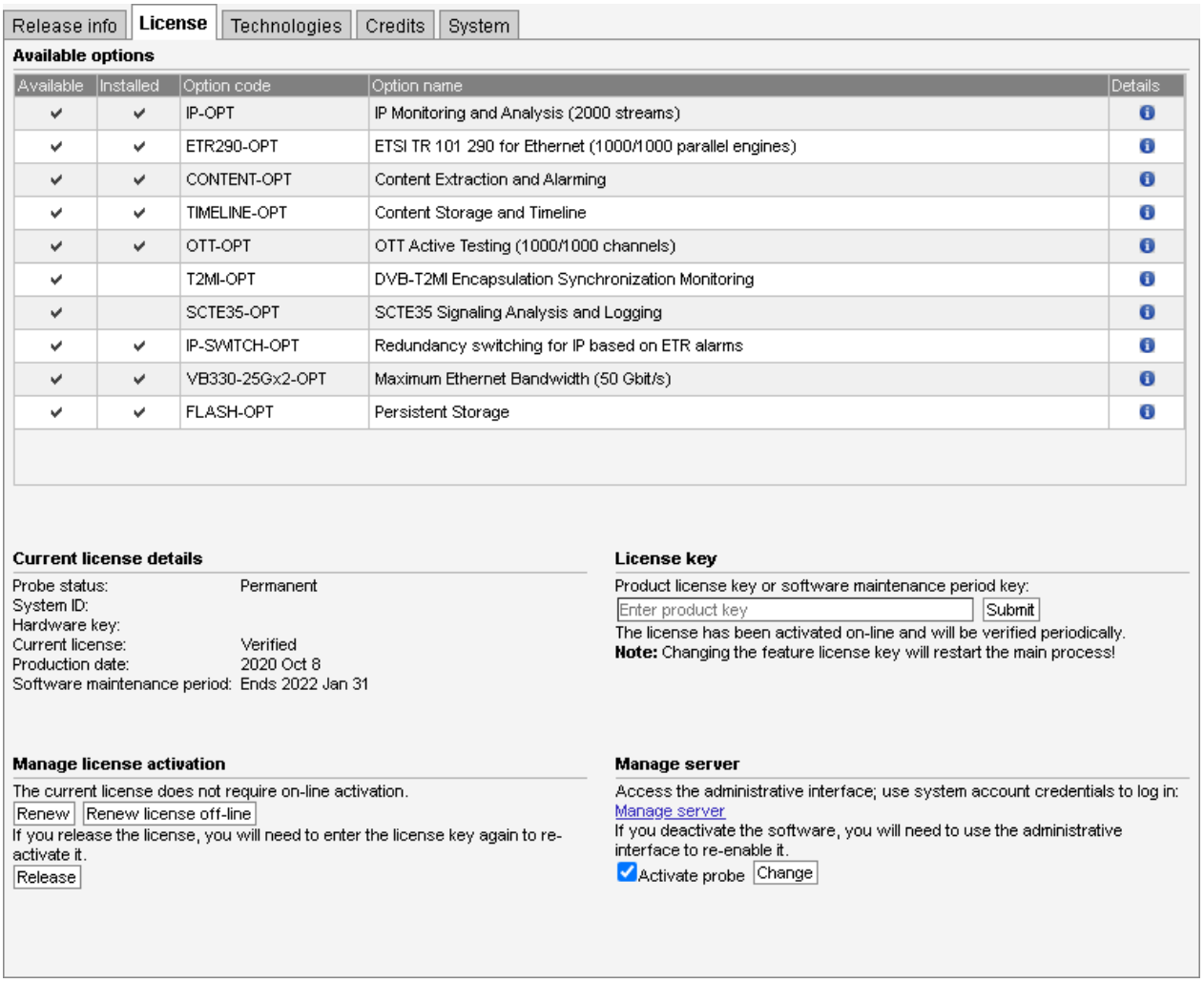
5.15 About

5.15.1 About — Release info



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

5.15.2 About — License



The **License** view displays the currently active license. The license includes the available 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 license key is activated towards a license server. Depending on the license properties, the activation might need to be updated periodically. The key is transferable between systems running the same software, as long as the license is not permanently assigned to a system. The system identifier is used to identify the system. The **Current license** field will display information on when the license key was last activated and possibly when it needs to be activated again. 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.

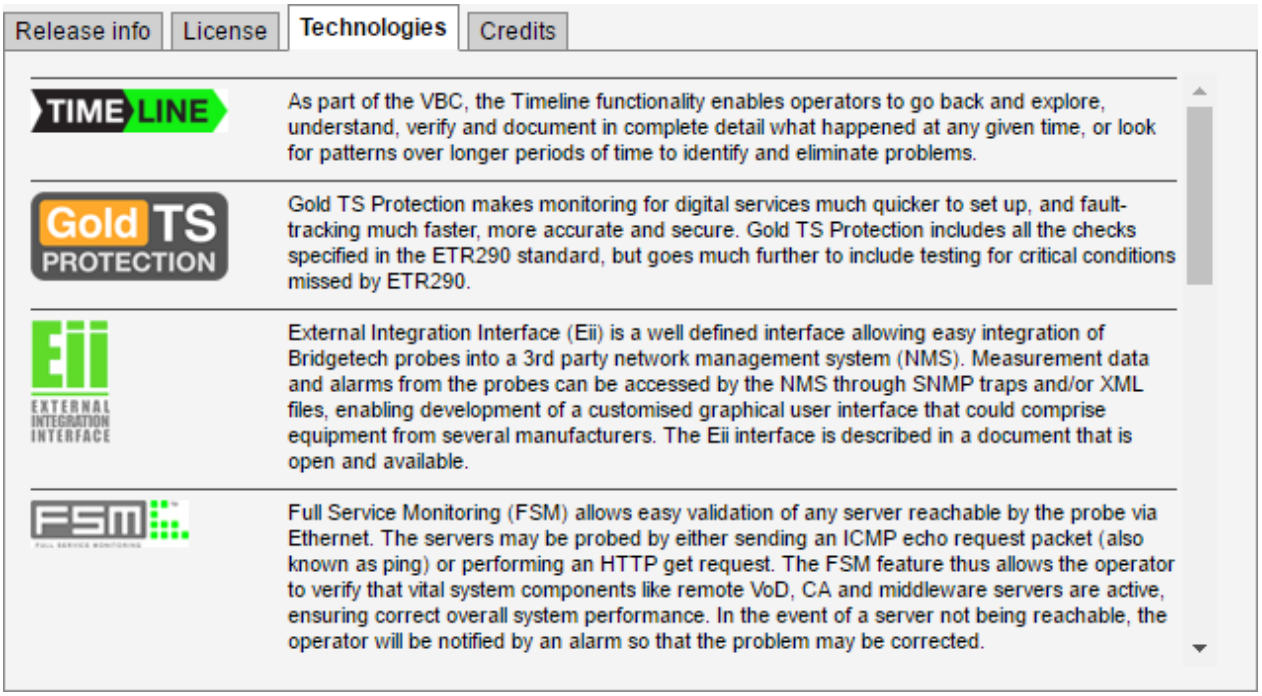
Please refer to G Appendix: On-line License Activation for more information on how to use on-line activated licenses. This appendix also describes how to renew the license when the Software Probe cannot connect to the Internet.

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

Click the **Manage server** link to access the Cockpit administrative interface, see chapter 3.4 for more information.

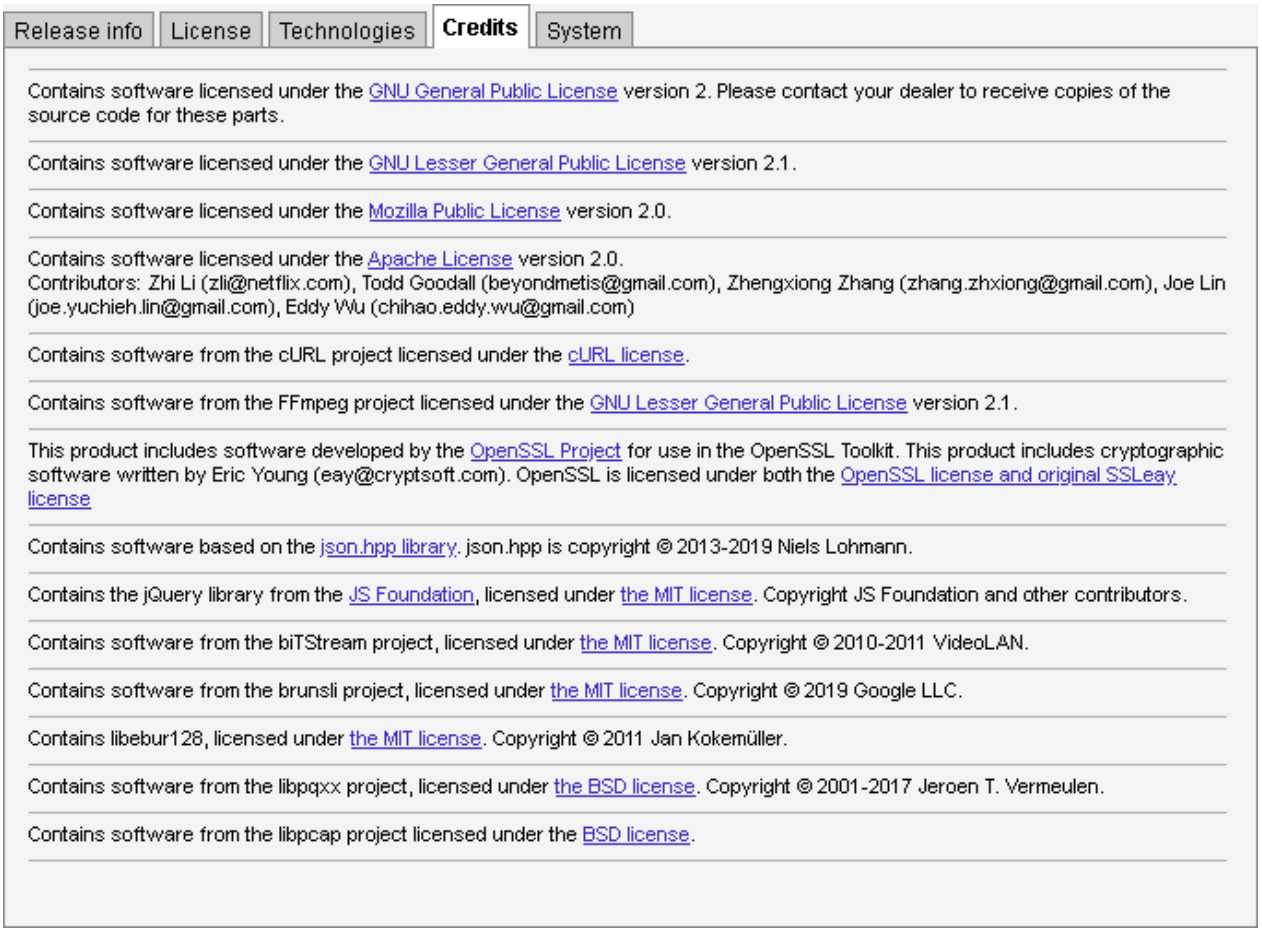
To disable the Software Probe, uncheck the **Activate software** checkbox and click the **Change** button. You cannot do this if it has been set as the default software through the administrative interface (which is done by default the first time you activate the software), you will need to remove it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

5.15.3 About — Technologies



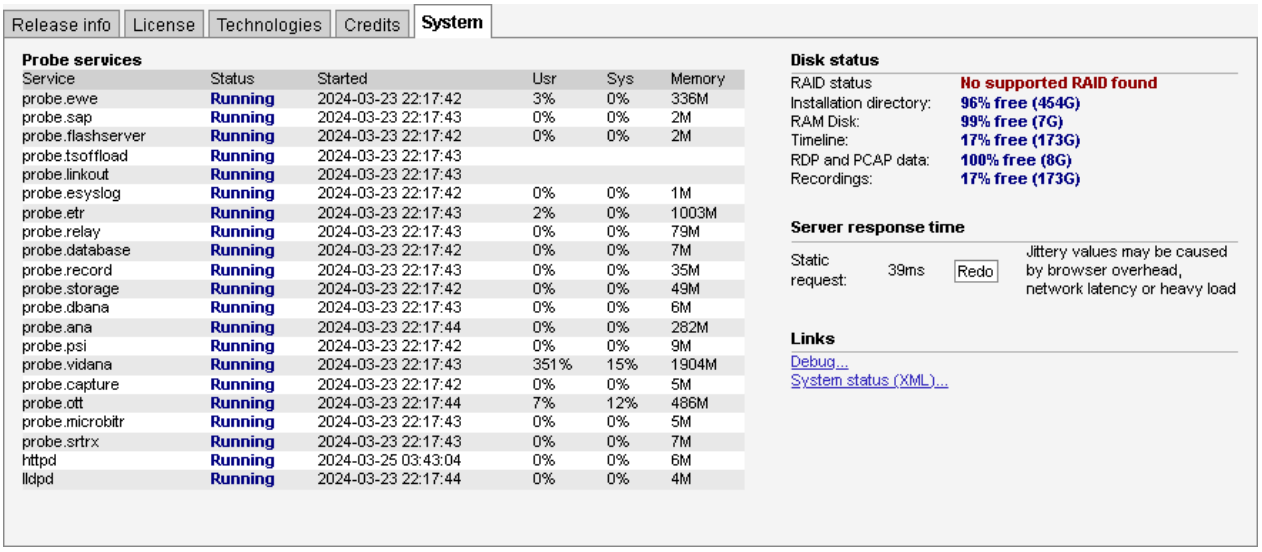
The **Technologies** view lists some of the technologies available in the Sencore VideoBRIDGE product family.

5.15.4 About — Credits



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

5.15.5 About — System



The **System** view displays a snapshot of the current status of the system, to ensure correct 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* or *Disabled* if the corresponding feature is not licensed or available. The current CPU and memory usage is also displayed.

Disk status displays free disk space to give the user some overview of disk resources available. It will additionally display the status of the RAID system, if supported. If no RAID system is installed, the message “No supported RAID found” will be displayed in red. The same message will be displayed if a RAID system is installed but not detected, as the installed software is unable to differentiate between the two cases.

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 Software Probe alarms are independent of the VideoBRIDGE Controller alarms. The 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 Software Probes. The VBC therefore generates alarms based on error-second statistics gathered from 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 VB7880 Advanced 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 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 Software Probe together with Ethernet error-second threshold values (as set in the VB330-SW 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.

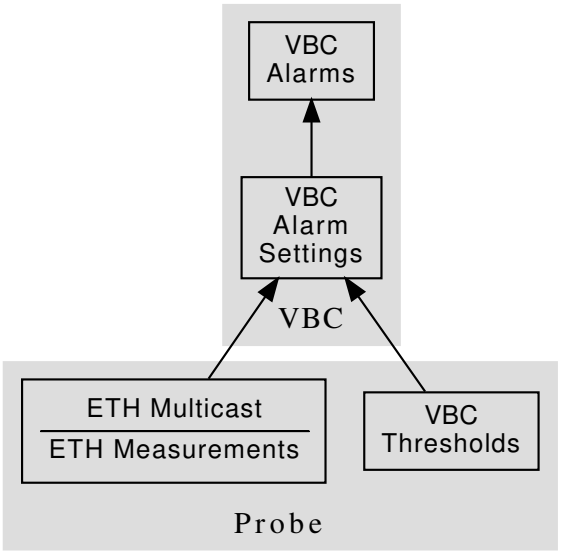


Figure A.1: VBC alarming based on Software Probe measurements

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.

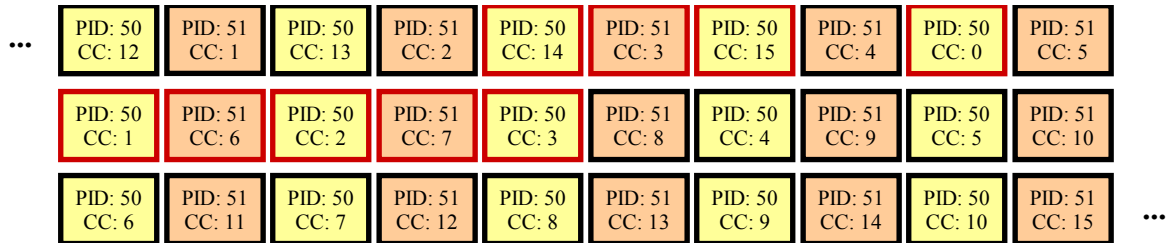
Example of RTP sequences and their effects on monitoring:

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 ($15 \rightarrow 12$)	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)**

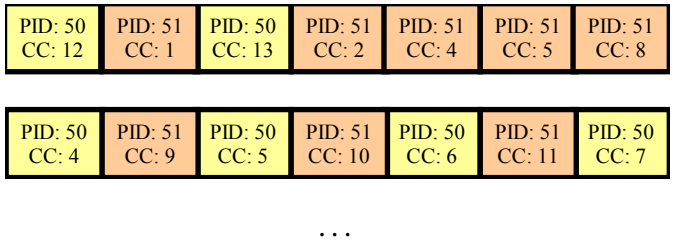
B.2 Default Multicast Monitoring

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.

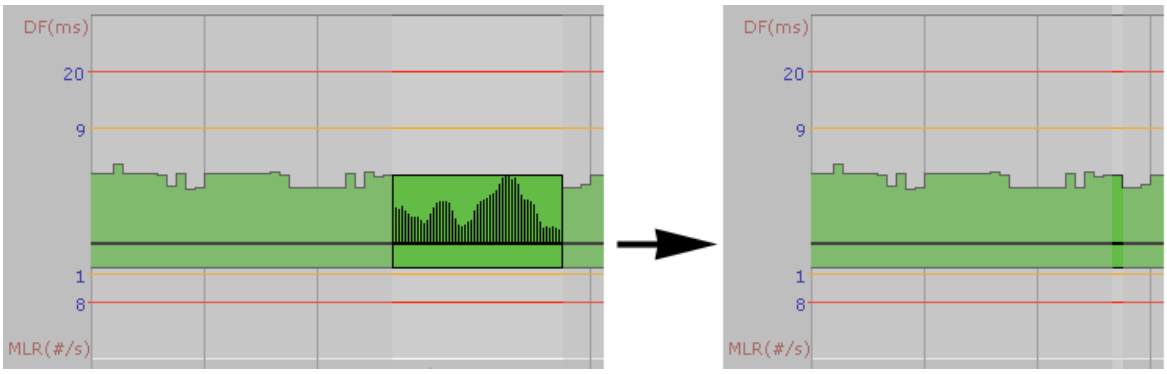
The range of the MediaWindow graphs can be configured by the user. Even when the graph is updated in “real-time” each bar in the graph will represent a large number of elementary measurements. For a 5Mbit/s stream there will be approximately 500 elementary measurements per second, assuming a mapping 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.

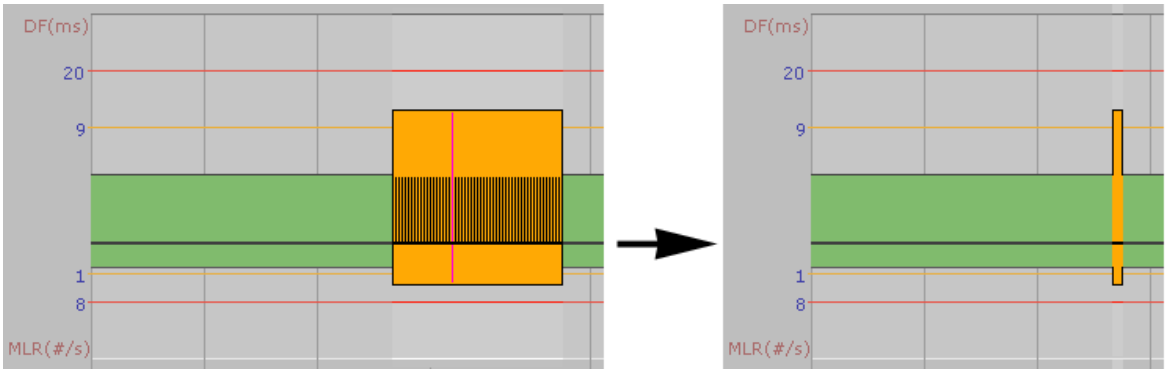
The rest of this discussion assumes the MediaWindow graph range is set to “running” since that lowers the probability that more packet losses occurred inside the same bar-interval.

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

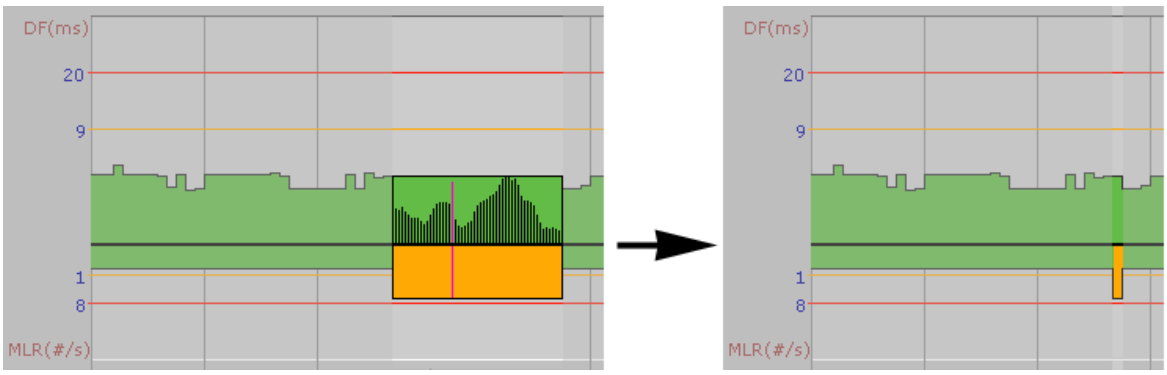


B.3.1 IAT Before and After Router

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.

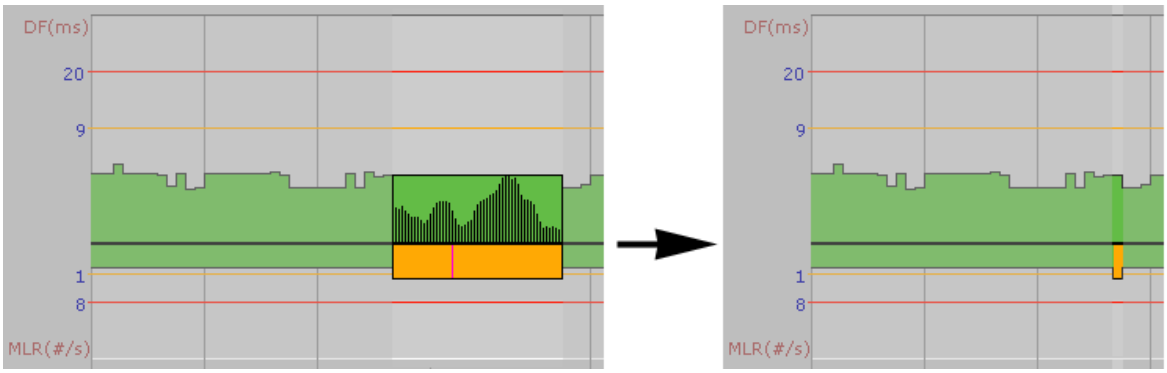


For VBR streams a similar packet-loss will not necessarily affect the IAT graph even if the time between two neighboring packets doubles. The pink line represents the IAT and MLR value measured for the missing packet.

B.3.2 Identifying UDP Packet Loss

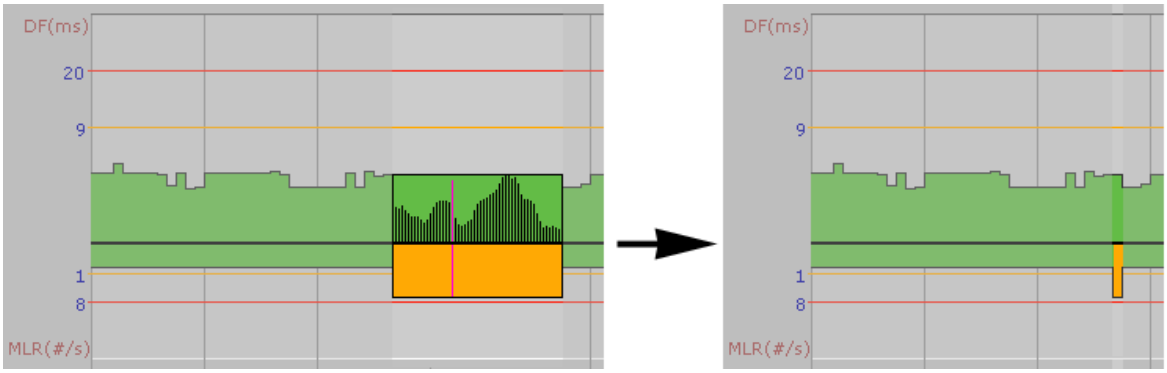
This discussion does not apply to streams with TS/RTP mapping since in that case identifying UDP packet loss is straight forward.

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 Content Thresholds

When enabling the various content analysis options in the **Content — Content thresh.**, a processing overhead is introduced. Some of the options introduce a relatively small performance overhead, whereas some may introduce a greater overhead. The overhead is also relative to the data that is being analyzed, performing picture analysis is heavier on a 4K UHD video stream than on an SD stream.

While picture analysis does not require every video frame to be decoded, enabling real-time audio analysis does require the entire audio stream to be decoded. MOS scoring is quite CPU intensive, and should only be enabled for the services where such scoring is required.

The **Main — CPU usage** view contains a **Backlog** column that indicate the length of the content analysis queue for each of CPU core. As long as the backlog value is stable, the system should have enough resources to handle the configured load. If the value keeps increasing, try disabling content analysis for a few streams, or filter away PIDs that do not need to be analyzed in the content threshold.

The VB330-SW will raise a *Content analysis overloaded* system alarm if it detects that it is unable to keep up with the configured load. If the backlog numbers indicate that only a few CPU cores are overloaded, you can try redistributing the streams using the **Main — CPU usage — Advanced** view, or try to reduce the load, as described above.

If the load on the content analysis process becomes extremely high, it might start to drop incoming data that it is unable to process. If this happens, the VB330-SW will raise a *Data queue overflow (btvidana) – Thumbnailing and freeze-frame analysis paused, SCTE35 data may be lost* system alarm.

B.6 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 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.7 Monitoring HTTP Live Streaming (HLS)

In HLS, each profile is identified by its own playlist, whose URL is listed in the master playlist, which in turn is downloaded from the **Manifest URL** as configured in the channel configuration in the **OTT – Channels** view.

By default, the OTT profiles are identified by their URL. Some streaming systems generate profile URLs based on a session ID, and in some cases these session IDs are re-generated every time the master manifest is downloaded. In these cases, the OTT engine will see all profiles as new every round and is unable to retain any profile history. If this happens once, the event *All playlist URLs changed* is flagged, and if it happens repeatedly, the alarm *HLS playlist URLs unstable* will be raised on the channel.

In both cases, the recommendation is to enable the setting **Monitor HLS profile manifests only**. This will keep the downloaded master manifest in memory until the session times out (as indicated by the playlist URLs becoming unavailable), and will also change the way profiles are identified to instead use their position in the master manifest.

To avoid unwanted alarms about the session timing out, and gaps in the monitoring or Timeline, set the **Reset connection after** timeout value in the **OTT — Settings** view to a value shorter than the session timeout.

B.8 Monitoring RTMP and SHOUTcast

For RTMP and SHOUTcast, data is transmitted in real-time. To allow time for analysis, the Software Probe downloads data in chunks of ten seconds and then stops, which means that it cannot continuously monitor streams of these types. Since monitoring blocks the OTT engine, channels of these types should be assigned their own engine or at least not be mixed with channels of other types.

B.9 OTT descrambling with Verimatrix

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

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

B.10 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 segments, 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

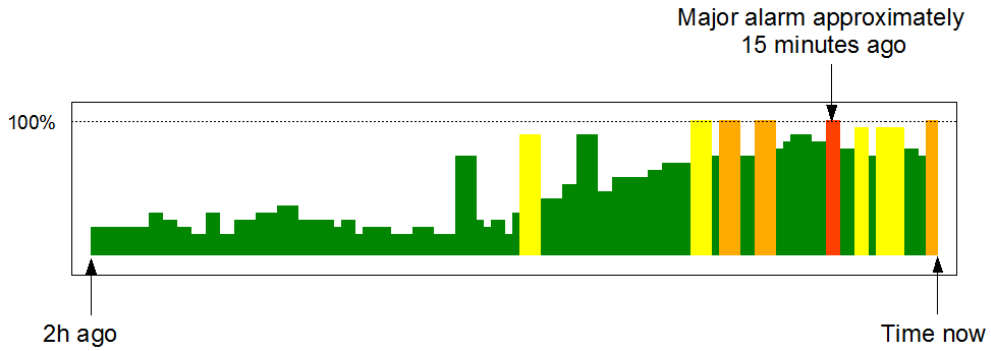
C.1 OTT Profile Health Bar

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 segment length. The graph is scaled so that 100% indicates a segment download time identical to segment length (in seconds), segment length being signaled in the profile manifest. Quick segment 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.

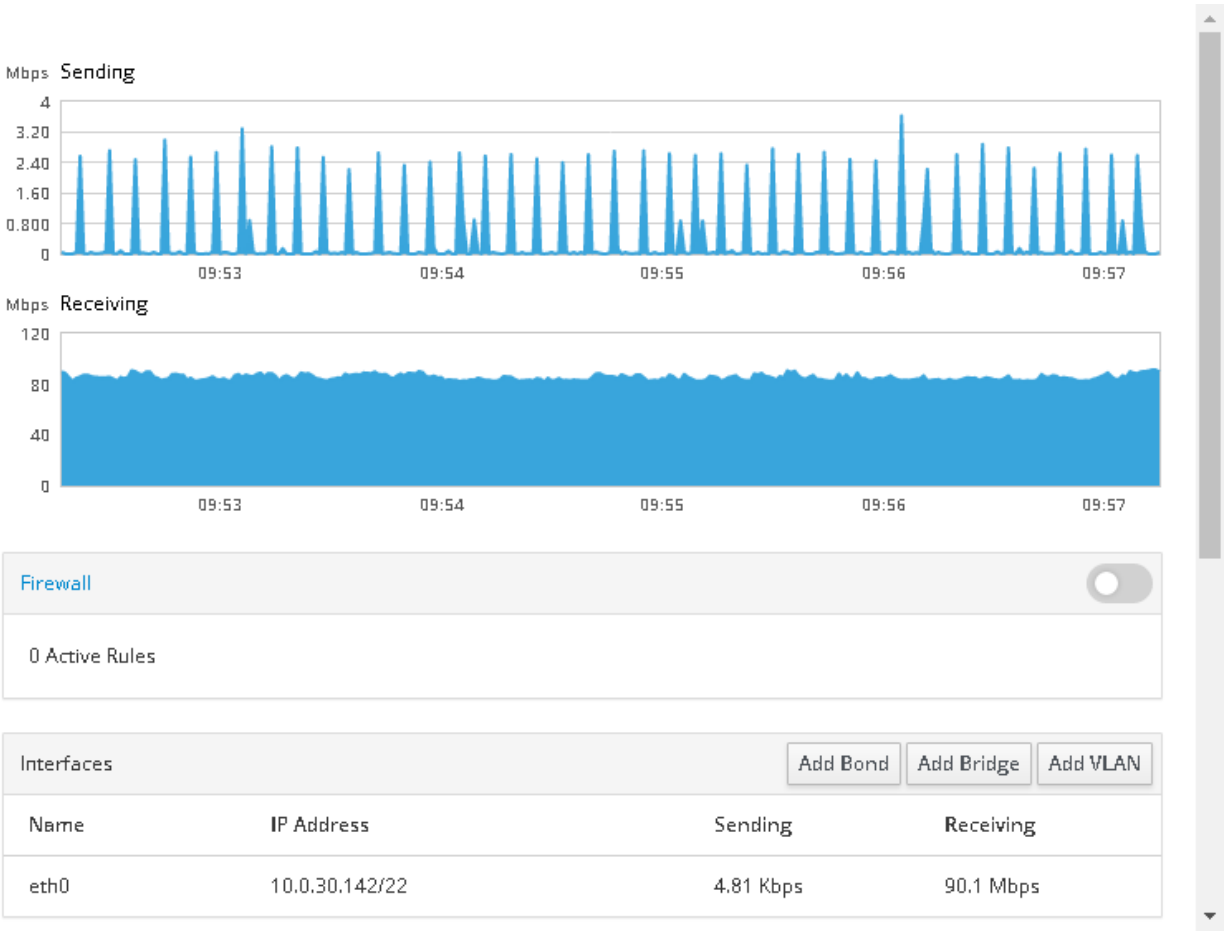
D Appendix: Network configuration

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 Cockpit administrative interface, as described in section 3.4. The Cockpit administrative interface uses the same log-in credentials as the system accounts.

Click on the **Network** heading to open the network configuration.



For more information on how use Cockpit, please refer to the Cockpit documentation[1].

[1] https://cockpit-project.org/documentation.html

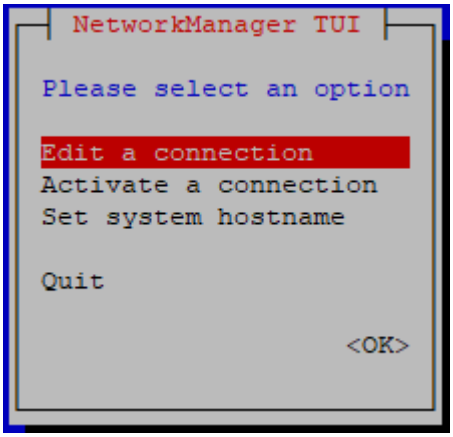
If you make changes here that causes you to lose web access to the server, you may need to use the command-line tools as described below.

D.2 Command-line based configuration

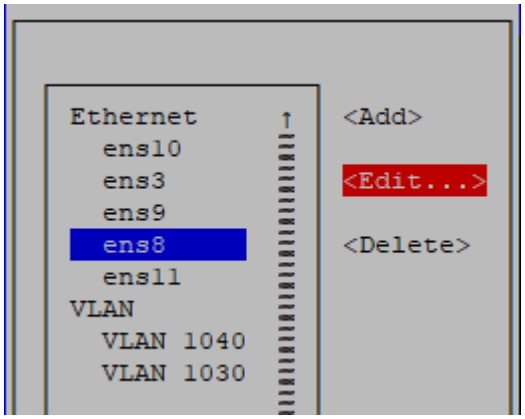
Changes to network configuration, adding new interface devices and VLANs can be done with the **nmtui** tool. Simply type **sudo nmtui** whilst logged into the server command shell[2]. Navigate the nmtui menus using the cursor (arrow) keys and Enter to select.

Editing Network interface configuration

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

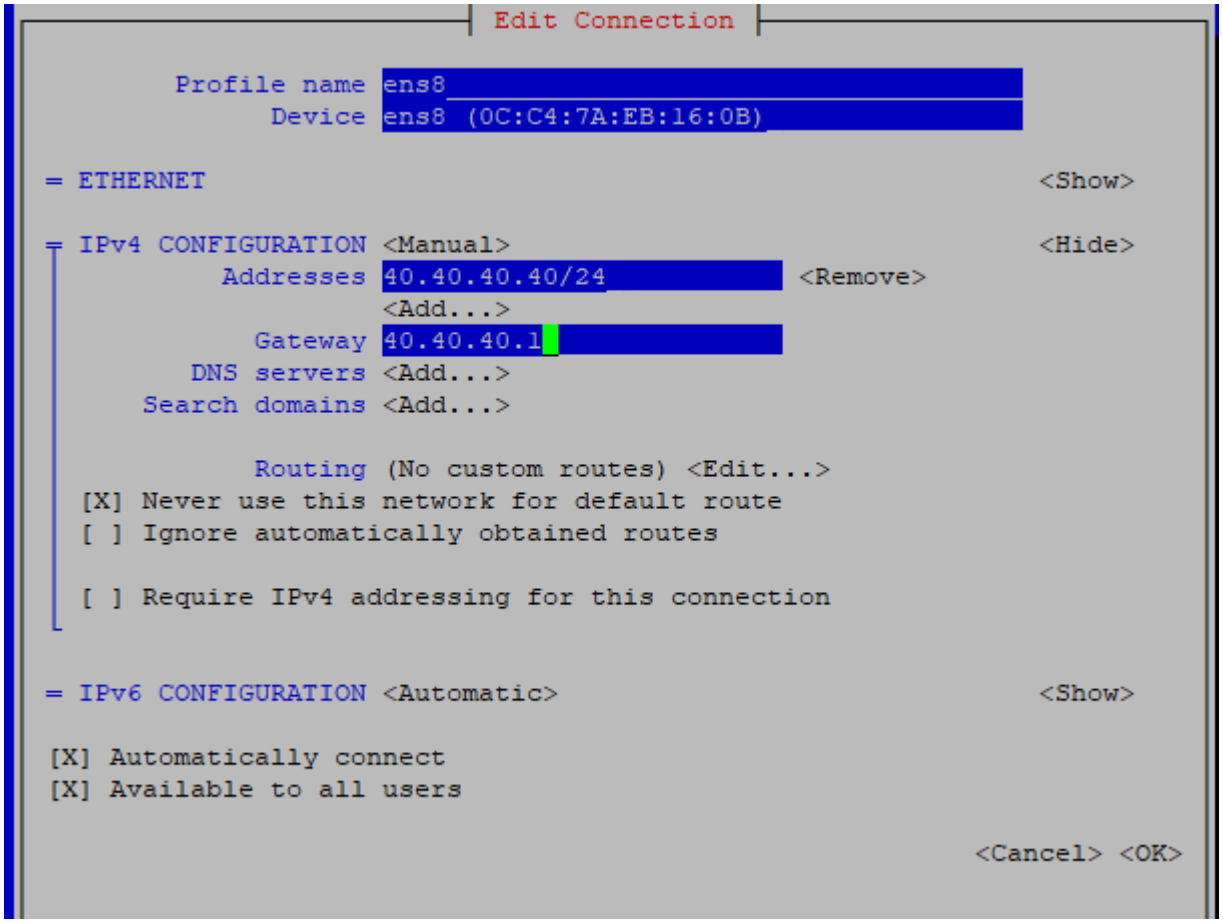


Select the interface to be edited and then select **Edit...** from the menu.



[2]If the **nmtui** tool is not available on your system, you can install it by issuing the command **sudo apt install network-manager**

Make the necessary changes to IPv4 and IPv6 configuration.



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

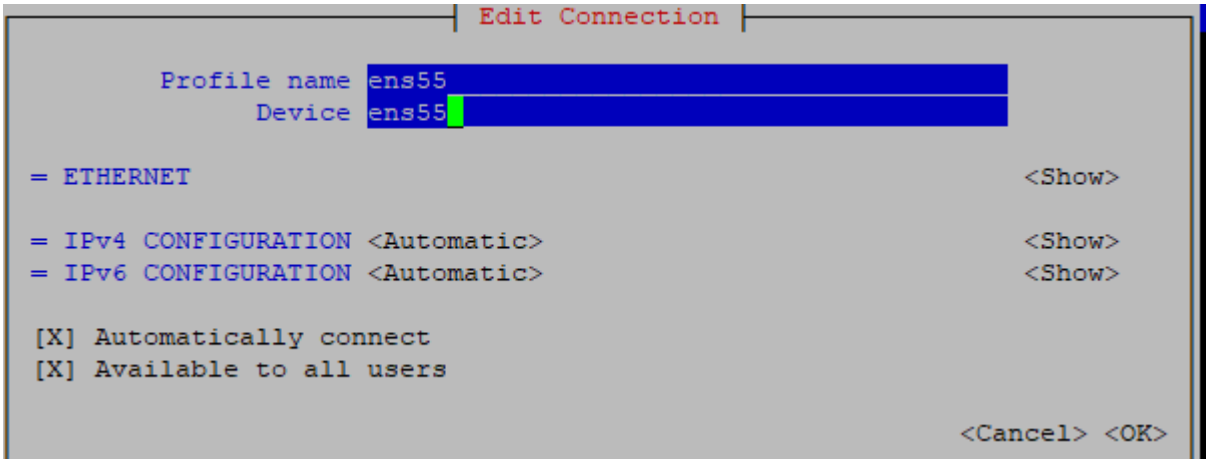
Sometimes it is desirable to select **Never use this interface for default route**, particularly if additional interfaces are only used for monitoring multicast traffic or when setting up a native interface for adding VLANs.

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**.

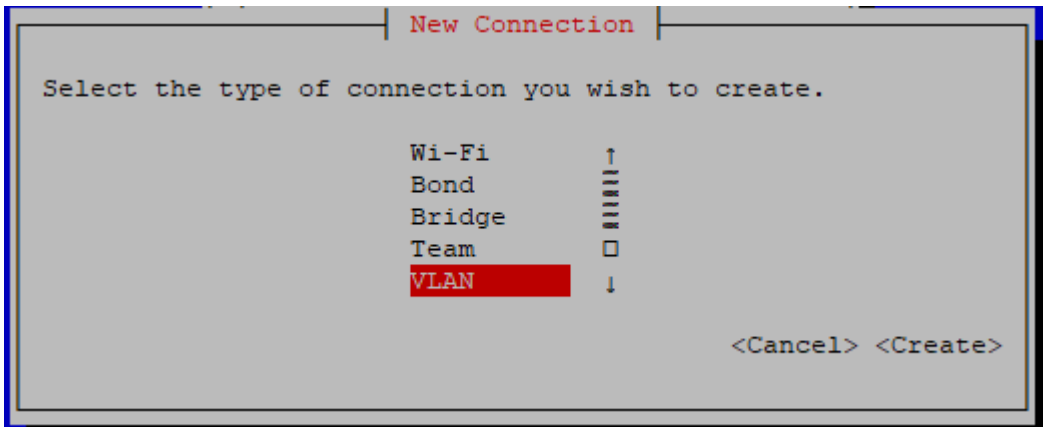
Adding new and VLAN interfaces

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.

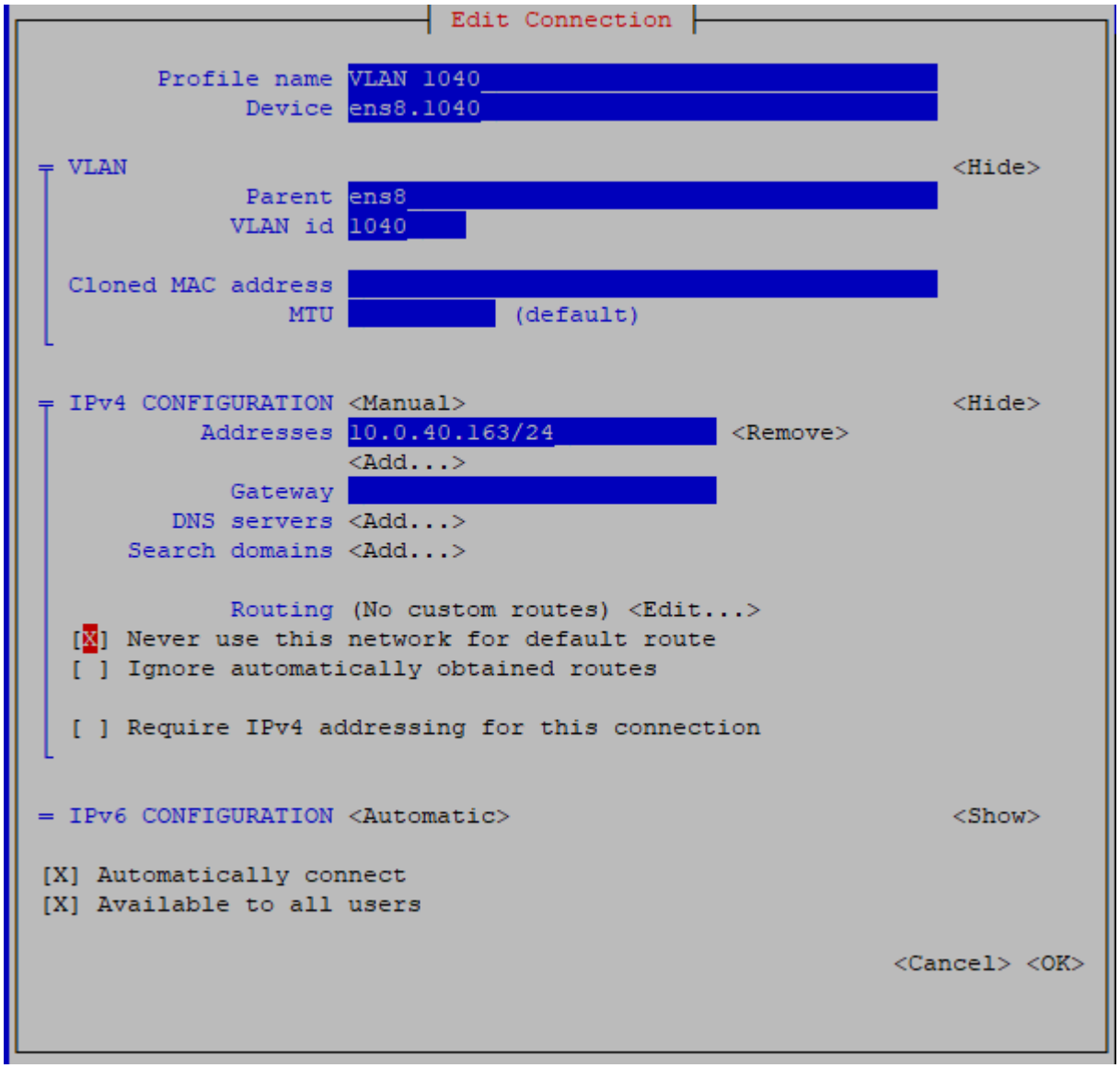
To find the system assigned name for a newly added hardware device use the command line **ifconfig** or search in the output of the **dmesg** tool. It can be helpful to keep the nmtui **Profile name** for the device the same as the device name itself, for example:



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.

D.3 Further reading

For more documentation, please refer to the *Introduction to networking*[3].

[3] https://ubuntu.com/server/docs/introduction-to-networking

E Appendix: Enabling NTP time synchronization

It is strongly recommended that the server running the 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 — Routing** view will automatically add it as a time synchronization source.

For more details on how to configure Chrony, please refer to *How to serve the Network Time Protocol with Chrony*[1].

[1] `https://ubuntu.com/server/docs/how-to-serve-the-network-time-protocol-with-chrony`

F Appendix: SRT Streams

F.1 Introduction

F.1.1 Overview

SRT is a user-level transport protocol that ensures *secure*, *reliable transport* of video and audio across multiple unstable network connections. With the UDP data transfer protocol at its base, SRT introduces several enhancements such as end-to-end encrypted data packets (using AES), improved congestion control and efficient packet loss recovery.

F.1.2 Reception

The probe currently supports receiving up to 200 concurrent SRT streams. SRT reception is configured by editing a stream in the **Multicasts — Streams** Edit view and providing the necessary SRT parameters. In this manner the received SRT stream is turned into a stream for TS monitoring. More details are provided in section 5.4.8.

The probe can use the SRT protocol to receive streams in three modes of operation:

- Caller: the probe sends the connection request to the peer, which must be listener, and this way it initiates the connection.
- Listener: the probe waits to be contacted by any peer caller.
- Rendezvous: both parties are equivalent and both the probe and the peer attempt to initiate a connection simultaneously. Whichever party happens to start first (or succeeds in punching through the firewall first) is considered to have initiated the connection.

When using the probe in **Listener** mode it is mandatory to specify:

- Port: local port to listen for connections on

The **Host** field is ignored in **Listener** mode.

When using the probe in **Caller** or **Rendezvous** mode it is mandatory to specify:

- Host: remote IP address to connect to
- Port: remote port to connect to

All modes of operation may be encrypted and therefore accept a passphrase to decrypt the stream.

In all modes of operation the probe utilizes the network interface the stream is “joined” on, specified in the **General** tab in the **Multicasts — Streams** Edit view.

F.1.3 Transmission

The probe supports relaying up to two streams using **RDP (Return Data Path)**, and these may be transmitted using the SRT protocol. SRT transmission is configured in the **RDP — Setup** view.

When mode *Relay over IP* is selected, *Encapsulation* can be set to *SRT*.

Encapsulation can be set to *SRT* when the *Relay over IP* mode is selected. It is then possible to specify these SRT Transmit options:

- Mode: The SRT mode of operation utilized to transmit.
- Passphrase: passphrase to encrypt the forwarded stream. Must be between 10 and 79 characters long.
- The latency value insisted upon by the sender side as a minimum value for the receiver. Minimum 120ms.

The probe can use the SRT protocol to transmit streams in three modes of operation:

- Caller: the probe sends the connection request to the peer, which must be listener, and this way it initiates the connection.
- Listener: the probe waits to be contacted by any peer caller.
- Rendezvous: both parties are equivalent and both the probe and the peer attempt to initiate a connection simultaneously. Whichever party happens to start first (or succeeds in punching through the firewall first) is considered to have initiated the connection.

In all modes of operation the probe utilizes the network interface the stream is “relayed” over, specified by the *Relay via interface* configuration option in the RDP Setup page.

The current version of the SRT implementation is based on version 1.5.3 of the Haivision reference implementation.

G Appendix: On-line License Activation

G.1 Introduction

The Software Probe uses licenses which are activated 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 Software Probe sends the on-license activation over the Internet, it includes some basic information to verify the 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 activation procedure is available as well.

The VB330-SW must also be configured with a correct date and time. Please refer to E Appendix: Enabling NTP time synchronization for more information on configuring time synchronization.

Direct access to activation server

To activate the license automatically, 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.

Using the VBC server as a proxy

When installing the VBC software to a server, a proxy is automatically configured to allow its connected blades to connect to (and only to) the licensing system as described in the previous section.

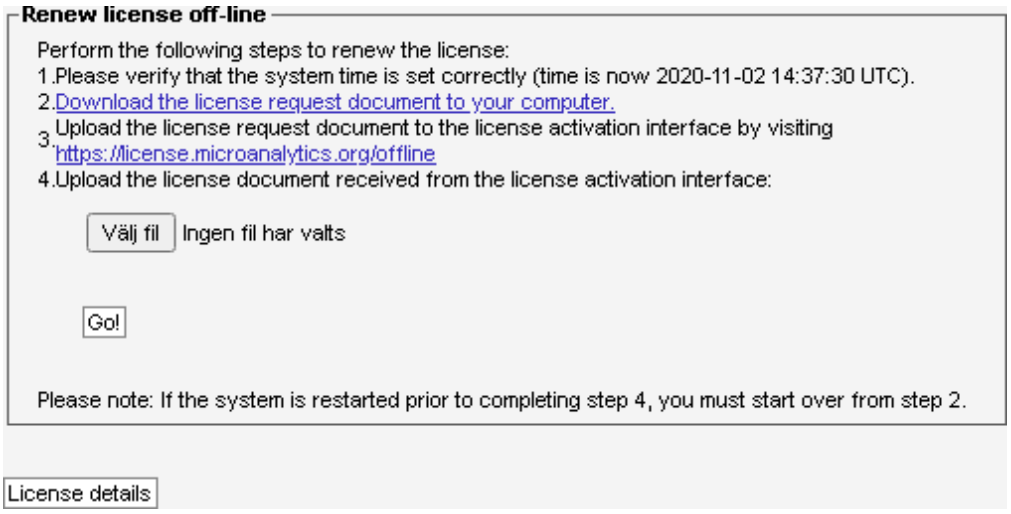
When the VB330-SW has been configured with the address to the VBC server in the **Setup — Routing** view, the VB330-SW will automatically attempt to use this proxy if a direct connection fails.

Using an arbitrary proxy server

The 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 — Security — Ports** view, the VB330-SW will automatically attempt to use this proxy if a direct connection fails.

Off-line activation procedure

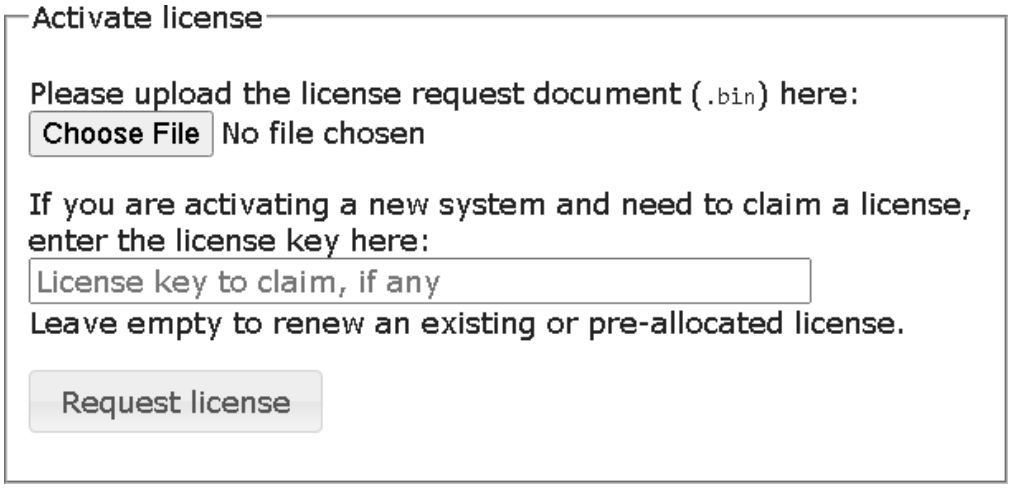
If the VB330-SW network is completely disconnected from the Internet, it is still possible to activate the license using the off-line activation procedure. When using this, the license will be tied to the system and will not be transferable to another server. Click the **Renew license off-line** button to start the off-line activation 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 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[1].

[1] `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 Software Probe.

The software maintenance can be purchased for a two or four 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 5.15.2 for more details. For an overview of software maintenance periods for multiple units, please refer to the **Equipment** view on the VideoBRIDGE Controller server.

Use the **Data — Software** view to update the VB330-SW software, please refer to chapter 5.14.2.

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 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

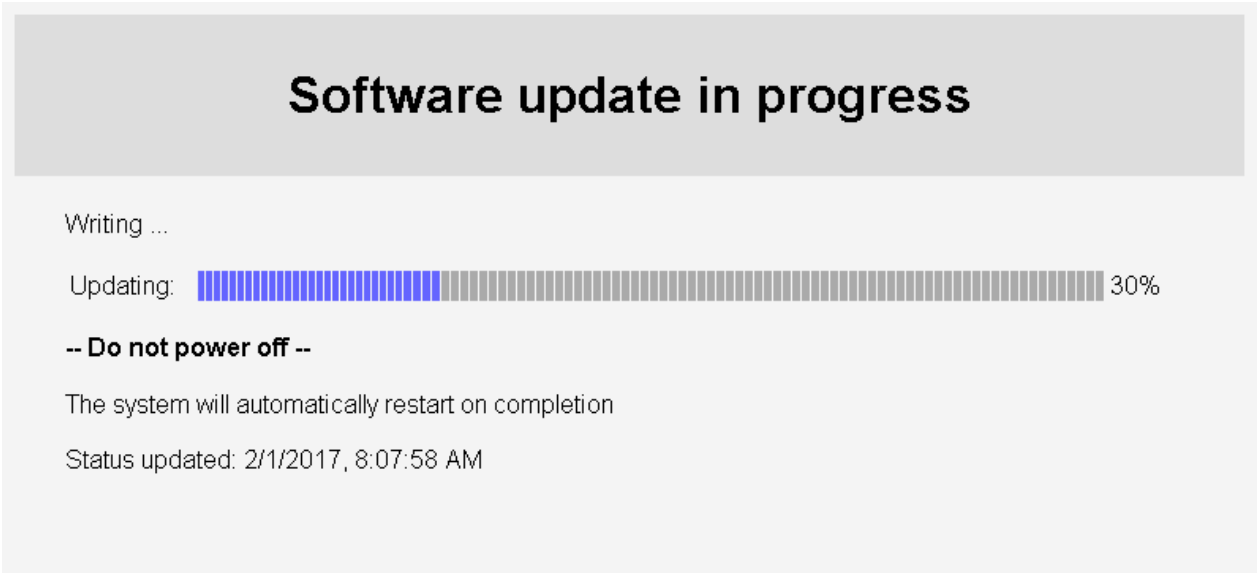
Software upgrade should not alter the probe configuration, however for safety is is a good idea to export the probe configuration (from the **Data — Configuration** view) and save it to a file. Please refer to chapter 5.14.1.

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 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 shell to get a command prompt. If you copied the file as the same user you are logging in as, 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
sudo cp filename.tea /var/opt/btech/probe
sudo /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.

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 system running the probe is not connected to the internet, the software upload progress may in some cases be blocked by the PackageKit software trying to refresh its software package database. If this happens, it is recommended to disable the internet-based package repositories.

To make it possible for the system to receive security and bug fix updates, it is in this case recommended to replace these internet-based package repositories with locally hosted mirrors and update the configuration accordingly. Use the **Software Updates** view in the Cockpit administrative interface.

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:

[1] `https://www.chiark.greenend.org.uk/~sgtatham/putty/`

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

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.