



Test, Measurement, Monitoring and Quality Control



## ENTERPRISE VX1

### Operators Manual

March 2015

v1.6.3

© 2015 Hamlet Video International Ltd. All rights reserved

This handbook contains proprietary information of Hamlet Video International Limited and may not be copied in whole or in part nor its contents disclosed to any third parties without the express written consent of the company.

#### Corporate Head Office

Hamlet Video International Limited.

Maple House, 11 Corinium Business Centre, Raans Road, Amersham, Bucks HP6 6FB England.

Main Line: +44 (0)1494 729 728, Fax Line: +44 (0)1494 723 237, Free phone (UK): 0500 625 525

E-mail: [service@hamlet.co.uk](mailto:service@hamlet.co.uk) Web site: [www.hamlet.co.uk](http://www.hamlet.co.uk)

IN CORRESPONDENCE CONCERNING THIS INSTRUMENT  
PLEASE QUOTE THE SERIAL NUMBER PRINTED ON THE  
LABEL AT THE REAR OF THE UNIT

## Table Of Contents

Table Of Contents .....	2
Table of Figures .....	4
General Information.....	6
Warranty .....	6
Terms and conditions.....	6
Safety compliance .....	6
EMC Compliance .....	6
Product disposal instructions.....	7
Product disposal instructions for business users. ....	7
Hardware Layout.....	8
Introduction .....	9
Highlights .....	9
Software Overview.....	10
System Bar Overview .....	13
Applications.....	14
Video and audio decoding application. ....	14
Audio application. ....	15
Ethernet packet decoder application.....	16
OTT/ABR Analysis application. ....	18
Bit rate Graph application. ....	19
Transport stream table decoder application.....	20
ETR 101 290 application.....	21
Alarms Description.....	21
Web browser application. ....	24
Ping application.....	25
VT100 terminal emulator application (SSH application).....	26
Comm port application. ....	27
Tablet Settings.....	28
Network .....	28
Wireless.....	30
System .....	32
Decoder.....	34
SNMP.....	36
ETR 101 290 .....	38
Browser .....	40
Comms .....	41
Misc.....	43
Operation .....	44
Stream Select .....	44
Decoder Configuration.....	46

# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

Stream Playout.....	47
Screen Brightness.....	48
Quick Start Guide .....	49
Stream Playout and Loop-back .....	49
Appendix A.....	54
Technical Specification .....	54
Appendix B.....	55
Options.....	55
Appendix C.....	56
Berkeley Packet Filter (BPF) syntax .....	56
Appendix D.....	60
Berkeley Packet Filter Examples .....	60
Appendix E .....	61
Useful Websites.....	61
Appendix F .....	61
Contact details and customer support .....	61

## Table of Figures

Figure 1: Hamlet Enterprise VX1 hardware layout .....	8
Figure 2: Initial Start Screen.....	10
Figure 3: Close up of Information Center .....	11
Figure 4: Video player Application.....	14
Figure 5: Audio Bar Application .....	15
Figure 6: Packet Shark Application.....	16
Figure 7: Packet Shark Application - close up of right hand side of screen .....	16
Figure 8: Packet Shark Application - close up of extracted information.....	17
Figure 9: Shark Filter Builder .....	17
Figure 10: OTT Application.....	18
Figure 11: Bitrate Graph.....	19
Figure 12: PID Tree Application.....	20
Figure 13: ETR 101 290 Application .....	21
Figure 14: Web Browser Application .....	24
Figure 15: Smart Ping Application.....	25
Figure 16: SSH Application .....	26
Figure 17: Comm Application .....	27
Figure 18: System Configuration Menu .....	28
Figure 19: Ethernet configuration close up .....	29
Figure 20: Wireless Network Configuration .....	30
Figure 21: Wireless Network Configuration close up .....	30
Figure 22: Available network list close up .....	31
Figure 23: System Configuration .....	32
Figure 24: System update close up .....	32
Figure 25: Image update close up.....	33
Figure 26: Date and Time close up .....	33
Figure 27: Cursor enable close up.....	33
Figure 28: Record option close up .....	33
Figure 29: Screensaver enable close up.....	33
Figure 30: Decoder Configuration.....	34
Figure 31: Stream Reconnect close up .....	34
Figure 32: Speaker setup close up .....	34
Figure 33: De-Interlacer setup close up.....	35
Figure 34: Performance mode setup close up .....	35
Figure 35: SNMP Configuration .....	36
Figure 36: SNMP Configuration close up .....	36
Figure 37: SNMP Trap Configuration close up .....	36
Figure 38: PID Tree Configuration .....	37
Figure 39: Bitrate setup close up .....	37
Figure 40: Tree expand setup close up .....	37
Figure 41: ETR 101 290 Configuration .....	38
Figure 42: Disable alarm close up .....	38

# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

Figure 43: Transport alarm close up .....	39
Figure 44: Browser Configuration .....	40
Figure 45: Browser Configuration close up.....	40
Figure 46: Communications Configuration .....	41
Figure 47: File Transfer Dialog .....	42
Figure 48: Miscellaneous Configuration .....	43
Figure 49: Change logo close up .....	43
Figure 50: Typical operational screen display .....	44
Figure 51: Stream Select Dialog .....	45
Figure 52: Decoder Configuration.....	46
Figure 53: Stream Playout Dialog.....	47
Figure 54: Screen brightness adjustment .....	48

## General Information

### Warranty

This product is manufactured for Hamlet Video International Ltd and is warranted to be free from defects in components and factory workmanship under normal use and service for a period of one year from the date of purchase.

### Terms and conditions

During the warranty period, Hamlet Video International Ltd will undertake to repair or at its option, replace this product at no charge to its owner when failing to perform as specified, provided the unit is returned shipping prepaid, to the factory or authorised service facility.

No other warranty is expressed or implied. Warranty shall not be applicable and be void when this product is subjected to:

1. Repair work or alteration by persons other than those authorised by Hamlet Video International Ltd in such a manner as to injure the performance, stability, reliability or safety of this product.
2. Misuse, negligence, accident, act of God, war or civil insurrection.
3. Connection, installation, adjustment or use otherwise than in accordance with the instructions in this manual.

Hamlet Video International Ltd reserves the right to alter specifications without notice. This warranty does not affect the statutory rights of the UK customer.

### Safety compliance

This product is manufactured and tested to comply with **BS EN 61010-1 : 1993**

Safety requirements for electrical equipment for measurement, control and laboratory use.



### EMC Compliance

We, Hamlet Video International Limited, Maple House, 11 Corinium Business Centre, Raans Road, Amersham, Bucks, HP6 6FB, England, declare under our sole responsibility that the product **Hamlet Enterprise VX1** to which this declaration relates is in conformity with the following standards:

**EN50081-1** Generic emissions standard for light industrial applications.

**EN50082-1** Generic immunity standard for light industrial applications.

Following the provisions of EU EMC directives 89/336/EEC and 92/31/EEC.

**NOTE.** During the EMC certification of this product, shielded cables were used.

We recommend that they be used in operation.

## Product disposal instructions

B2B COMPLIANCE REG NO.  
WEE/GJ0146QT



The symbol shown above and on the Enterprise VX1 means the product is classed as Electrical or Electronic Equipment and should not be disposed with other commercial waste at the end of its working life. The Producer Registration Number above, WEE/GJ0146QT proves that Hamlet are formally registered with a legally approved Compliance Scheme. The Scheme we are registered with is called "B2B Compliance". B2B Compliance takes on the legal responsibilities of the reporting on, and the collection and treatment of, all WEEE that Hamlet Video International Limited is obliged for - and ensures that the appropriate recycling targets are met on this WEEE. The Waste of Electrical and Electronic Equipment (WEEE) Directive (2002/96/EC) has been put in place to recycle products using best available recovery and recycling techniques to minimise the impact on the environment, treat any hazardous substances and avoid the increasing landfill.

## Product disposal instructions for business users.

Business users in the EU should contact their Enterprise VX1 supplier to arrange for its return to Hamlet head office in the UK, who will safely dispose of it and ensure that this Enterprise VX1 is not mixed with other commercial waste for disposal.

## Hardware Layout



Figure 1: Hamlet Enterprise VX1 hardware layout

- Handheld.
- Dimensions 15"w x 8"h x 1.5"d/ 38cm w x 20.3cm h x 3.8cm d.
- Weight 7.1lbs/ 3.2Kg.
- Wi-Fi (802.11b/g/n).
- Dual IP, ASI Input & Output, RF interfaces.
- VESA mountable rack design.
- Ruggedised Aluminium Unibody Construction.



## Introduction

As the broadcast landscape continues to shift into an era where audio and video are readily accessible and streamed onto almost any digital surface, the need for consolidated monitoring and analysis becomes more of necessity to any professional operation. The Hamlet Enterprise series product line of portable stream analyzers have been engineered to provide real-time analysis of streaming IP and ASI based services encoded as MPEG-2, H.264 (MPEG-4 part 10) and many other compression formats. This platform presents an intuitive graphical user touch interface allowing for dynamic configuration with user definable presets developed on a portable and convenient tablet architecture.

## Highlights

- High Resolution integrated video/audio decoder
- Deep IP stream packet interrogation
- Detailed statistics on all PIDs, services and table information
- Quality of Service (QoS) compliancy per TR 101290
- Bitrate view including trending and graphing
- Real time record & playback of captured streams

## Software Overview

The initial boot screen of the Enterprise VX1 is shown in Figure 2. The default operation is four applications visible at one time. The screen is divided into three areas:

1. Application Bar (left hand side) - shows all the available applications
2. System Bar (bottom)
3. Application Display Area (center)

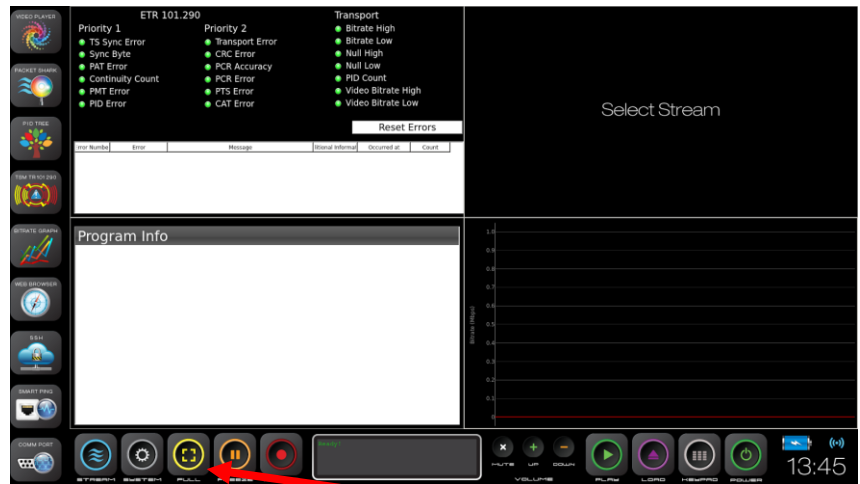


Figure 2: Initial Start Screen

# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

To use an application, or to place it in a different quadrant, press and drag the application icon from the Application Bar into the desired quadrant. When in full screen mode, drag the application to replace the current one.

**Note:** When in quad split mode, the applications are view only. To interact with an application (for example, to scroll through alarm



information), bring the application full screen by selecting the window and pressing



The information center in the bottom center of the system bar (shown in detail in Figure 2) shows the current status of the unit. The first two lines will indicate details on the stream being received. The third line displays stream recording information, while the fourth line displays stream play-out info.

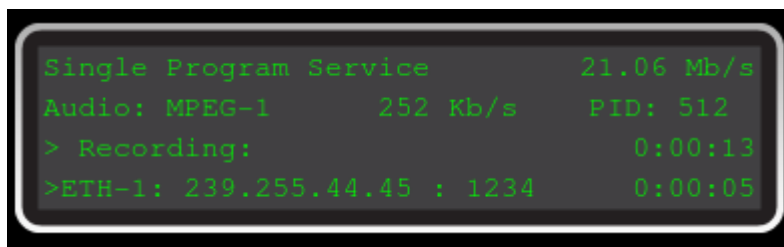
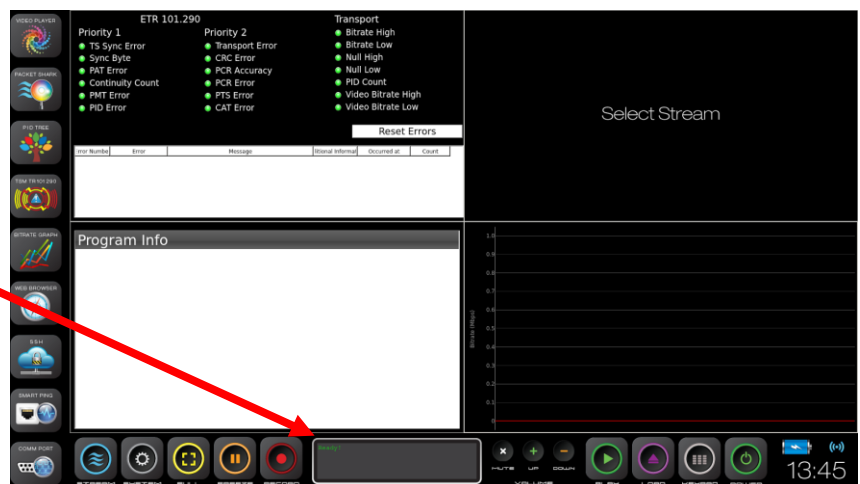




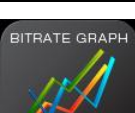




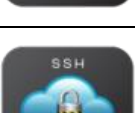


Figure 3: Close up of Information Center

	Video and audio decoding application for the currently selected stream.
	Audio bar level meters for the currently selected stream.
	Ethernet packet decoder, displaying received packet summary and byte displayed.
	OTT/ABR Analysis - HLS, Flash, Silverlight, RTSP and RTP.
	Bitrate view trending and graphing.
	Transport stream table decoder displayed PID in tree structure.
	ETR 101 290 alarm display.
	Simple webkit based web browser.
	Ping application for pinging a single host or a network range.
	SSH utility with VT100 terminal emulator.

## System Bar Overview

	Stream utility used to begin decoding a stream for analysis.
	System utility used for system configuration
	This button is used to switch between quad-split and full screen for the currently selected application
	Record utility is used for Transport Stream capture
	Play utility is used to playout a Transport Stream
	Load utility is used for decoder configuration
	Keyboard utility is used for keyboard display
	Power button used to power OFF or restart the tablet. Press for two seconds to bring up the power down screen.

## Applications

### Video and audio decoding application.



*Figure 4: Video player Application*

High-Res: 1080p video decoder.

Viewing Size: 11.6" / 16:9.

Resolution: True 1080P/60 1920x1080.

HEVC, H.264, MPEG-2 decoding.

Real time record & playback of streams.

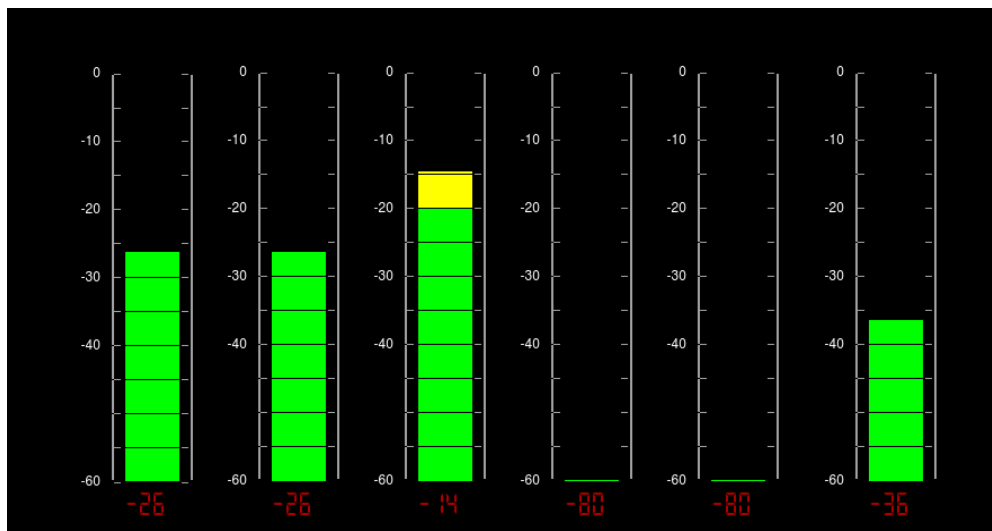
Playback of recordings to prove service faults.

Allows visual monitoring of video streams.

Can record the video - store on internal disc for play out at a later date.

The Video Player application is a full decode of a program in the selected transport stream. The application has no user interaction. To change the video or audio program being decoded, use the Decoder Configuration as outlined on page 46.

## Audio application.



*Figure 5: Audio Bar Application*

Allows visual monitoring of multi channel audio streams.  
The audio can be decoded to optional headphones.  
Peak levels are shown numerically.

The Audio Bar application is a visual representation of the decoded audio program. It will show from one to six audio bars depending on the audio program being decoded (from mono to Dolby AC3 5.1). It is set to the IEC 60268-18 standard. The channels mappings are Left, Right, Center, Low-Frequency, Left Surround, Right Surround. To change the audio program being monitored, use the Decoder Configuration as outlined on page 46.

## Ethernet packet decoder application.

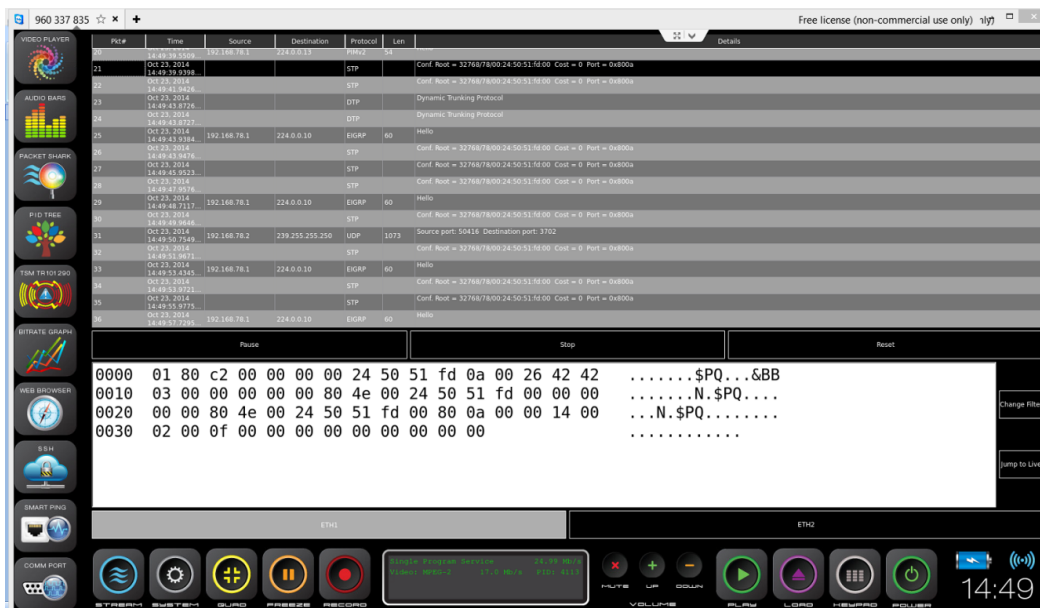
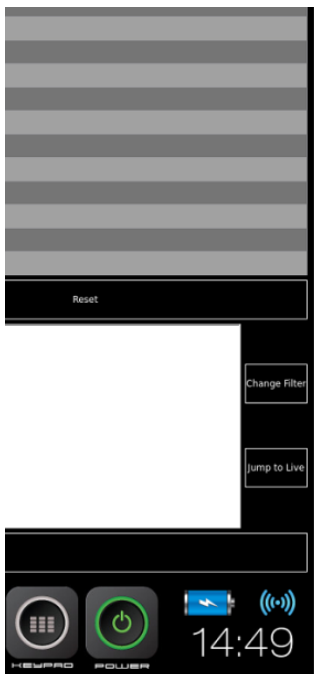


Figure 6: Packet Shark Application

Used to view detailed information on every Ethernet packet that comes into the Enterprise. The Packet Shark application is used capture live IP packet data from the network interfaces.

**Note:** This application is best view in Full screen mode



The following steps describe how to use the packet shark application:

Drag and drop the Packet Shark  application into the application viewing area.

Previous packet history can be seen by swiping down on the packet table. To return to live update mode, select '**Jump to Live**' on the bottom right.

To filter out incoming Ethernet traffic, select the '**Change Filter**' button and use the drag and drop interface dialog to construct a new packet filter, as seen in Figure 8.

Figure 7: Packet Shark Application - close up of right hand side of screen



Pkt#	Time	Source	Destination	Protocol	Len	
20	Oct 23, 2014 14:49:39.5509...	192.168.78.1	224.0.0.13	PMIPv2	54	
21	Oct 23, 2014 14:49:39.9398...			STP		Conf. Root = 32768/78/00:24:50:51:fd:00 Cost = 0 Port = 0x800a
22	Oct 23, 2014 14:49:41.9426...			STP		Conf. Root = 32768/78/00:24:50:51:fd:00 Cost = 0 Port = 0x800a
23	Oct 23, 2014 14:49:43.8726...			DTP		Dynamic Trunking Protocol
24	Oct 23, 2014 14:49:43.8727...			DTP		Dynamic Trunking Protocol
25	Oct 23, 2014 14:49:43.9384...	192.168.78.1	224.0.0.10	EIGRP	60	Hello
26	Oct 23, 2014 14:49:43.9476...			STP		Conf. Root = 32768/78/00:24:50:51:fd:00 Cost = 0 Port = 0x800a
27	Oct 23, 2014 14:49:45.9523...			STP		Conf. Root = 32768/78/00:24:50:51:fd:00 Cost = 0 Port = 0x800a

Figure 8: Packet Shark Application - close up of extracted information

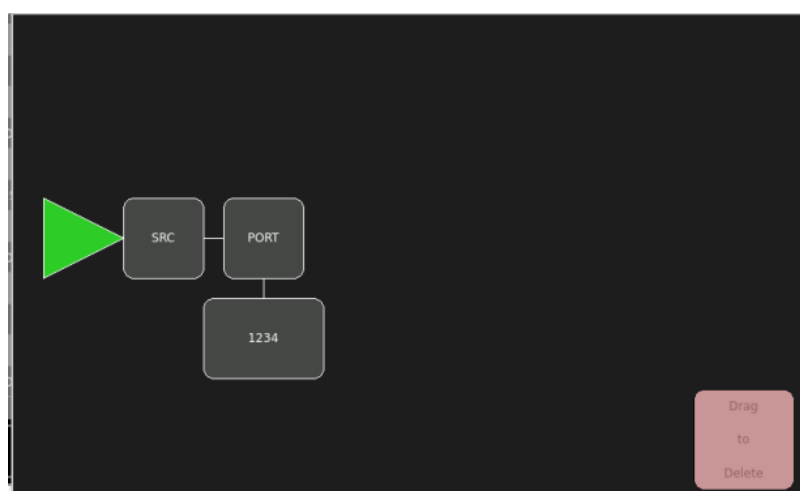


Figure 9: Shark Filter Builder

To construct a filter, drag the filter elements at the bottom into an available slot. Filter elements will only snap into place if they are a valid part of the chain. To remove an unwanted filter element, drag

it to the 'Drag to Delete' portion of the canvass.

**Example:** The filter constructed in **Figure 8** will capture packets with Source Port 1234 only.

The Boolean expressions AND, OR and NOT will allow complex chains to be built. The filter syntax is based off the Berkeley Packet Filter (BPF) syntax See Appendix C for more information.

# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

## OTT/ABR Analysis application.

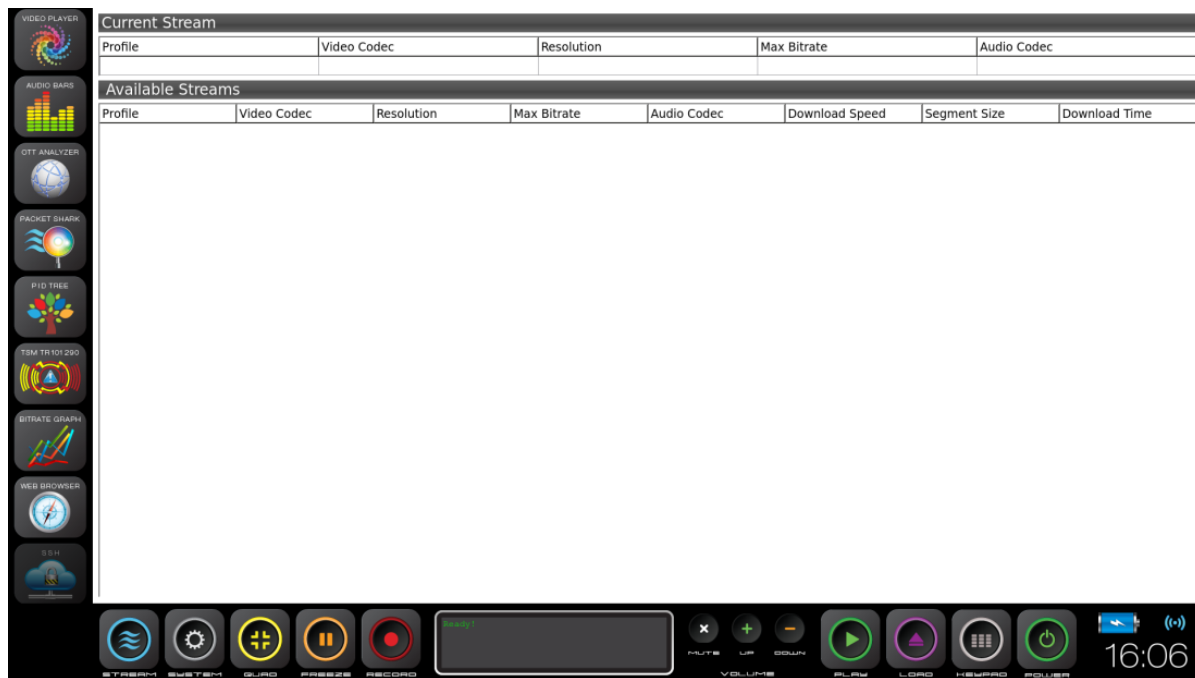


Figure 10: OTT Application

OTT - Over the Top.

ABR - Adaptive Bit Rate.

HLS, Flash, Silverlight, RTSP and RTP.

Monitoring of manifest files and chunks.

For OTT analysis, The Enterprise analyse and verify the manifest file, and then parse the manifest file and compare profiles to actual contents. The Enterprise compare the advertised bitrate to the measured content and download rate, as well as the resolution and any other details if they are present. The Enterprise do monitoring on the base TCP/IP layer to log and indicate any problems with the link, including reconnecting attempts and excessive hops.

Analysis:

- Segment bitrate and comparison of downloading time vs. media time
- Analyze playlist files and monitor segment downloading
- Comparison of manifest file to actual content format

## Bit rate Graph application.



*Figure 11: Bitrate Graph*

Bitrate view trending and graphing.

## Transport stream table decoder application.

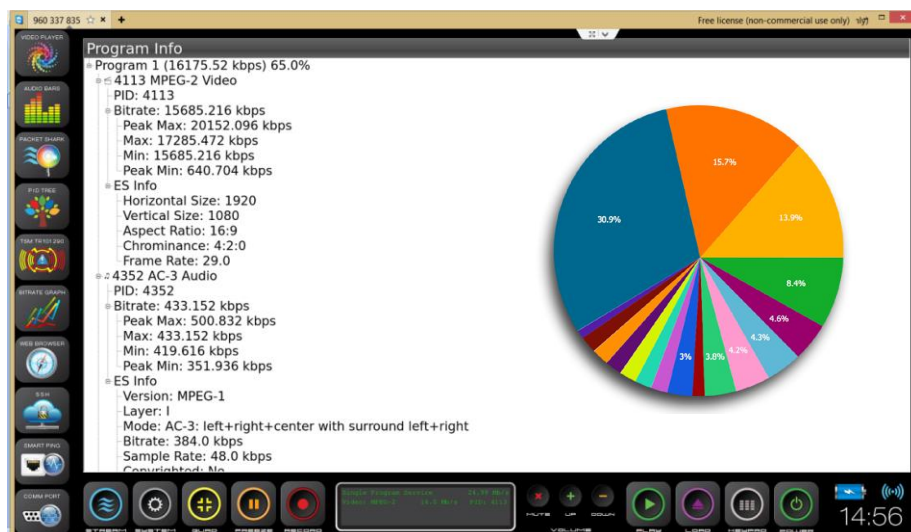


Figure 12: PID Tree Application

Detailed statistics on PIDS, services and tables with pie chart graphing.

Each program is colour coded to the pie chart - click on program in tree to see the colour

## ETR 101 290 application.

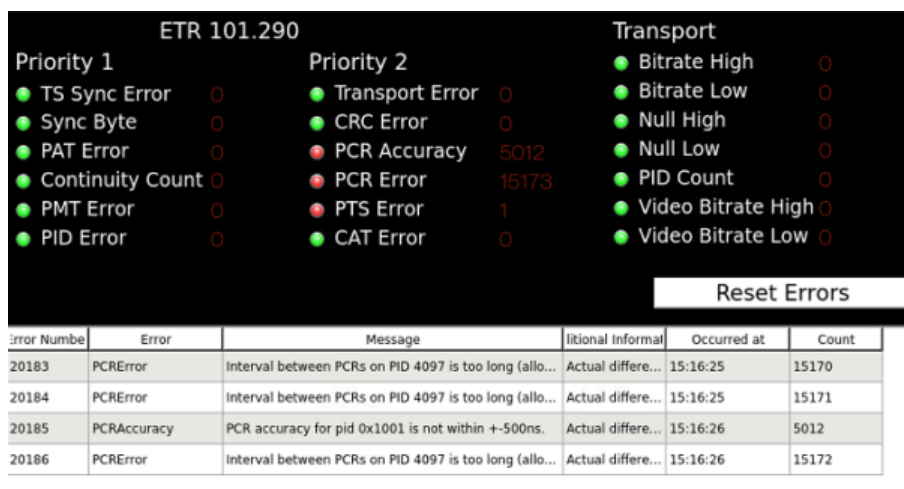


Figure 13: ETR 101 290 Application

Quality of Service (QoS) per TR 101290.

- No priority 3 monitoring

Green LED means no errors since start or Reset button pressed

Red LED means errors detected since start or Reset button pressed

Can only scroll through the list of errors in full screen mode

## Alarms Description

### TS Sync Error

The most important function for the evaluation of data from the MPEG-2 TS is the sync acquisition. The actual synchronization of the TS depends on the number of correct sync bytes necessary for the device to synchronize and on the number of distorted sync bytes which the device can not cope with. It is proposed that five consecutive correct sync bytes (ISO/IEC 13818-1 [1], clause G.01) should be sufficient for sync acquisition, and two or more consecutive corrupted sync bytes should indicate sync loss.

**Note:** After synchronization has been achieved the evaluation of the other parameters can be carried out.

### Sync Byte

The indicator "**Sync Byte**" is set as soon as the correct sync byte (0x47) does not appear after 188 or 204 bytes. This is fundamental because this structure is used throughout the channel encoder and decoder chains for synchronization. It is also important that every sync byte is checked for correctness since the encoders may not necessarily check the sync byte. Apparently some encoders use the sync byte flag signal on the parallel interface to control randomizer re-seeding and byte inversion without checking that the corresponding byte is a valid sync byte.

## **PAT Error**

The Program Association Table (PAT), which only appears in PID 0x0000 packets, tells the decoder what programs are in the TS and points to the Program Map Tables (PMT) which in turn point to the component video, audio and data streams that make up the program. If the PAT is missing then the decoder can do nothing, no program is decodable. Nothing other than a PAT should be contained in a PID 0x0000.

## **Continuity Count Error**

For this indicator three checks are combined. The preconditions "Incorrect packet order" and "Lost packet" could cause problems for IRD which are not equipped with additional buffer storage and intelligence. It is not necessary for the test equipment to distinguish between these two preconditions as they are logically OR-ed, together with the third precondition, into one indicator. The latter is also covering the packet loss that may occur on ATM links, where one lost ATM packet would cause the loss of a complete MPEG-2 packet. The precondition "a packet occurs more than twice" may be symptomatic of a deeper problem that the service provider would like to keep under observation.

## **PMT Error**

The Program Association Table (PAT) tells the decoder how many programs there are in the stream and points to the PMTs which contain the information where the parts for any given event can be found. Parts in this context are the video stream (normally one) and the audio streams and the data stream (e.g. Teletext). Without a PMT the corresponding program is not decodable.

## **PID Error**

It is checked whether there exists a data stream for each PID that occurs. This error might occur where TS are multiplexed, or demultiplexed and again remultiplexed.

## **Transport Error**

The primary Transport Error indicator is Boolean, but there should also be a re-settable binary counter which counts the erroneous TS packets. This counter is intended for statistical evaluation of the errors. If an error occurs, no further error indication should be derived from the erroneous packet.

## **CRC Error**

The CRC check for the CAT, PAT, PMT, NIT, EIT, BAT, SDT and TOT indicates whether the content of the corresponding table is corrupted. In this case no further error indication should be derived from the content of the corresponding table.

## **PCR Accuracy**

Error is triggered if the PCR accuracy of a selected program is not within  $\pm 500$  ns.

## **PCR Error**

The PCRs are used to re-generate the local 27 MHz system clock. If the PCR do not arrive with sufficient regularity then this clock may jitter or drift. The receiver/decoder may even go out of lock. A repetition period of not more than 40 ms is recommended.

## **PTS Error**

The Presentation Time Stamps (PTS) should occur at least every 700 ms. The PTS is only accessible if the TS is not scrambled.

## **CAT Error**

The Conditional Access Table(CAT) Error is the pointer to enable the IRD to find the EMMs associated with the conditional Access(CA) system(s) that it uses. If the CAT is not present, the receiver is not able to receive management messages.

## **Bitrate High**

This alarm is triggered is the overall transport stream bitrate exceed the value set by the user in the **“Transport Alarm Settings”** section

## **Bitrate Low**

This alarm is triggered is the overall transport stream bitrate drops below the value set by the user in the **“Transport Alarm Settings”** section

## **Null High**

This alarm is triggered is the null packets bitrate exceed the value set by the user in the **“Transport Alarm Settings”** section

## **Null Low**

This alarm is triggered is the null packets bitrate drops below the value set by the user in the **“Transport Alarm Settings”** section

## **Video Bitrate High**

This alarm is triggered if the **Program Bit Rate** (Video PID) bitrate exceed the value set in the **“Transport Alarm Settings”** section

## **Video Bitrate Low**

This alarm is triggered if the **Program Bit Rate** (Video PID) bitrate drops below the value set in the **“Transport Alarm Settings”** section

## **PID Count**

This alarm is triggered if the total PID count within a transport stream doesn't match the value set in the **“Transport Alarm Setting”** section

## Web browser application.



Figure 14: Web Browser Application

Simple web browser for looking out on to the world wide web. Not flash enabled

Based on WebKit which is an open source web browser engine.

WebKit is a layout engine software component for rendering web pages in web browsers. It powers Apple's Safari web browser and a fork of the project is used in Google's Chrome web browser. By September 2013, WebKit browser market share was larger than that of both the Trident engine used by Internet Explorer and the Gecko engine used by Firefox.



## Ping application.

Host IP: 127 0 0 1 Timeout(s): 1 **PING**

Interface: wlan0 Count: 1 **STOP**

**Ping a Network:**

Start IP: 127 0 0 1 **PING**

End IP: 127 0 0 2 **CLEAR**

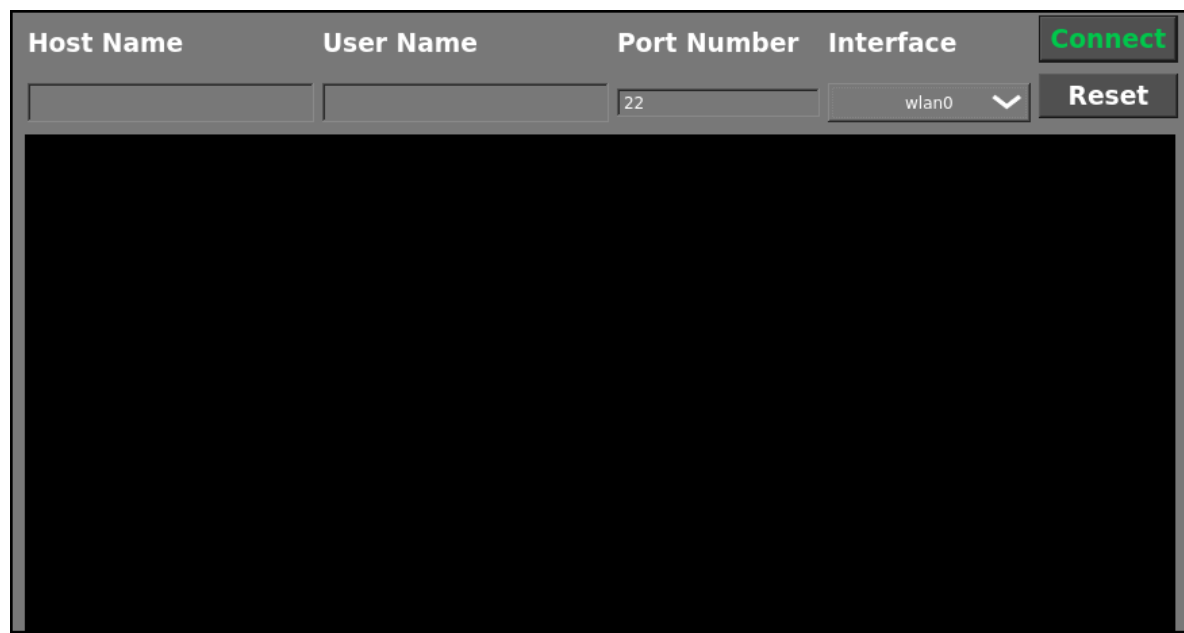
SUCCESS

Figure 15: Smart Ping Application

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. The name comes from active sonar terminology which sends a pulse of sound and listens for the echo to detect objects underwater.

Ping operates by sending Internet Control Message Protocol (ICMP) *echo request* packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (*round-trip time*) and records any packet loss. The results of the test are printed in the form of a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times, and sometimes the standard deviation of the mean.

## VT100 terminal emulator application (SSH application).



The screenshot shows the Hamlet Enterprise VT100 terminal emulator application interface. It features a header bar with four input fields: 'Host Name', 'User Name', 'Port Number', and 'Interface'. The 'Port Number' field is pre-filled with '22', and the 'Interface' field is set to 'wlan0' with a dropdown arrow. To the right of these fields are two buttons: 'Connect' (highlighted in green) and 'Reset'. Below the header bar is a large, empty black rectangular area representing the terminal screen.

*Figure 16: SSH Application*

The VT100 is a video terminal that was made by Digital Equipment Corporation (DEC). Its detailed attributes became the de facto standard for terminal emulators to emulate.

The VT100 is a simple device to operate. The terminal is basically a typewriter that uses a video screen instead of paper and communicates with a computer. If you can operate a typewriter, you can operate a VT100.

## Comm port application.



*Figure 17: Comm Application*

Simple RS232 communication interface

## Tablet Settings



To access tablet settings press **System**, the window in Figure 17 will appear:

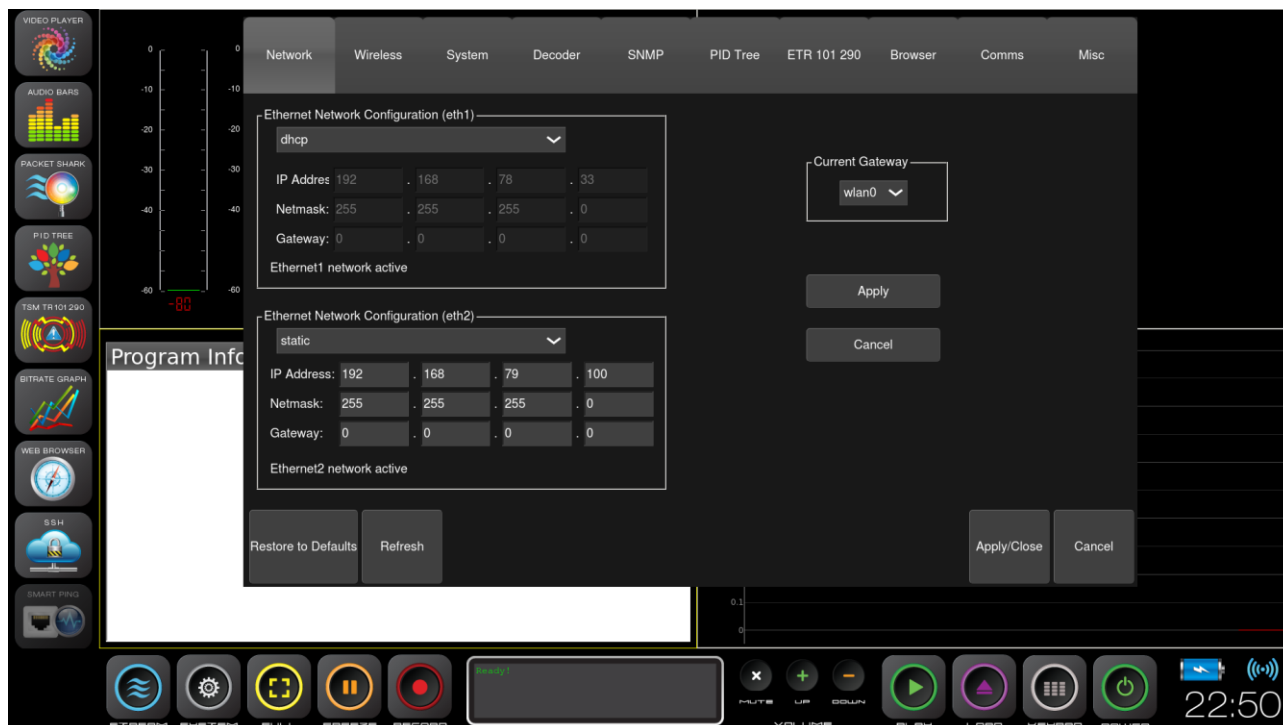


Figure 18: System Configuration Menu

Below is a description of each of the **System** tabs.

## Network

Use this tab to specify the physical IP address of Ethernet ports number 1 & 2

**Important:** Ethernet Port(s) must be configured prior to stream capture and analysis

1. Enter the Configuration menu System by pressing
2. Select the **Network** tab

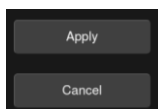


3. Enter in the network settings for Ethernet port 1 and/or 2

The image shows two network configuration panels. The top panel is for 'Ethernet Network Configuration (eth1)' and has a dropdown menu set to 'dhcp'. Below it are input fields for IP Address (192, 168, 78, 33), Netmask (255, 255, 255, 0), and Gateway (0, 0, 0, 0). A status bar at the bottom says 'Ethernet1 network active'. The bottom panel is for 'Ethernet Network Configuration (eth2)' and has a dropdown menu set to 'static'. Below it are input fields for IP Address (192, 168, 79, 100), Netmask (255, 255, 255, 0), and Gateway (0, 0, 0, 0). A status bar at the bottom says 'Ethernet2 network active'.

Figure 19: Ethernet configuration close up

4. Select Apply button on the right side.



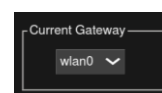
**Note:** If using DHCP, select refresh to see the network configuration that was applied.

5. Connect an Ethernet cable to the each Ethernet port and confirm the connection with activity LED's lit up.

6. Select apply to exit the System Configuration dialog.



The global device gateway can be selected here in the Current Gateway drop-down.



## Wireless

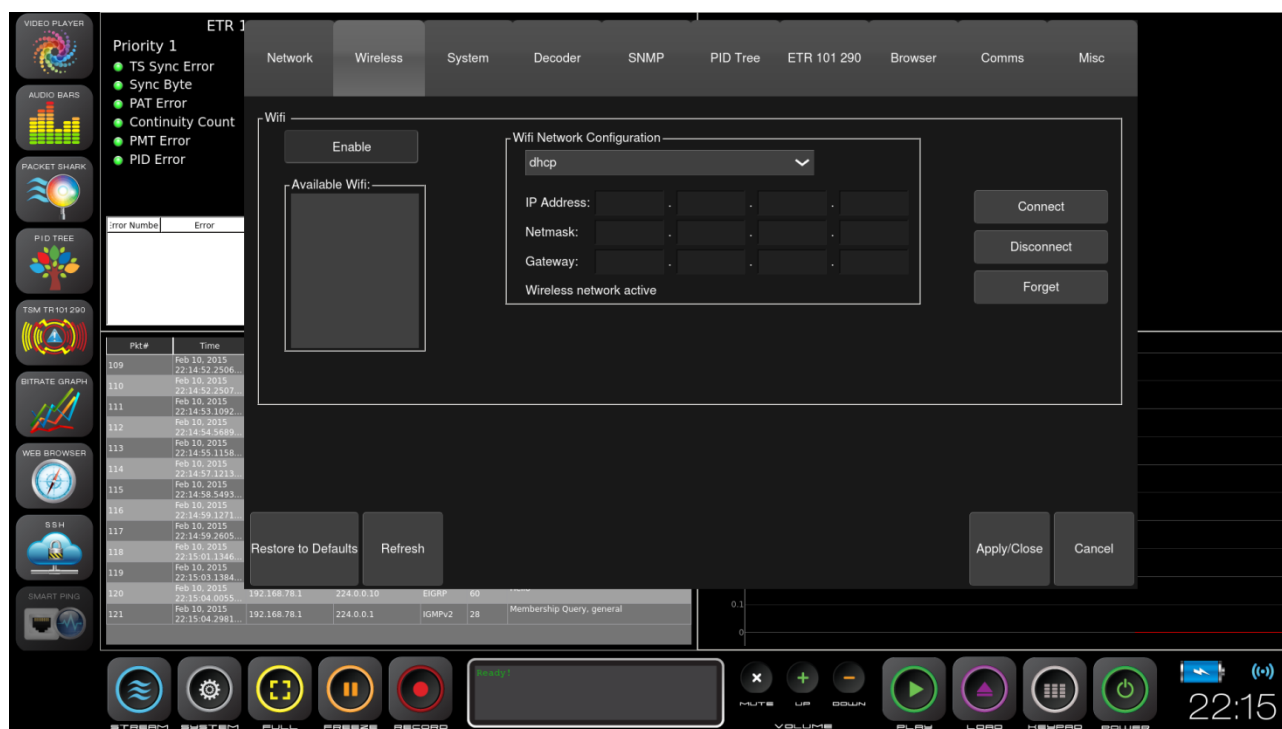


Figure 20: Wireless Network Configuration

Use this tab to enable and select a wireless network.

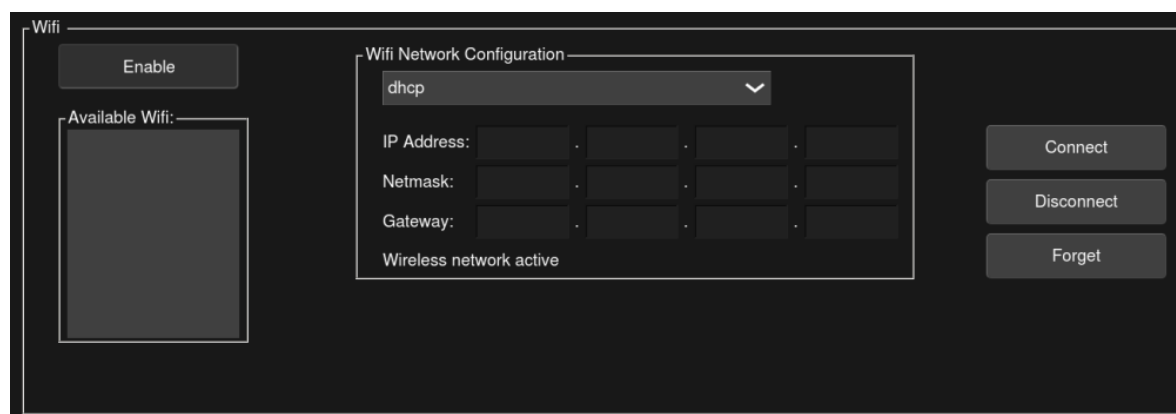
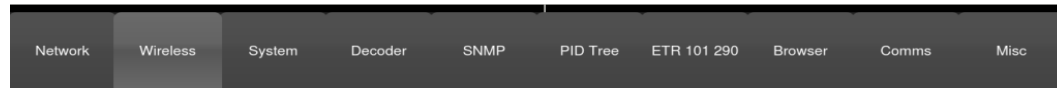


Figure 21: Wireless Network Configuration close up

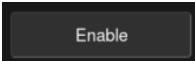
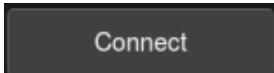

When enabled,  any available wireless networks will be listed in the 'Available WiFi' area.



Figure 22: Available network list close up

Select the desired network, and press the Connect button.  If needed, a password/key dialog will open to connect.

When connected to a WiFi network a wireless icon will be shown on the main screen 



# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

## System

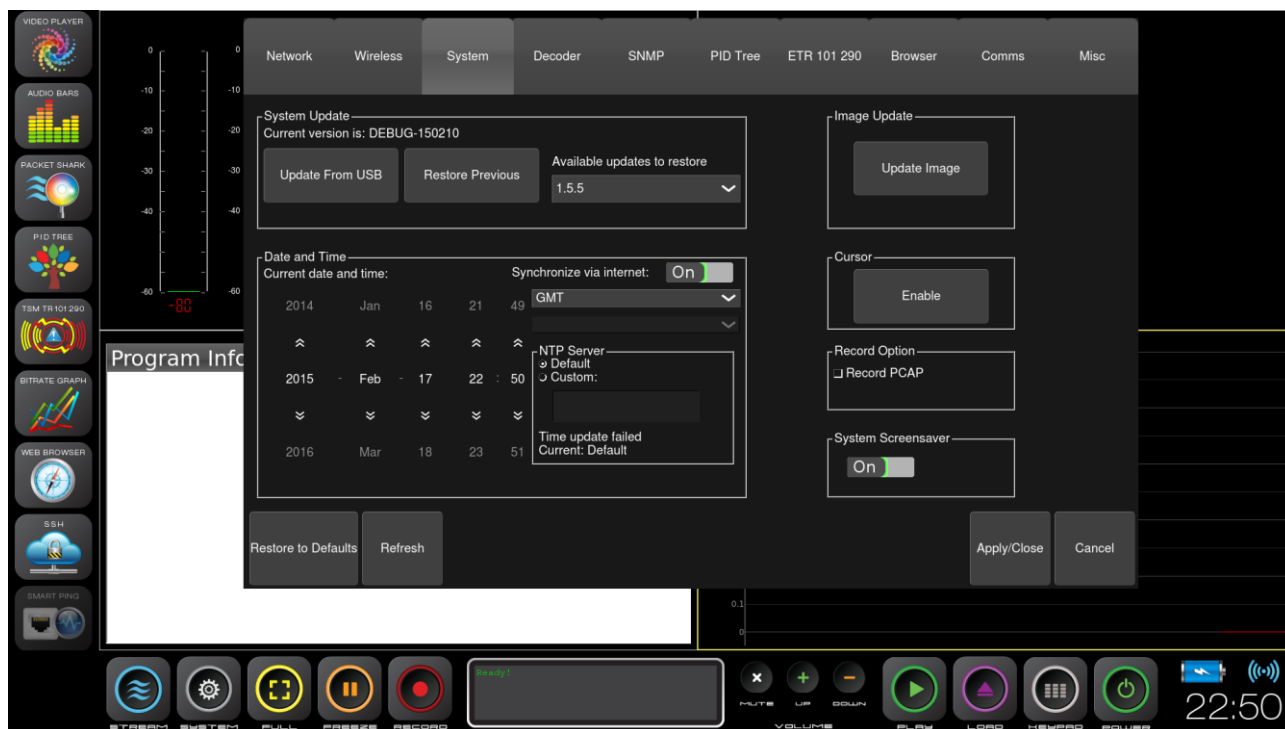
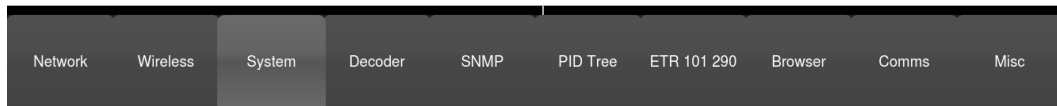


Figure 23: System Configuration



**System Update:** To upgrade the unit, insert a USB stick containing the upgrade file, select 'Update from USB' and choose the file from the file selection dialog. To roll-back to a previously installed version, select 'Restore Previous'.

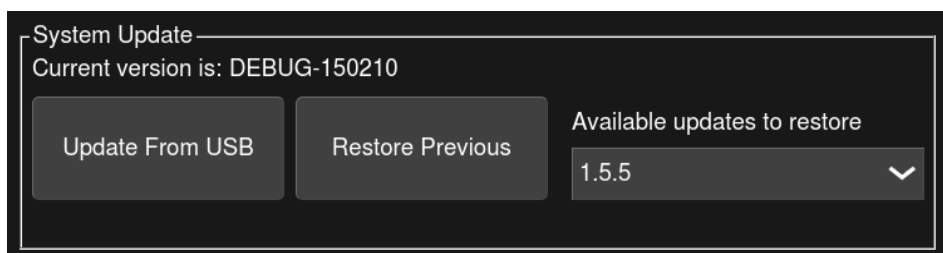


Figure 24: System update close up



# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

**Image Update:** To apply a system image update, insert a USB stick containing the update file, select 'Update Image' and choose the file from the file selection dialog

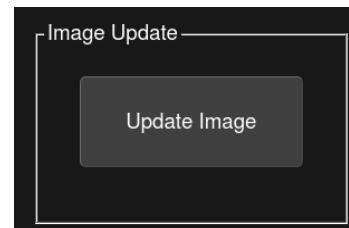


Figure 25: Image update close up

**Date and Time:** Used to set the data and time of the unit. To synchronize via an online NTP server, select 'Synchronize via Internet' to ON. Turn OFF to set the date and time manually using the touch sliders. The Time Zone can be set using the drop down selections.

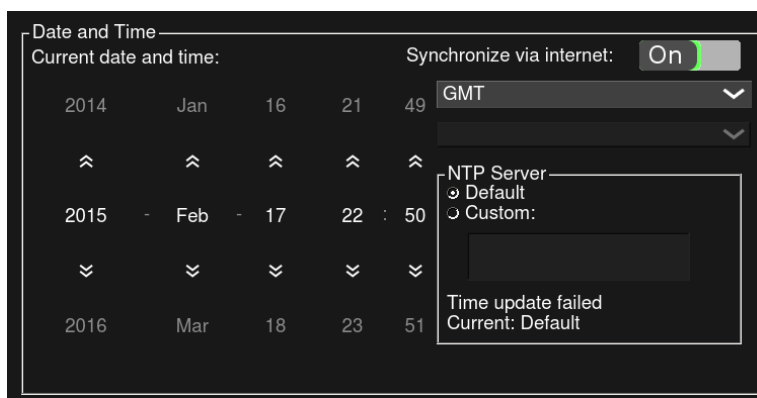


Figure 26: Date and Time close up

To reach a local or custom NTP server, select Custom and enter the URL or IP address of the desired NTP server.

The last successful connection will be displayed below the Custom NTP server entry field.

**Cursor:** An on-screen cursor can be enabled/disabled.



Figure 27: Cursor enable close up

**Record Option:** By default, when recording a stream the Transport Stream will be recorded. To record the raw Ethernet packets for an IP stream, select 'Record PCAP'

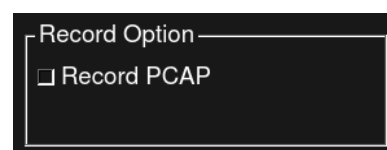


Figure 28: Record option close up

**System Screensaver:** By default, if no stream is playing the screen will turn off after 10 minutes of activity. Select Off to disable this screensaver.

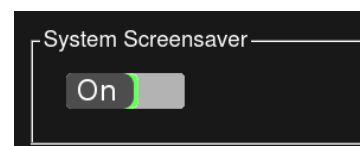


Figure 29: Screensaver enable close up

## Decoder

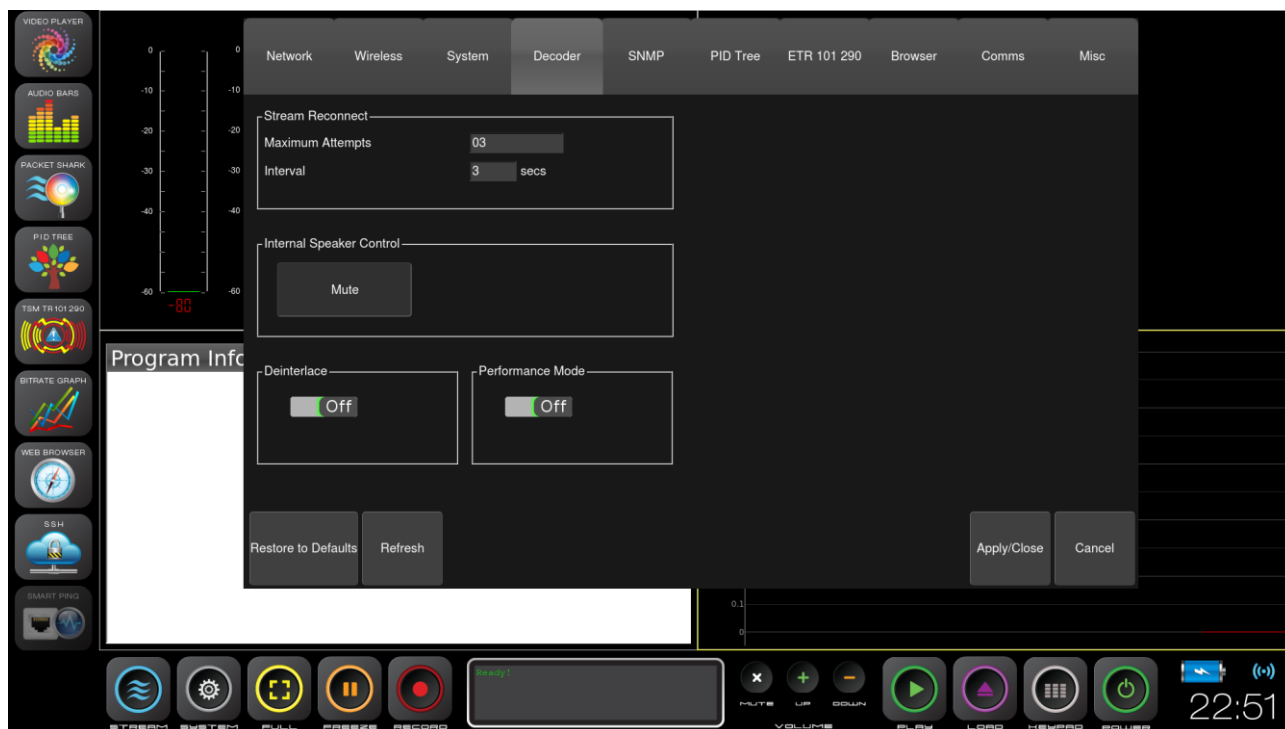
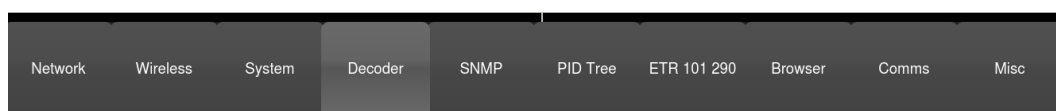


Figure 30: Decoder Configuration



### Stream Reconnect

Specifies the parameters for when the device cannot connect to a stream.

**Maximum Attempts:** Specifies how many attempts the device will make to connect to a stream.

**Intervals:** Specifies the time in between reconnecting attempts.

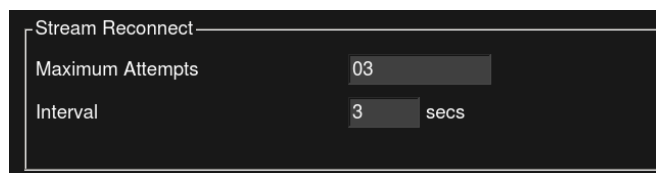


Figure 31: Stream Reconnect close up

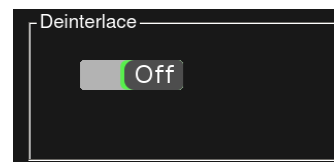
**Internal Speaker Control:** This setting will enable or disable the internal speaker. This does not affect the headphone out.



Figure 32: Speaker setup close up

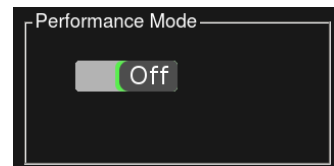
# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

**De-Interlace:** This setting will enable or disable the decoder de-interlacer.



*Figure 33: De-Interlacer setup close up*

**Performance Mode:** When enabled, the device will be able to decode high quality H.264 422 10-bit streams. This mode may cause some instability in the device.



*Figure 34: Performance mode setup close up*

## SNMP

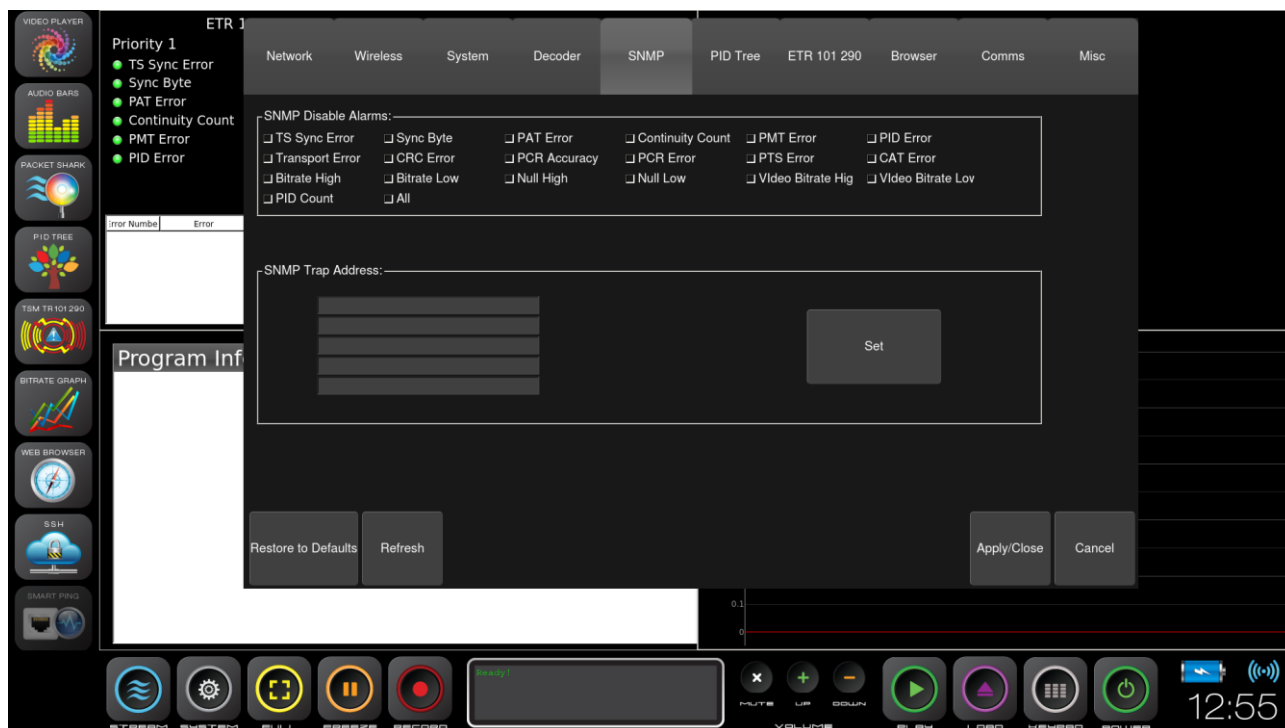
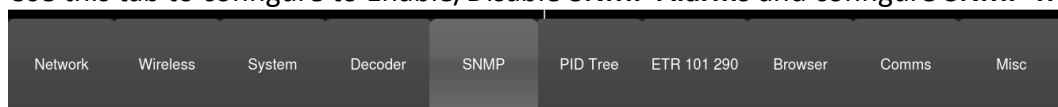


Figure 35: SNMP Configuration

Use this tab to configure to Enable/Disable **SNMP Alarms** and configure **SNMP Trap Address**



**SNMP Disable Alarms:** To enable an SNMP alarm checkmark the box to the left of the alarm. To disable an alarm uncheck the box to the left of the alarm.

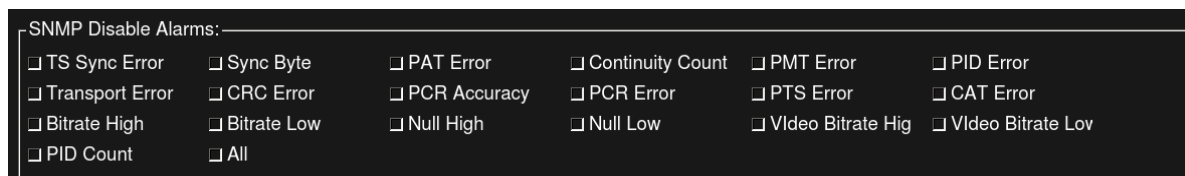


Figure 36: SNMP Configuration close up

**SNMP Trap Address:** To set an SNMP trap destination enter a trap(s) destination IP address in the field(s) below then click **Set**

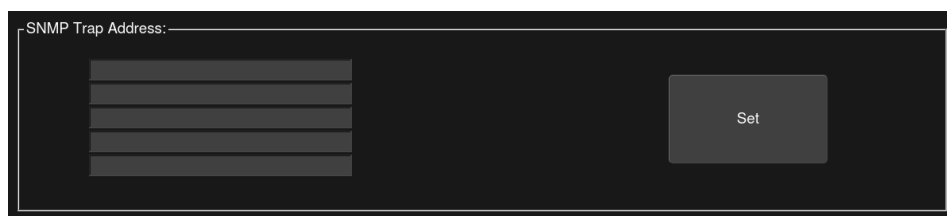


Figure 37: SNMP Trap Configuration close up

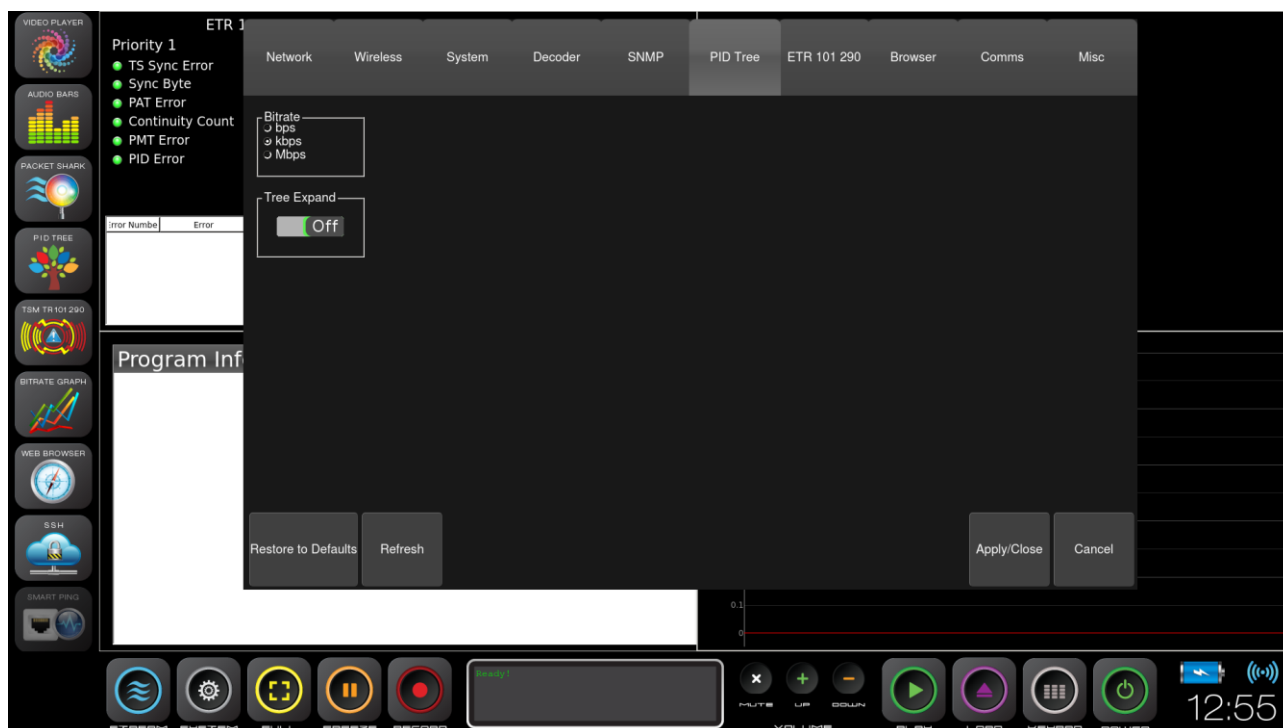


Figure 38: PID Tree Configuration

Use this tab to set the PID Tree viewing preferences



**Bitrate:** Specify how to view the bitrate associated with each PID

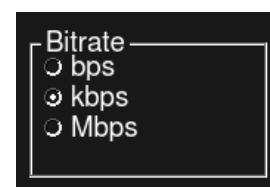


Figure 39: Bitrate setup close up

**Tree Expand:** Specifies whether the tree app will open with all nodes expanded or collapsed.

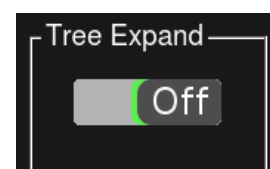


Figure 40: Tree expand setup close up

## ETR 101 290

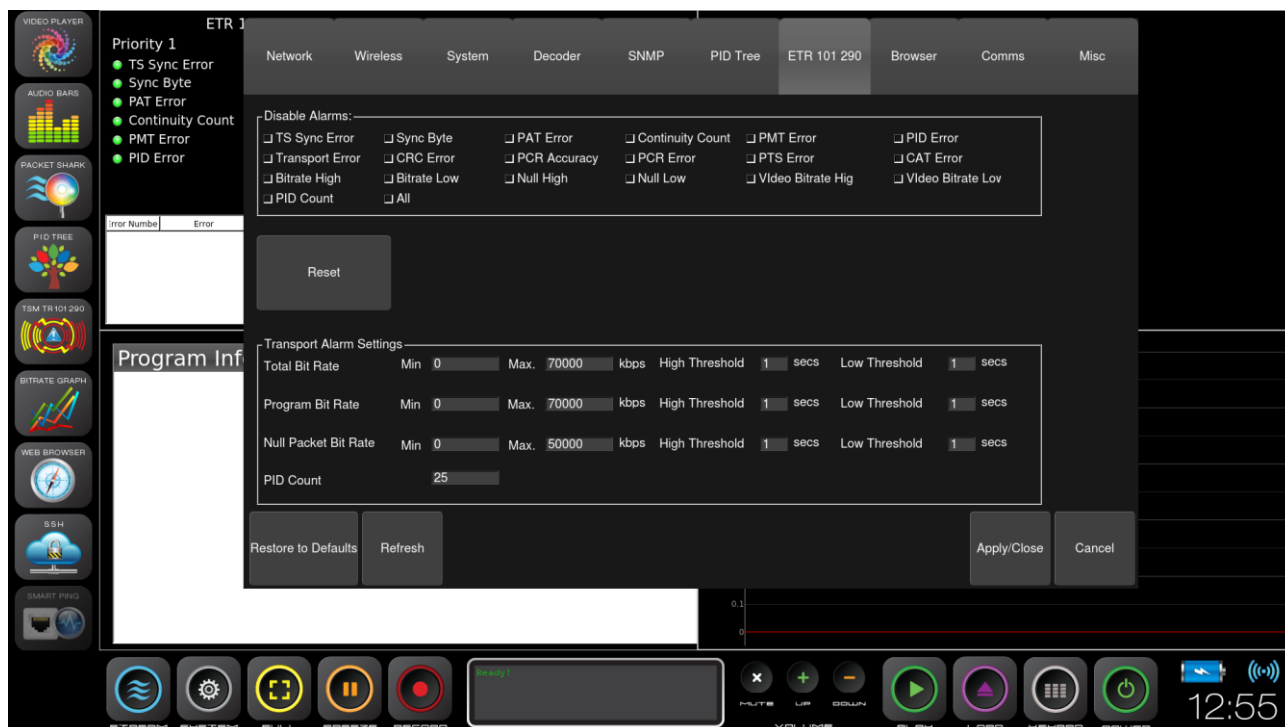


Figure 41: ETR 101 290 Configuration

Use this tab to set the parameters that you want the analyzer to track and alarm for when a fault is detected



**Disable Alarms:** To enable an alarm checkmark the box to the left of the alarm. To disable an alarm uncheck the box to the left of the alarm.

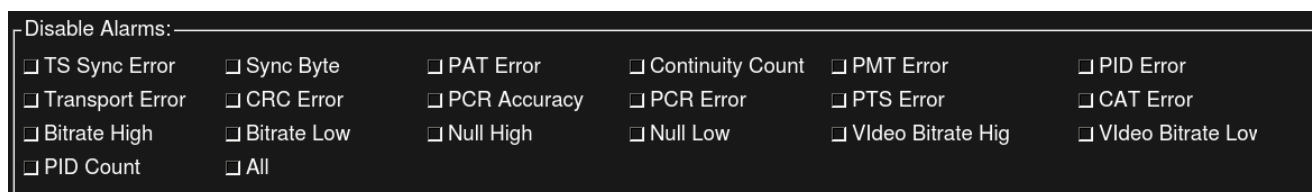


Figure 42: Disable alarm close up

## Transport Alarm Settings: Custom settings for the transport alarms

Transport Alarm Settings						
Total Bit Rate	Min	<input type="text" value="0"/>	Max.	<input type="text" value="70000"/>	kbps	High Threshold <input type="text" value="1"/> secs Low Threshold <input type="text" value="1"/> secs
Program Bit Rate	Min	<input type="text" value="0"/>	Max.	<input type="text" value="70000"/>	kbps	High Threshold <input type="text" value="1"/> secs Low Threshold <input type="text" value="1"/> secs
Null Packet Bit Rate	Min	<input type="text" value="0"/>	Max.	<input type="text" value="50000"/>	kbps	High Threshold <input type="text" value="1"/> secs Low Threshold <input type="text" value="1"/> secs
PID Count		<input type="text" value="25"/>				

Figure 43: Transport alarm close up

**Total Bit Rate:** Specifies the alarm conditions for the total transport bitrate

**Program Bit Rate:** Specifies the alarm conditions for the video program currently being decoded

**Null Packet Bit Rate:** Specifies the alarm conditions for the null packets of the transport stream

**PID Count:** Specifies the expected total number of PIDs within the Transport Stream

## Browser

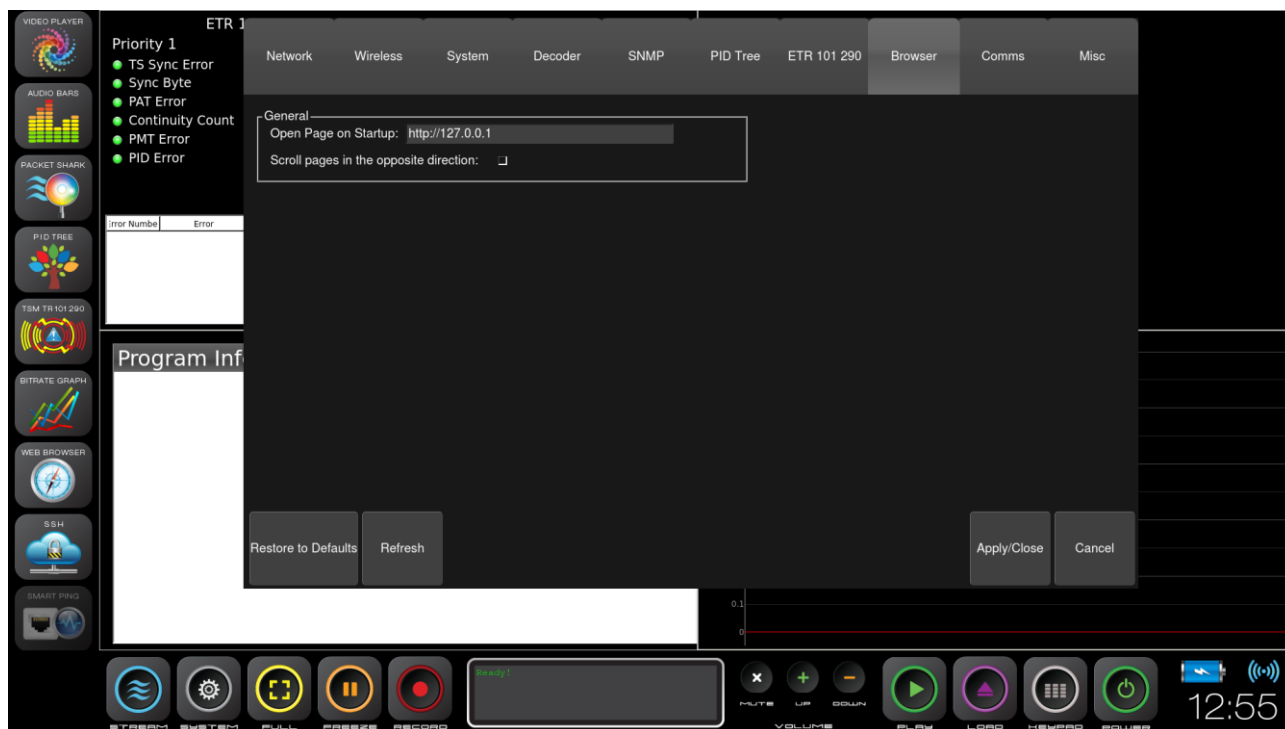


Figure 44: Browser Configuration

Use this tab to set your **Browser** general preferences

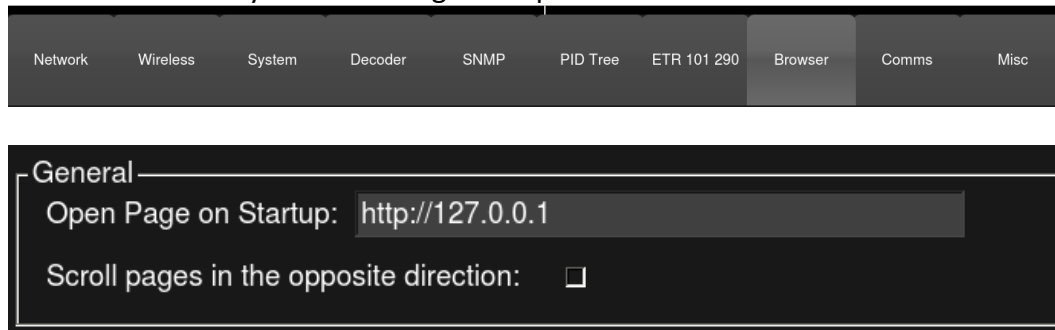


Figure 45: Browser Configuration close up

**Open Page on Start-up:** Set the address of your browser's start-up page (http://127.0.0.1 in this case)

**Scroll pages in the opposite direction:** When enabled, the scroll gesture will move the page in the opposite direction. Place checkmark in box to right of text to enable.



## Comms

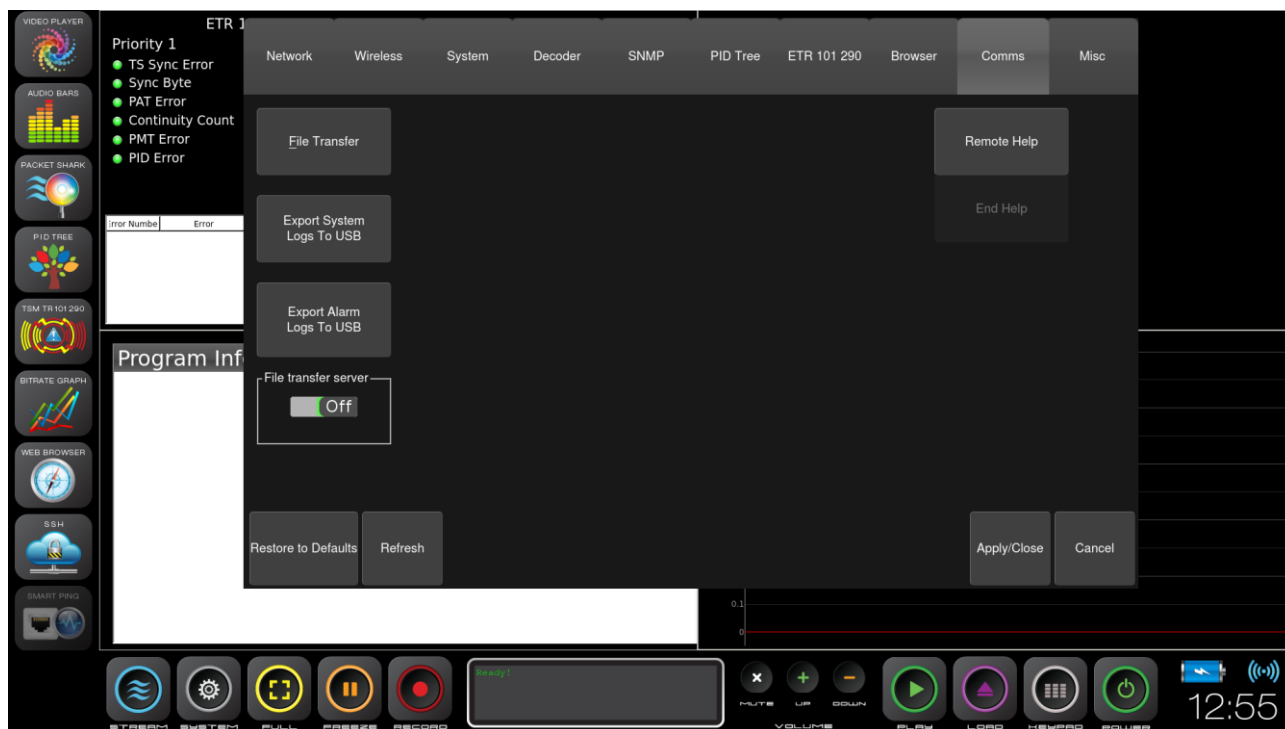
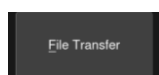
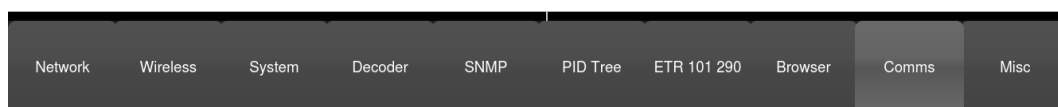


Figure 46: Communications Configuration



**File Transfer:** Opens a file dialogue for file transfer from/to a USB key, as shown in **Error! Reference source not found..** To transfer a file, drag and drop the icon. There is a progress indicator at the bottom that shows the transfer status. This dialog can be closed without interrupting the file transfer.

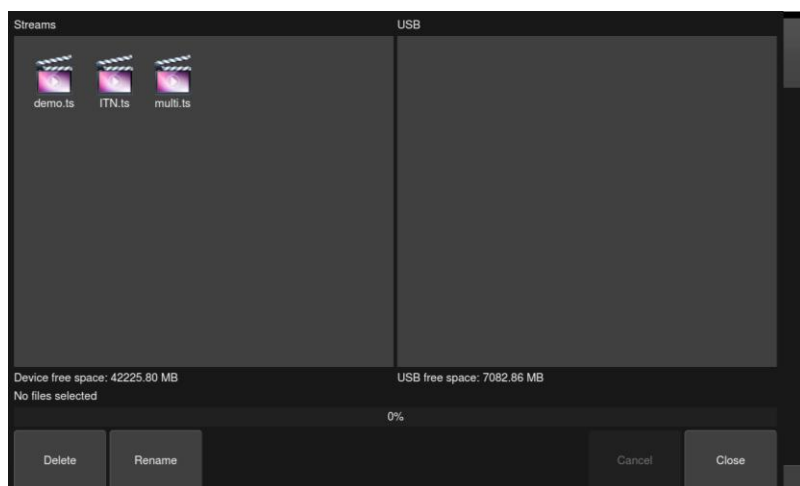
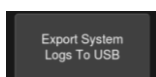
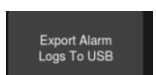


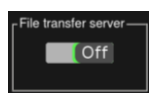
Figure 47: File Transfer Dialog



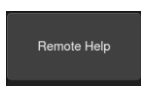
**Export System Logs to USB:** Exports system diagnostic information to a USB key, when requested by support personnel.



**Export Alarm Logs to USB:** Exports the ETR 101 290 alarm database to a USB key.



**File Transfer Server:** When enabled, the device acts as a file server at port 5000 on the WiFi address for accessing files. (i.e. if the device is set to IP Address 192.168.77.100, it can be reached at <http://192.168.77.100:5000>).



**Remote Help:** When the device is connected to the Internet via WiFi, Remote Help will securely connect to a remote help server for allowing service personnel to collect diagnostic information.

**Note:** If any changes made do not forget to apply before closing



## Misc

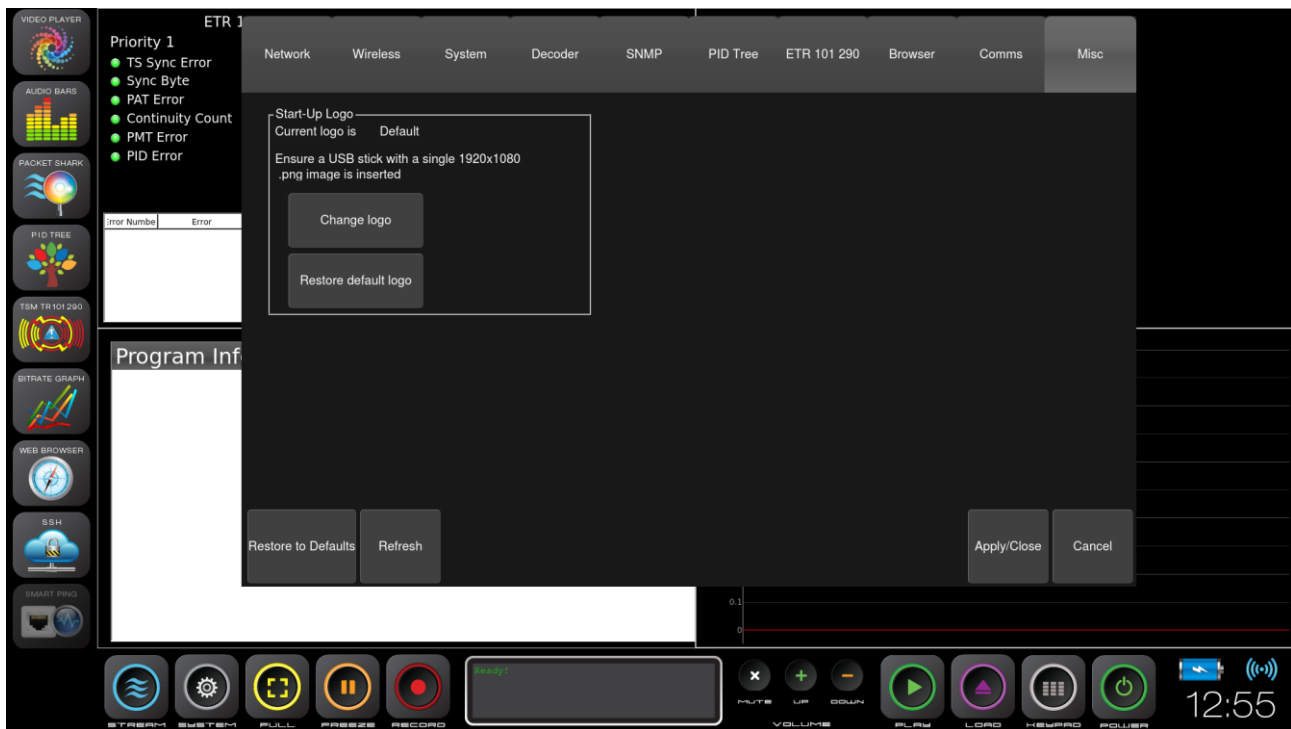


Figure 48: Miscellaneous Configuration

The Misc tab is currently used to enable changing the on-screen logo during the bootup.

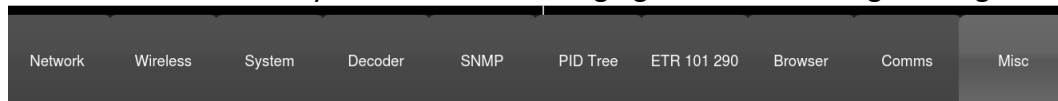


Figure 49: Change logo close up

## Operation Stream Select

The following steps describe how to decode and analyse a transport stream:


- 1) Drag and drop the Video Player  application into one of the four application display areas



Figure 50: Typical operational screen display

2) Press on Stream utility , the following window will appear:



Figure 51: Stream Select Dialog

- 3) Select your **Input Source**: Eth 1, Eth 2, ASI
  - a. If your Input source is ASI continue to step #7
  - b. If your Input Source is Eth1 or Eth 2 continue to step #4
- 4) Enter IP **Stream Address** and **Port Number**
- 5) Enter SSM (Source Specific Multicast - actual IP address of network port sending the video) address, if not available leave field blank.
 

Note: SSM is required for IGMPv3 networks and in loop back mode.
- 6) Specify video streaming protocol used: UDP, RTP (usually UDP in loop back mode)

- 7) Specify your **Program Select Mode** option, 2 modes are available:
  - a. **Auto Program:** Analyzer will automatically auto tune to a program
  - b. **Manual:** Force analyzer to decode a program, Enter program number in **Program Number** field below
- 8) Specify TS Mode, ATSC or DVB (Use DVB for Outside of USA)
- 9) Click OK

## Presets:

Presets are used to store Stream address details. There are five preset slots on the right hand side for quick access to commonly used configurations.

To save a Transport Stream IP address details follow the Stream Capture instructions up-to step #8, press and hold the plus (+) icon, the Transport Stream details are now saved.

## Decoder Configuration



will bring up a configuration dialog for the decoder. From here, you can select a different video program to decode (if available), a different audio track (if available) or enable captioning or subtitle burn-in (if present).

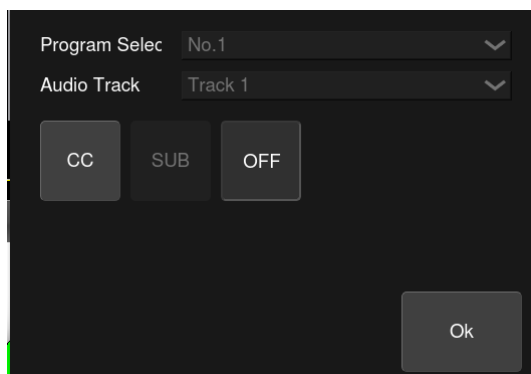


Figure 52: Decoder Configuration

## Stream Playback

The following steps describe how to playback a transport stream:



1. Press on the Play utility.



2. The window in Figure 51 will appear.
3. Select the **Output** Source ETH1, ETH2, ASI. If ASI is selected continue to step #5
4. Enter an output IP address and port number (just configured in Stream select above)
5. Select a file to playback
6. Press OK

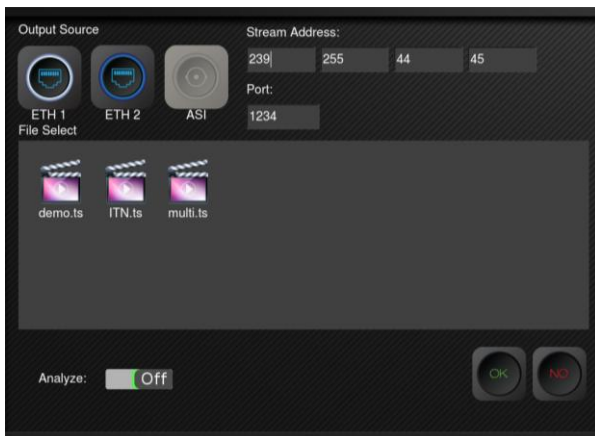


Figure 53: Stream Playback Dialog




To stop stream playback, press the Stream Playback button again (now a Stop indicator)



To test the stream that is playing out, turn the 'Analyze' mode On. This will run the stream through the analyzer as if it were playing in.

In stand alone demo mode use 'Analyze' mode On

## Screen Brightness

To adjust the brightness of the screen, press the battery icon  on the lower right.



Slide your finger along to adjust when finished press OK.



*Figure 54: Screen brightness adjustment*



## Quick Start Guide

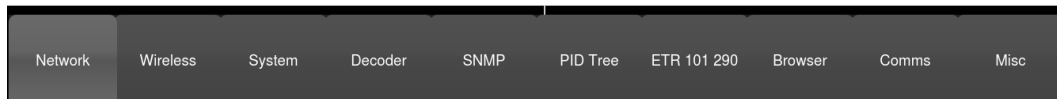
### Stream Payout and Loop-back



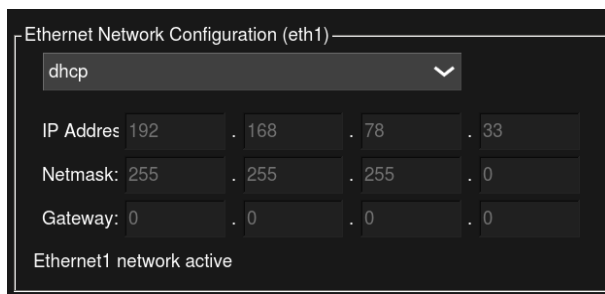
1. Enter the Configuration menu by pressing



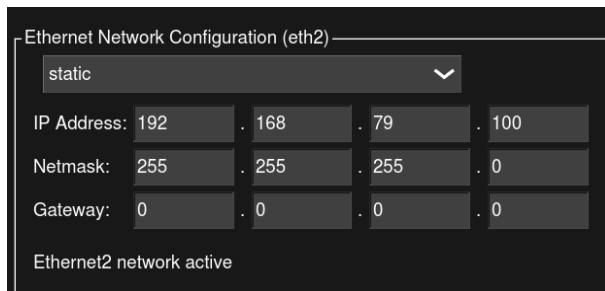
2. Select the Network tab.



3. Enter in the network settings for Eth1,



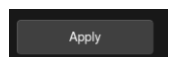
4. Repeat step #3 for Eth2.



**Note:** Eth1 and Eth2 must be on different subnets for proper operation.

**Note:** For a connection between Eth1 and Eth2, static mode must be selected for both.

5. When finished with the ethernet configuration select Apply button on the right side of the screen.



# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

6. Connect an Ethernet cable between Eth1 and Eth2 and confirm the connection with activity LED's lit up.

**Note:** The status on the Network configuration page for Eth1 and Eth2 will change from Inactive to Active.

7. Select OK to exit the System Configuration dialog.



8. Enter the playout dialog by pressing



9. Select Eth1 as the output source.



10. Select the desired file to playout



11. Select Analyze to On
12. Enter a multicast address and port number, and select OK.



13. Press on






# Hamlet® Enterprise™



15. In the stream dialog, enter the same multicast address from the playout dialog, along with the port number and the SSM address if appropriate.
16. Select Eth2 as the Input source.
17. Select OK when finished.




18. The stream should be pulled in and decoded.
19. Main apps to show in quad split mode:-

- Video player 
- ETR 101 290 alarm display 
- PID in tree 

then either:-

- Audio bar graphs 
- or Bitrate graph 

**Note:-** Full operation of the displays can made whilst in single display mode use  to toggle between single and quad mode



# Hamlet<sup>®</sup> Enterprise<sup>™</sup>

**Note:-** If looking at a multiple program Transport Stream and want to switch programs use the



Stream utility



Select manual program mode then choose the program number

**Note:** Make sure in the screen DVB is selected for correct decoding of DVB transport streams



## Appendix A

### Technical Specification

#### GENERAL

Storage: SSD Internal 32GB / optional expandable to 64GB  
Resolution: True 1080P/60 1920x1080

Viewing Size: 11.6" / 16:9.

Wifi: 802.11b/g/n

#### ETHERNET INPUT

Connector Dual RJ-45 for primary and backup link monitoring  
Data Rate: 10/100/1000

Protocols: UDP/RTP/IGMP v2 & v3/MDI/SPTS/MPTS/SNMP  
Physical Layer: 1EEE 802.3ab

#### ASI INPUT/OUTPUT (optional)

Connector: 75Ohm BNC  
Packet Size: 188 or 204 Byte Sequence

Bit Rate Range: 0 - 214 Mb/s  
Output: ASI On model ASIO only

#### DVB-S/S2 RF INPUT (optional)

Monitored: Lock status, Modulation Type, RF Level, MER, BER  
Connector: BNC  
Input level: < -23dBm  
Modulation Types:

Frequency: 950~2150 MHz

Impedance: 75Ω

Symbol Rate: 0.2-45Msps

DVB-S2

CCM, ACM, VCM

QPSK: 1/4, 1/3, 2/5, 1/2, 3/5, 2/3, 3/4, 4/5, 5/6, 8/9, 9/10

8PSK: 3/5, 2/3, 3/4, 5/6, 8/9, 9/10

16APSK: 2/3, 3/4, 4/5, 5/6, 8/9, 9/10

32APSK: 3/4, 4/5, 5/6, 8/9, 9/10

DVB-S

QPSK+1/2, 2/3, 3/4, 5/6, 7/8

#### Spectrum Analyser (optional) - TBC

Frequency: ~50-2500 MHz  
Sensitivity: > -100 dBm

Bandwidth/Span: <~50 MHz

#### OTT (optional) - TBC

Formats: HLS, HDS, RTMP, MPEG-DASH  
future release

Input: GigE Ethernet  
WiFi future release

Codec Support: Full decode of any stream from the profile.

Video: H.264 (up to HP 4.2), HEVC up to HP 4.0 future release

Audio: MP3, AAC, HE-AAC.

#### TEMPERATURE

Operating: +5 to +40° C

Non Operating: -20 to +60° C

#### POWER

Built-In: 11.1v/4600mA Battery  
Adapter: DC 19V/2.1

Endurance: Up to 2Hrs

#### PHYSICAL

Dimensions: - 15"w x 8"h x 1.5"d

Weight:- 1lbs/3.2Kg

## Appendix B

### Options

<b>Enterprise</b>	
<b>ENT-101</b>	IP MPEG Stream Analyser
<b>ENT-102</b>	IP and ASI MPEG Stream Analyzer "all in package"
<b>ENT-103</b>	IP, ASI MPEG Stream Analyzer and Playout "all in package"
<b>Software options</b>	
<b>ENT-S101</b>	tba
<b>ENT-S102</b>	OTT Analyzer Software
<b>ENT-S103</b>	Record & Playback Software
<b>Hardware options</b>	
<b>ENT-H101</b>	ASI input option card - <i>factory installed</i>
<b>ENT-H102</b>	DVB RF input option for card - <i>factory installed</i>
<b>ENT-H103</b>	ATSC RF input option for card - <i>factory installed</i>
<b>ENT-H104</b>	RF Spectrum Analyser board - <i>factory installed</i>
<b>Accessories</b>	
<b>ENT-A101</b>	Ruggedized Hard Case
<b>ENT-A102</b>	Expansion by 64Gb
<b>ENT-A103</b>	Spare Power Supply
<b>ENT-A104</b>	Rack Mount Rail

## Appendix C

### Berkeley Packet Filter (BPF) syntax

The *expression* consists of one or more *primitives*. Primitives usually consist of an *id* (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

#### *type*

qualifiers say what kind of thing the id name or number refers to. Possible types are **host**, **net**, **port** and **portrange**. E.g., 'host foo', 'net 128.3', 'port 20', 'portrange 6000-6008'. If there is no type qualifier, **host** is assumed.

#### *dir*

qualifiers specify a particular transfer direction to and/or from *id*. Possible directions are **src**, **dst**, **src or dst** and **src and dst**. E.g., 'src foo', 'dst net 128.3', 'src or dst port ftp-data'. If there is no dir qualifier, **src or dst** is assumed. For some link layers, such as SLIP and the "cooked" Linux capture mode used for the "any" device and for some other device types, the **inbound** and **outbound** qualifiers can be used to specify a desired direction.

#### *proto*

qualifiers restrict the match to a particular protocol. Possible protos are: **ether**, **fddi**, **tr**, **wlan**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp**. E.g., 'ether src foo', 'arp net 128.3', 'tcp port 21', 'udp portrange 7000-7009'. If there is no proto qualifier, all protocols consistent with the type are assumed. E.g., 'src foo' means '(ip or arp or rarp) src foo' (except the latter is not legal syntax), 'net bar' means '(ip or arp or rarp) net bar' and 'port 53' means '(tcp or udp) port 53'.

Allowable primitives are:

#### **dst host** *host*

True if the IPv4/v6 destination field of the packet is *host*, which may be either an address or a name.

#### **src host** *host*

True if the IPv4/v6 source field of the packet is *host*.

#### **host** *host*

True if either the IPv4/v6 source or destination of the packet is *host*.

Any of the above host expressions can be prepended with the keywords, **ip**, **arp**, **rarp**, or **ip6** as in:

#### **ip host** *host*

#### **ether dst** *ehost*

True if the Ethernet destination address is *ehost*. *Ehost* may be either a name from /etc/ethers or a number.

#### **ether src** *ehost*

True if the Ethernet source address is *ehost*.

#### **ether host** *ehost*

True if either the Ethernet source or destination address is *ehost*.

#### **gateway** *host*

True if the packet used *host* as a gateway.

#### **dst net** *net*

True if the IPv4/v6 destination address of the packet has a network number of *net*.

#### **src net** *net*

True if the IPv4/v6 source address of the packet has a network number of *net*.

#### **net** *net*

True if either the IPv4/v6 source or destination address of the packet has a network number of *net*.

#### **net net mask** *netmask*

True if the IPv4 address matches *net* with the specific *netmask*. May be qualified with **src** or **dst**. Note that this syntax is not valid for IPv6 *net*.

#### **net** *net/len*



True if the IPv4/v6 address matches *net* with a netmask *len* bits wide. May be qualified with **src** or **dst**.

**dst port** *port*

True if the packet is ip/tcp, ip/udp, ip6/tcp or ip6/udp and has a destination port value of *port*.

**src port** *port*

True if the packet has a source port value of *port*.

**port** *port*

True if either the source or destination port of the packet is *port*.

**dst portrange** *port1-port2*

True if the packet is ip/tcp, ip/udp, ip6/tcp or ip6/udp and has a destination port value between *port1* and *port2*. *port1* and *port2* are interpreted in the same fashion as the *port* parameter for **port**.

**src portrange** *port1-port2*

True if the packet has a source port value between *port1* and *port2*.

**portrange** *port1-port2*

True if either the source or destination port of the packet is between *port1* and *port2*.

**less** *length*

True if the packet has a length less than or equal to *length*. This is equivalent to:

**len** <= *length*.

**greater** *length*

True if the packet has a length greater than or equal to *length*. This is equivalent to:

**len** >= *length*.

**ip proto** *protocol*

True if the packet is an IPv4 packet (see *ip(4P)*) of protocol type *protocol*.

**ip6 proto** *protocol*

True if the packet is an IPv6 packet of protocol type *protocol*. Note that this primitive does not chase the protocol header chain.

**ip6 protochain** *protocol*

True if the packet is IPv6 packet, and contains protocol header with type *protocol* in its protocol header chain.

**ip protochain** *protocol*

Equivalent to **ip6 protochain** *protocol*, but this is for IPv4.

**ether broadcast**

True if the packet is an Ethernet broadcast packet. The *ether* keyword is optional.

**ip broadcast**

True if the packet is an IPv4 broadcast packet.

**ether multicast**

True if the packet is an Ethernet multicast packet. The **ether** keyword is optional. This is shorthand for **`ether[0] & 1 != 0`**.

**ip multicast**

True if the packet is an IPv4 multicast packet.

**ip6 multicast**

True if the packet is an IPv6 multicast packet.

**ether proto** *protocol*

True if the packet is of ether type *protocol*.

**decnet src** *host*

True if the DECNET source address is *host*, which may be an address of the form ``10.123'', or a DECNET host name. [DECNET host name support is only available on ULTRIX systems that are configured to run DECNET.]

**decnet dst** *host*

True if the DECNET destination address is *host*.

**decnet host** *host*

True if either the DECNET source or destination address is *host*.

**ifname** *interface*

True if the packet was logged as coming from the specified interface

**on** *interface*

Synonymous with the **ifname** modifier.

## **rn timer**

True if the packet was logged as matching the specified PF rule number

## **rule number**

Synonymous with the **rn timer** modifier.

## **reason code**

True if the packet was logged with the specified PF reason code.

## **rset name**

True if the packet was logged as matching the specified PF ruleset name of an anchored ruleset (applies only to packets logged by **pf(4)**).

## **ruleset name**

Synonymous with the **rset** modifier.

## **srnr timer**

True if the packet was logged as matching the specified PF rule number of an anchored ruleset

## **subrule number**

Synonymous with the **srnr** modifier.

## **action act**

True if PF took the specified action when the packet was logged. Known actions are: **pass** and **block**

## **ip, ip6, arp, rarp, atalk, aarp, decnet, iso, stp, ipx, netbeui**

Abbreviations for:

**ether proto p**

where *p* is one of the above protocols.

## **lat, mopr, mopr, mopr**

Abbreviations for:

**ether proto p**

where *p* is one of the above protocols.

## **vlan [vlan\_id]**

True if the packet is an IEEE 802.1Q VLAN packet.

## **mpls [label\_num]**

True if the packet is an MPLS packet. If *[label\_num]* is specified, only true if the packet has the specified *label\_num*.

## **pppoe**

True if the packet is a PPP-over-Ethernet Discovery packet (Ethernet type 0x8863).

## **pppoe**

True if the packet is a PPP-over-Ethernet Session packet (Ethernet type 0x8864).

## **tcp, udp, icmp**

Abbreviations for:

**ip proto p or ip6 proto p** - where *p* is one of the above protocols.

## **iso proto protocol**

True if the packet is an OSI packet of protocol type *protocol*. *Protocol* can be a number or one of the names **clnp**, **esls**, or **isis**.

## **clnp, esls, isis**

Abbreviations for:

**iso proto p**

where *p* is one of the above protocols.

## **l1, l2, iih, lsp, snp, csnp, psnp**

Abbreviations for IS-IS PDU types.

## **vpi n**

True if the packet is an ATM packet

## **vci n**

True if the packet is an ATM packet

## **lane**

True if the packet is an ATM packet

## **llc**

	True if the packet is an ATM packet
<b>oamf4s</b>	True if the packet is an ATM packet
<b>oamf4e</b>	True if the packet is an ATM packet,
<b>oamf4</b>	True if the packet is an ATM packet
<b>oam</b>	True if the packet is an ATM packet
<b>metac</b>	True if the packet is an ATM packet
<b>bcc</b>	True if the packet is an ATM packet
<b>sc</b>	True if the packet is an ATM packet
<b>ilmic</b>	True if the packet is an ATM packet
<b>connectmsg</b>	True if the packet is an ATM packet
<b>metaconnect</b>	True if the packet is an ATM packet
<b>expr relop expr</b>	True if the relation holds, where <i>relop</i> is one of >, <, >=, <=, =, !=, and <i>expr</i> is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+ , - , * , / , & ,   , << , >>], a length operator, and special packet data accessors.

Primitives may be combined using:

A parenthesized group of primitives and operators (parentheses are special to the Shell and must be escaped).  
Negation ('!' or **not**).  
Concatenation ('&&' or **and**).  
Alternation ('||' or **or**).

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right. Note that explicit **and** tokens, not juxtaposition, are now required for concatenation.

If an identifier is given without a keyword, the most recent keyword is assumed. For example,

## **not host vs and ace**

is short for

## **not host vs and host ace**

which should not be confused with

## **not ( host vs or ace )**

Expression arguments can be passed to *tcpdump* as either a single argument or as multiple arguments, whichever is more convenient. Generally, if the expression contains Shell metacharacters, it is easier to pass it as a single, quoted argument. Multiple arguments are concatenated with spaces before being parsed.

## Appendix D

### Berkeley Packet Filter Examples

To capture all packets arriving at or departing from *sundown*: **host sundown**

To capture traffic between *helios* and either *hot* or *ace*: **host helios and \ ( hot or ace )**

To capture all IP packets between *ace* and any host except *helios*: **ip host ace and not helios**

To capture all traffic between local hosts and hosts at Berkeley: **net ucb-ether**

To capture all ftp traffic through internet gateway *snu*: (note that the expression is quoted to prevent the shell from (mis-)interpreting the parentheses): **gateway snup and (port ftp or ftp-data)**

To capture traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net). **ip and not net localnet**

To capture the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host. **tcp[tcpflags] & (tcp-syn | tcp-fin) != 0 and not src and dst net localnet**

To capture all IPv4 HTTP packets to and from port 80, i.e. print only packets that contain data, not, for example, SYN and FIN packets and ACK-only packets. (IPv6 is left as an exercise for the reader.) **tcp port 80 and (((ip[2:2] - ((ip[0]&0xf)<<2)) - ((tcp[12]&0xf0)>>2)) != 0)**

To capture IP packets longer than 576 bytes sent through gateway *snu*: **gateway snup and ip[2:2] > 576**

To capture IP broadcast or multicast packets that were *not* sent via Ethernet broadcast or multicast: **ether[0] & 1 = 0 and ip[16] >= 224**

To capture all ICMP packets that are not echo requests/replies (i.e., not ping packets): **icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echoreply**

See Berkeley Packet Filter web site for more information <http://biot.com/capstats/bpf.html>

## Appendix E

### Useful Websites

Hamlet	<a href="http://www.hamlet.co.uk">http://www.hamlet.co.uk</a>
Hamlet (USA)	<a href="http://www.hamlet.tm">http://www.hamlet.tm</a>
SMPTE	<a href="http://www.smpte.org">http://www.smpte.org</a> Society of Motion Picture Television Engineers
DIN	<a href="http://www.din.de">http://www.din.de</a> German Standards Institute
EBU	<a href="http://www.ebu.ch">http://www.ebu.ch</a> European Broadcasting Union
AES	<a href="http://www.aes.org">http://www.aes.org</a> Audio Engineering Society
ITU	<a href="http://www.itu.int">http://www.itu.int</a> International Telecommunication Union
Berkeley Packet Filter	<a href="http://biot.com/capstats/bpf.html">http://biot.com/capstats/bpf.html</a>

## Appendix F

### Contact details and customer support

Worldwide service and returns information for your Hamlet Enterprise VX1 can be found on our Website: <http://www.hamlet.co.uk/support/returns/>

In correspondence concerning this instrument, please quote the serial number, which you will find printed on the label at the back of the unit.