User Manual

Paragon-X

IP/Ethernet Network Emulation and Impairment solution

This manual applies to Paragon-X Network Emulation Application Software Releases 11.36.08 and later.

Notices

Warranty

The information contained in this document is subject to change without notice.

Calnex Solutions Ltd makes no warranty of any kind with regards to this material, including but not limited to, the implied warranties or merchantability and fitness for a particular purpose.

Calnex Solutions Ltd shall not be liable for errors contained herein and for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

WARNING

To prevent fire or shock hazard, do not expose the equipment to rain or moisture.

To avoid electrical shock, use only supplied AC/DC adaptor and connect only to a properly grounded power socket outlet. Ensure the power socket outlet is easily accessible and near the unit.

To avoid electrical shock, do not open covers. Refer servicing to qualified personnel only.

Power Requirements

The unit requires a power source of:
Voltage: 100 -240 Vac
Current: 1.5 A @ 100 Vac
Frequency: 50 – 60 Hz

Operating Environment

Temperature. The unit may be operated in temperatures from 0 ^{0}C to +50 ^{0}C.

Humidity. The unit may be operated in environments with relative humidity from 0% to 95%. However, the unit should also be protected from temperature extremes, which cause condensation within the unit.

Labels and Disposal Information

The Waste Electrical and Electronic Equipment regulations label indicates that the equipment should only be disposed of through an approved method. At the end of life please dispose of the equipment through a recognized and approved scheme fulfilling the local environmental requirements. Alternatively contact Calnex to have them arrange for return and disposal.

The CE mark indicates that the product meets all the appropriate provisions of the relevant legislation contained in the European Directives.

Table of Contents

Chapter 1 - Getting Started

This chapter describes how to install the Paragon-X Network Emulation Application Software.

Introduction

For IP/Ethernet, the Paragon-X Network Emulation option offers the ability to generate a broad range of real-world disruption scenarios to validate the operation of your network, devices and applications.

The main functions (with appropriate options installed) are:

- Ethernet interface rates of 100M, 1G and 10Gbit/s
- Through-mode packet delay, PDV, corruption and Bandwidth Control
- Multiple independent impairment profiles
- Capture Packet Delay Variation of real traffic from your network
- Edit and replay captured profiles to emulate the real network and test robustness
- Fully integrated Automatic and/or Manual filter set up with FlowWizard & FilterBuilder
- FlowWizard automatically identifies & classifies flows of interest to create traffic filters
- FilterBuider provides quick and easy manual filter set up
- Automated Script generation via Script Recorder

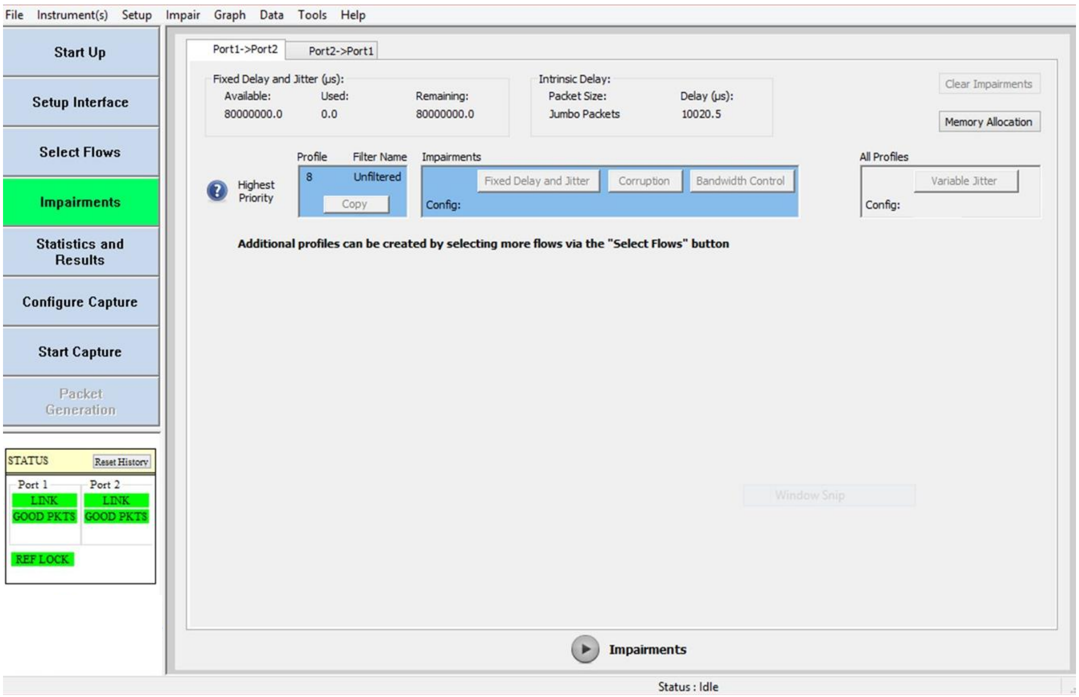
Installing the Paragon-X Network Emulation Application Software

The Paragon-X Network Application software comprises two parts; the application software which is on the CD-ROM delivered with Paragon-X, and Paragon-X's embedded software which is pre-installed prior to delivery. The CD-ROM application software must be installed on your computer as described in the following steps.

1. Uninstall any previously installed versions of the Paragon-X Network Emulation or Flow Wizard applications.

2. Insert the CD-ROM into your computer's CD-ROM drive.
   Double click the installer package (the Network Emulation application is bundled with the Paragon-X software suite) and follow the on-screen instructions to complete the installation.

3. Click on **Start** then **Calnex Paragon-X Network Emulation** to launch the Network Emulation application. The user interface is displayed as shown below.



Fixed Delay and Jitter (μs):
Available: 80000000.0
Used: 0.0
Remaining: 80000000.0

Intrinsic Delay:
Packet Size: Jumbo Packets
Delay (μs): 10020.5

Profile	Filter Name
8	Unfiltered

Impairments
Config:

All Profiles
Config:

Additional profiles can be created by selecting more flows via the "Select Flows" button

Status : Idle

4. To determine what revision of software application is running, click on **Help** then **About**

5. Additionally, you must also install either **Wireshark**. More details about Wireshark can be obtained from www.wireshark.org.

6. The Network Emulation application requires .NET Framework version 3.5, and also either version 4.0 or 4.5, to be enabled on your computer. These can be enabled at **Control Panel -> Programs -> Turn Windows features on or off**. If using older versions of Windows you may need to install the .NET Framework software from Microsoft.

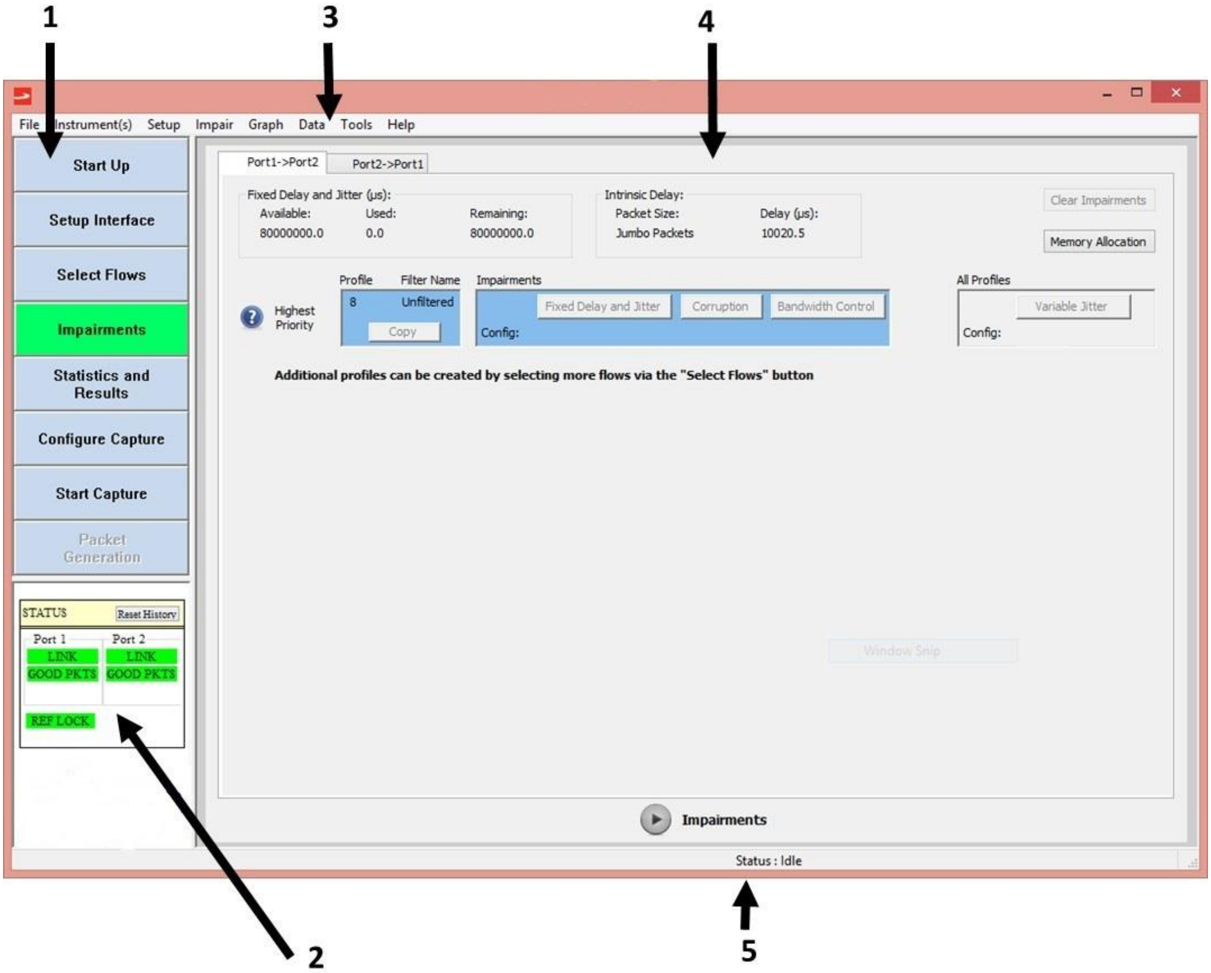
It is possible to use the Application while not connected to an instrument. In this case, click on **Help -> Demo** to enable Demo Mode. The Application will then automatically use pre-configured demo capture files to simulate traffic, or the user can import and use their own capture or replay files.

Chapter 2 - Getting to know the Application

The Application is a Windows based graphical user interface that has been designed to make set up quick and easy and also to provide the user with a clear overview of the traffic flows and the impairments applied. Help is provided via Tool Tips that automatically activate when the user hovers the mouse cursor over the area of interest.

Application Overview

The Application window's main features are shown and described below.



Fixed Delay and Jitter (µs):
Available: 80000000.0
Used: 0.0
Remaining: 80000000.0

Intrinsic Delay:
Packet Size: Jumbo Packets
Delay (µs): 10020.5

Profile: 8 — Filter Name: Unfiltered

Additional profiles can be created by selecting more flows via the "Select Flows" button

Status : Idle

Workflow Area/Buttons (1)

These buttons are arranged in order of sequence for easy flow through the main tasks. Start from the top button and work downwards to complete the task.

Start Up – click this button to Connect to (or disconnect from) the Paragon-X hardware and to Save/Recall instrument setup configurations.

Setup Interface – click this button to set up Ethernet Interface Settings; Line Rate, Interface etc.
Select Flows – this button launches the Flow Wizard tool to capture and detect the traffic being received at the Interface Ports. The detected traffic flows are then presented to the user to aid Filter selection.

Impairments – Click on this button to add impairments to the selected traffic flows.

Statistics and Results – Click on this button to view statistical information about the applied impairments and to view results.

Configure Capture - This button is used to configure the network capture period and also to select what packet bytes (if any) are to be captured during the network capture.

Start Capture – This button initiates a capture of network data related to the traffic received at the Paragon-X Ports. The arrival time and inter-packet time for each packet as well as the captured packet bytes (selected above) will be displayed.

Packet Generation – Click on this button to configure and generate simple test packets that can be used for device testing or jitter tolerance testing. This button is only active when the interface is set to **Tx + Rx Mode**.

Status Indicators (2)

Status indicators provide a quick visual indication of the status of the interface ports and clock reference. The colours of the following are indications of their status, with green = no alarms, red = current alarm and yellow= historical alarm;

- LINK: indicates if there is a physical Ethernet connection by detecting transitions on the selected port Rx side.
- GOOD PKTS: indicates if Ethernet packets are being received with no PCS or checksum errors (legend changes to BAD PACKETS in addition to going red if condition fails).
- REF LOCK: indicates if the instrument is locked to the selected frequency reference source as configured on the **Setup Interface** window.

Any event which causes these indicators to display an error condition during a period when impairments have been activated will, on clearing the condition, change to yellow rather than returning to green. This history may be reset at any time by clicking the **Reset History** button.

Menu Bar (3)

Use the drop down menus to select various configurations, settings and measurement modes. Some of these duplicate workflow buttons, in which case it’s recommended to use the workflow buttons directly.

Main Display Area (4)

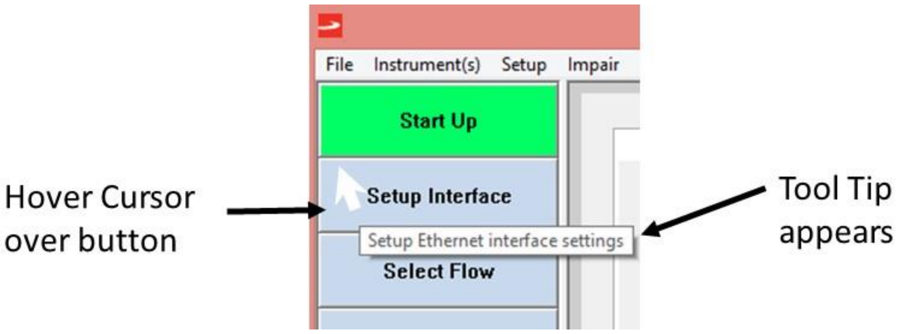
This is the main area for configuring multi-flow impairments, viewing packet bytes, network capture data and graphs.

Operation Status (5)

Indicates the current Operation Status – Idle, Capture or Replay.

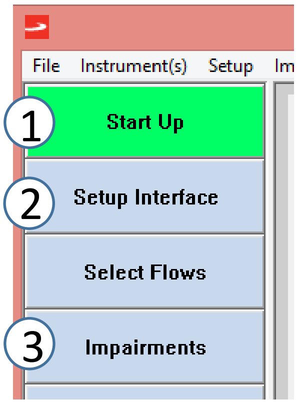
Tool Tips

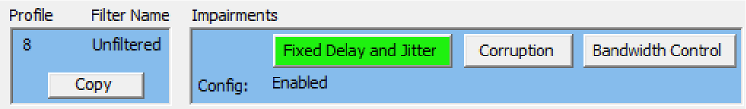
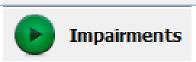
Many areas of the Application user interface have Tool Tips incorporated. Hover the cursor over an area using the mouse and the Tool Tip will appear as shown below.



Simple "Use Model" – Impair All Traffic

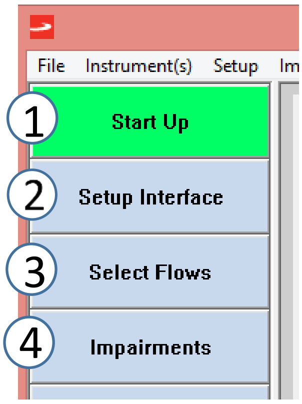
Impairments can be quickly set up and applied to all traffic using the single profile model shown below.

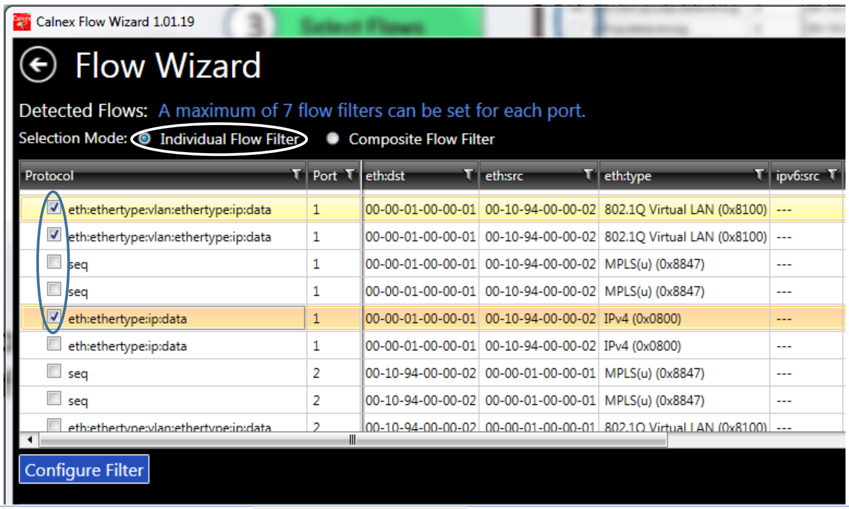
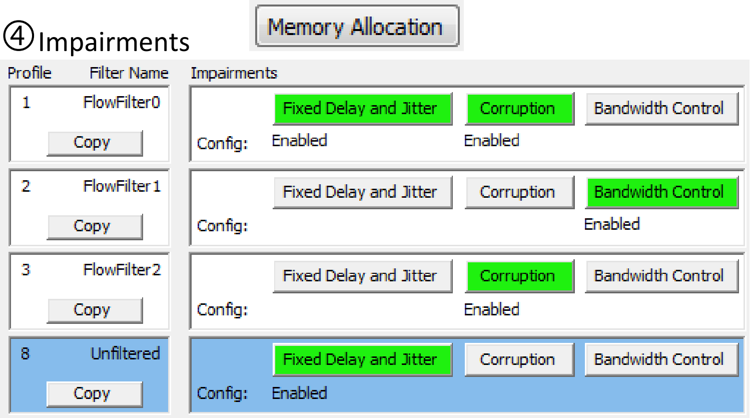
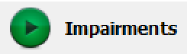


Simple Use Model	Adding Bulk Delay – all traffic streams
Connect Paragon-X to PC and to Network-Under-Test	①Start Up ②Setup Interface
Configure Impairments 1s Bulk Delay	③Impairments  Profile: 8 Filter Name: Unfiltered Copy Impairments: Fixed Delay and Jitter, Corruption, Bandwidth Control Config: Enabled
Apply Impairments	 Impairments

Simple "Use Model" – Selective Filtering & Multi-Profile Impairments

This model uses Flow Wizard to select traffic flows of interest that can be individually impaired using the Network Emulation application's multi-profile impairment capabilities.



Simple Use Model	Selective Impairments
Connect Paragon-X to PC and to Network-Under-Test	①Start Up ②Setup Interface
Select Traffic Flows of Interest	③Select Flows 
Allocate Memory to Profiles and Configure Impairments	④Impairments 
Apply Impairments	

Flow Wizard

Detected Flows: A maximum of 7 flow filters can be set for each port.

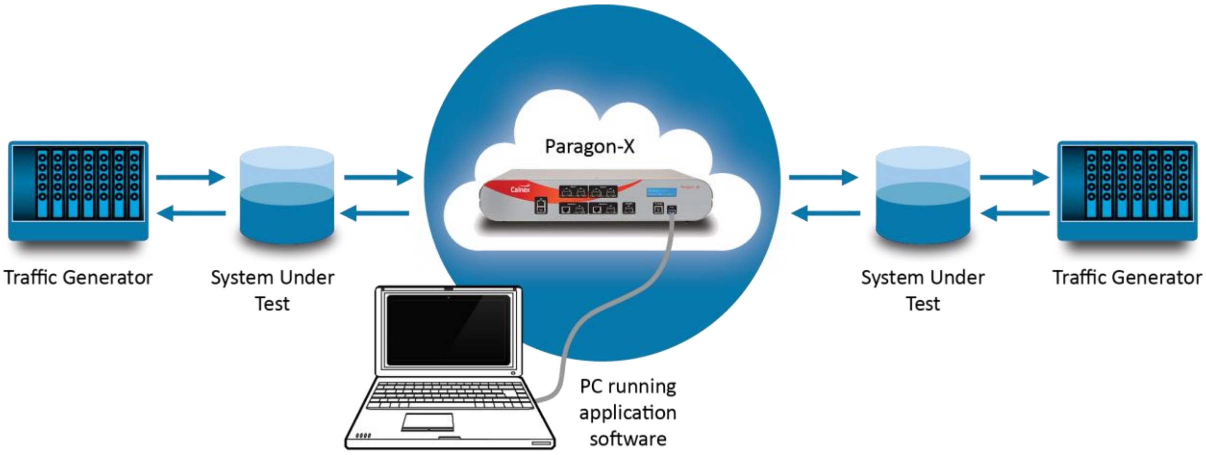
Selection Mode: ● Individual Flow Filter ○ Composite Flow Filter

	Protocol	Port	eth:dst	eth:src	eth:type	ipv6:src
☑	eth:ethertype:vlan:ethertype:ip:data	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---
☑	eth:ethertype:vlan:ethertype:ip:data	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---
☐	seq	1	00-00-01-00-00-01	00-10-94-00-00-02	MPLS(u) (0x8847)	---
☐	seq	1	00-00-01-00-00-01	00-10-94-00-00-02	MPLS(u) (0x8847)	---
☑	eth:ethertype:ip:data	1	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---
☐	eth:ethertype:ip:data	1	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---
☐	seq	2	00-10-94-00-00-02	00-00-01-00-00-01	MPLS(u) (0x8847)	---
☐	seq	2	00-10-94-00-00-02	00-00-01-00-00-01	MPLS(u) (0x8847)	---
☐	eth:ethertype:vlan:ethertype:ip:data	2	00-10-94-00-00-02	00-00-01-00-00-01	802.1Q Virtual LAN (0x8100)	---

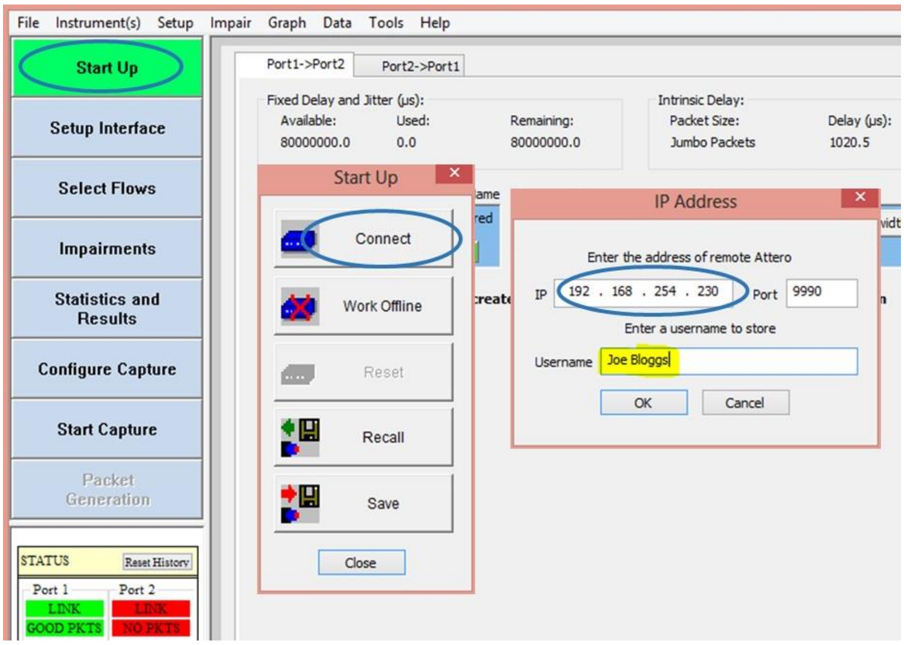
Profile	Filter Name	Impairments		
1	FlowFilter0	🟩 Fixed Delay and Jitter	🟩 Corruption	Bandwidth Control
	Copy	Config: Enabled	Enabled	
2	FlowFilter1	Fixed Delay and Jitter	Corruption	🟩 Bandwidth Control
	Copy	Config:		Enabled
3	FlowFilter2	Fixed Delay and Jitter	🟩 Corruption	Bandwidth Control
	Copy	Config:	Enabled	
8	Unfiltered	🟩 Fixed Delay and Jitter	Corruption	Bandwidth Control
	Copy	Config: Enabled		

Chapter 3 - Connecting to the Network-Under-Test

This chapter describes how to connect to the network-under-test and how to set up the Ethernet ports. The instrument is normally connected between the elements of the network-under-test as shown below.



- Click on **Start Up** then on **Connect.** Enter the IP address of the Paragon-X unit (see the example below). Entering your name in the **Username** field (highlighted below) helps other users identify who is currently connected to the instrument when they attempt to connect.
- Click **OK** to complete connecting.



Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
80000000.0	0.0	80000000.0

Intrinsic Delay:

Packet Size:	Delay (µs):
Jumbo Packets	1020.5

Enter the address of remote Attero

IP 192 . 168 . 254 . 230 Port 9990

Enter a username to store

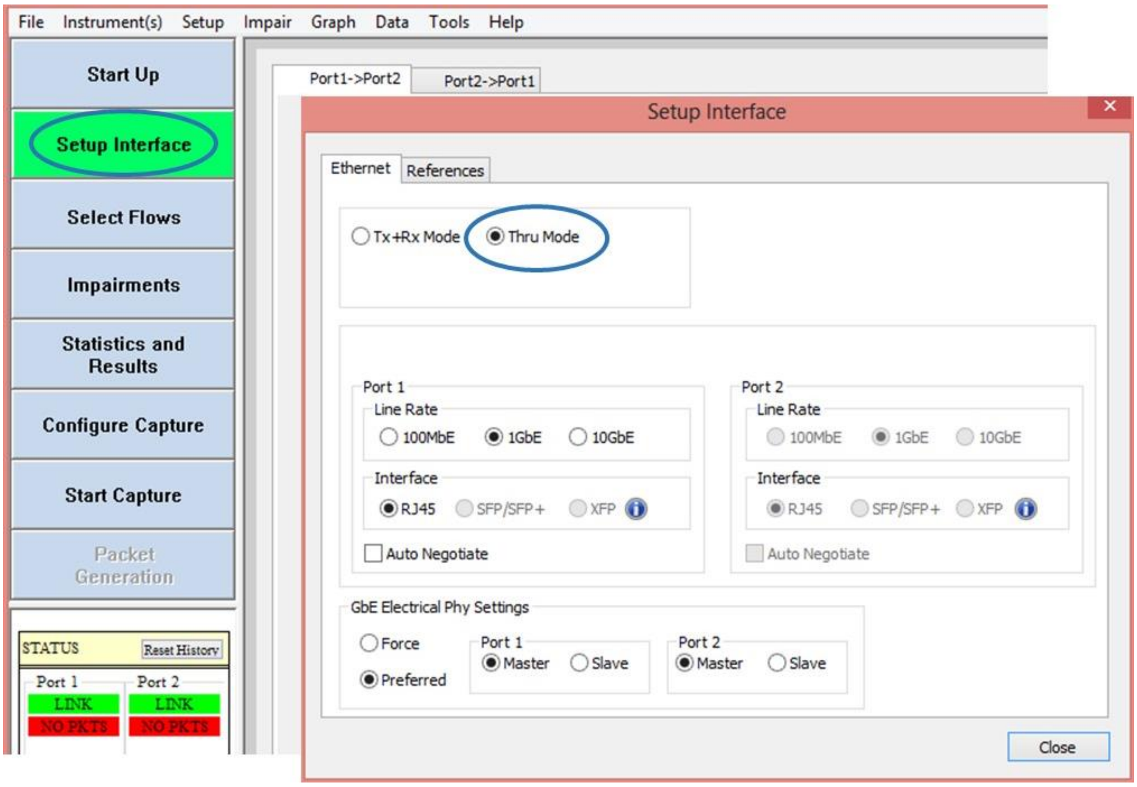
Username Joe Bloggs

- A dialog box will show the status of the connection. When Status = Connected click on the **OK** button.
- Press the **Close** button to close the Start Up dialog box

Setting-up the Line Interfaces

- Click on the **Setup Interface** button in the Workflow area and set the Mode to **Thru Mode** as shown encircled below. This mode passes traffic through the instrument from Port 1 to Port 2 and vice versa. The instrument can later be configured to impair selected traffic on these ports.

Ports 1 and 2 are always coupled; any changes made to Port 1 are duplicated on Port 2.
Tx + Rx Mode is used for generating and receiving simple Test Packets. This is described in Appendix 3 - Other Features and Functions.



○ Tx+Rx Mode ● Thru Mode

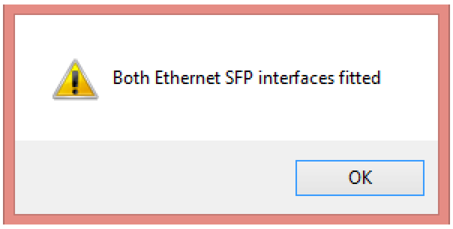
Port 1
Line Rate: ○ 100MbE ● 1GbE ○ 10GbE
Interface: ● RJ45 ○ SFP/SFP+ ○ XFP
□ Auto Negotiate

Port 2
Line Rate: ○ 100MbE ● 1GbE ○ 10GbE
Interface: ● RJ45 ○ SFP/SFP+ ○ XFP
□ Auto Negotiate

GbE Electrical Phy Settings
○ Force
● Preferred
Port 1: ● Master ○ Slave
Port 2: ● Master ○ Slave

- Set up the **Line Rate** and **Interface** on Ports 1 and 2 to match the network-under-test that the instrument is connected to.
  Note: some interface settings are dependent on the Line Rate setting - for example XFP is only valid for 10GbE Line rate.

The 1GbE Optical Ports (SFP/SFP+) auto-detect when the transceivers are inserted and removed. The **SFP/SFP+** selection is greyed-out unless both ports have transceivers fitted. The user is alerted to the availability of the **SFP/SFP+** selection by pop-up windows similar to the one shown below.



Both Ethernet SFP interfaces fitted

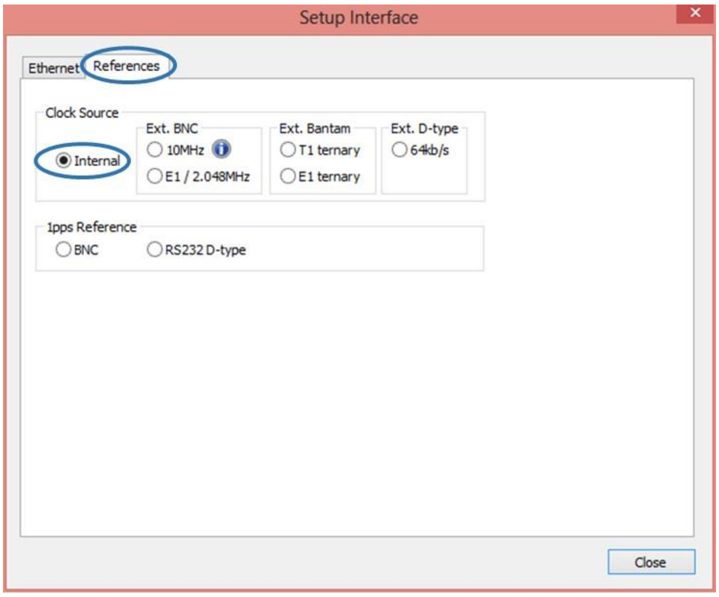
Note: Insertion of Transceivers in the 10GbE Optical Ports are not auto-detected.

Auto-negotiate can be selected to allow auto-negotiation of the interfaces.

The **GbE Electrical Phy Settings** allow flexibility in setting which device provides the Master clock for the Gigabit Ethernet Link (the device at the other end of the link would use the recovered clock). This setting can be "Forced" by the instrument or it can be set to "Preferred" to avoid conflicts where both ends of the link demand to be master. These settings are only active when the Line Rate is set to **1GbE**.

Selecting the Reference Clock

The **Reference Clock** defaults to **Internal.** A variety of external clock references are available within the **References** tab as shown below. The external clock reference interface ports are located on the rear panel of the instrument. It is recommended that the Internal Clock Reference is used for all main Network Emulation applications. The 1 pps Reference ports are for possible future use.



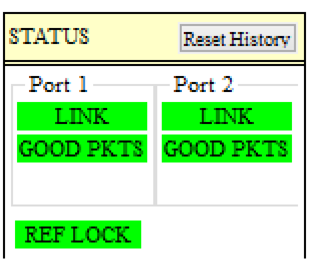
Setup Interface

Ethernet | References

Clock Source
- ● Internal
- Ext. BNC: ○ 10MHz, ○ E1 / 2.048MHz
- Ext. Bantam: ○ T1 ternary, ○ E1 ternary
- Ext. D-type: ○ 64kb/s

1pps Reference
- ○ BNC
- ○ RS232 D-type

- When the interface has been set up to match the network to which it is connected, the **LINK** and **REF LOCK** Indicators should be coloured green as shown below.



STATUS

Port 1	Port 2
LINK	LINK
GOOD PKTS	GOOD PKTS

REF LOCK

- Click on the Close button once the interface settings are complete.

Recalling Default Settings

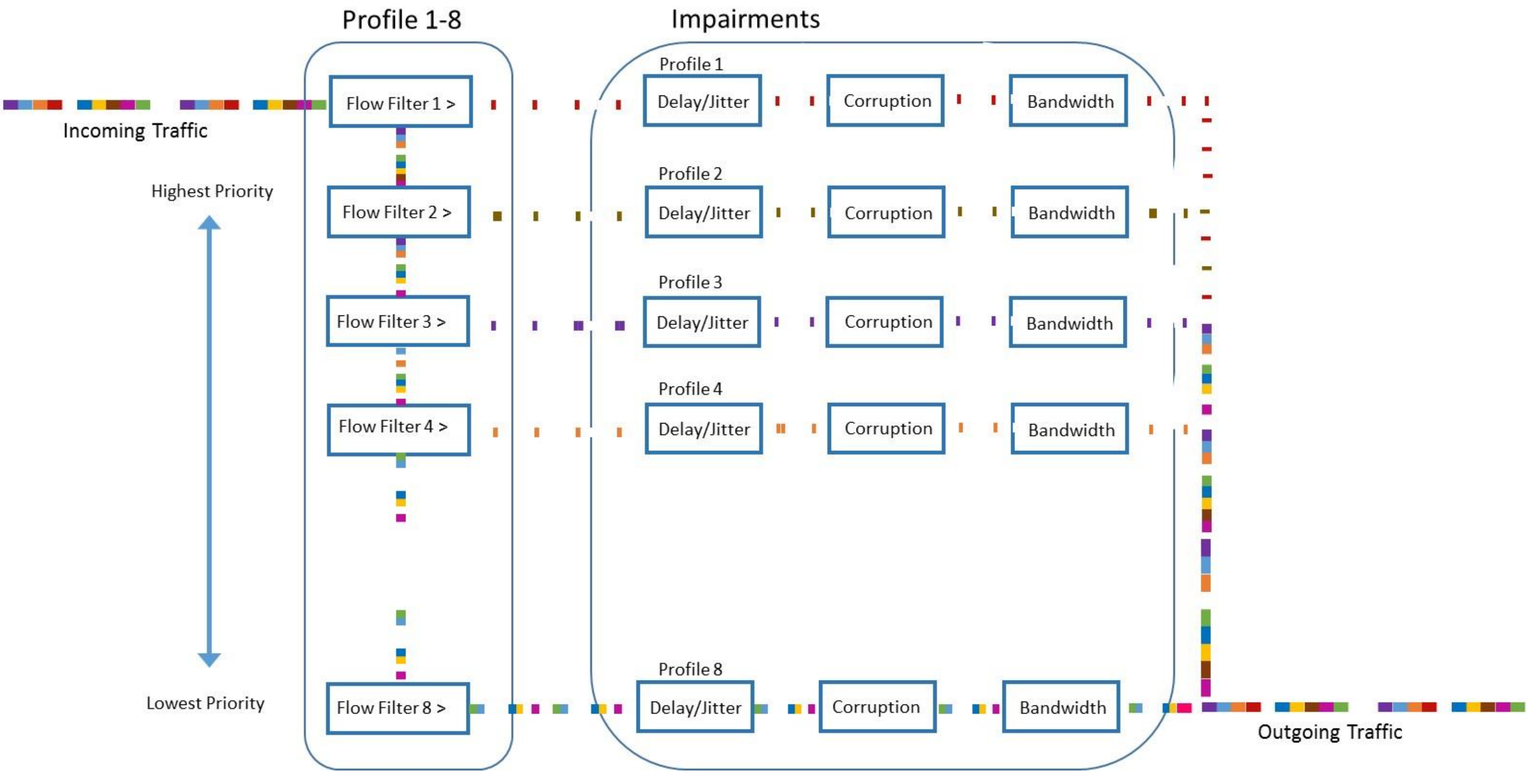
Instrument settings are preserved after a temporary disconnection. To reset the instrument to default settings click on **Setup -> Recall Default Settings**.

Chapter 4 – Selecting Filters

Chapters 4 and 5 explain how to filter specific flows of traffic and apply a profile of impairments to each filter. The model used is described below. If all traffic is to be impaired in one single impairment profile skip this chapter and go straight to Chapter 5.

Flow Filter and Impairment Profile Model

The diagram below illustrates how the Incoming Traffic enters the “Flow Filters” and how packets get filtered and processed through individual Impairment Profile paths before being recombined into the Outgoing Traffic.

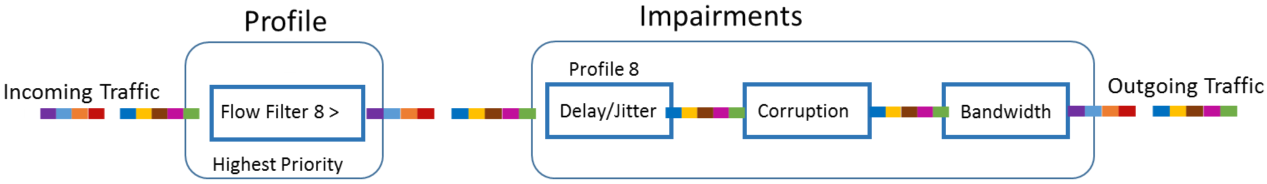


The various colours in the Incoming Traffic represent the various packet types that may be present at the Ethernet input ports. The Incoming Traffic is applied to Flow Filter 1 (this is the highest priority filter). Any packets that match Flow Filter 1 criteria are passed to the right-hand-side through Profile 1 where a combination of Fixed Delay, Jitter and Corruption Impairments can be applied. All remaining traffic that does not match Flow Filter 1 criteria is passed downwards to Flow Filter 2. Any packets that match Flow Filter 2 criteria are passed to the right-hand-side through Profile 2 where a different combination of Fixed Delay, Jitter and Corruption impairments can be applied. All remaining traffic that does not match Flow Filter 2 criteria is passed downwards to Flow Filter 3 and so on. Traffic that does not match any of the Flow Filters criteria passes through Flow Filter 8 and on to Impairment Profile 8.

The traffic at the output of all 8 Impairment Profiles is recombined to make-up the Outgoing Traffic after the impairments have been applied.

The above diagram and procedure is duplicated for traffic in each direction.

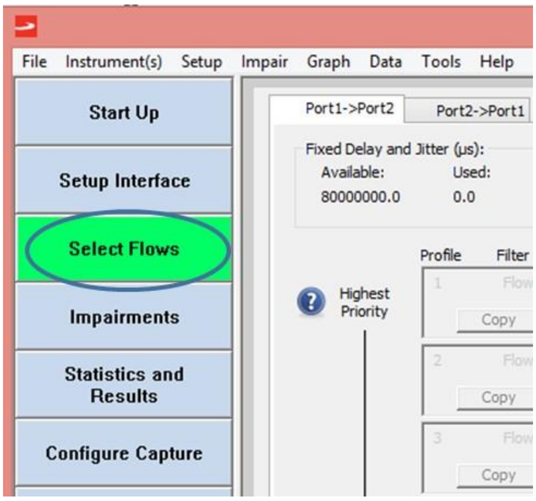
If no filters are set all traffic passes through Flow Filter 8 and Profile 8 as shown below.



Selecting Flows

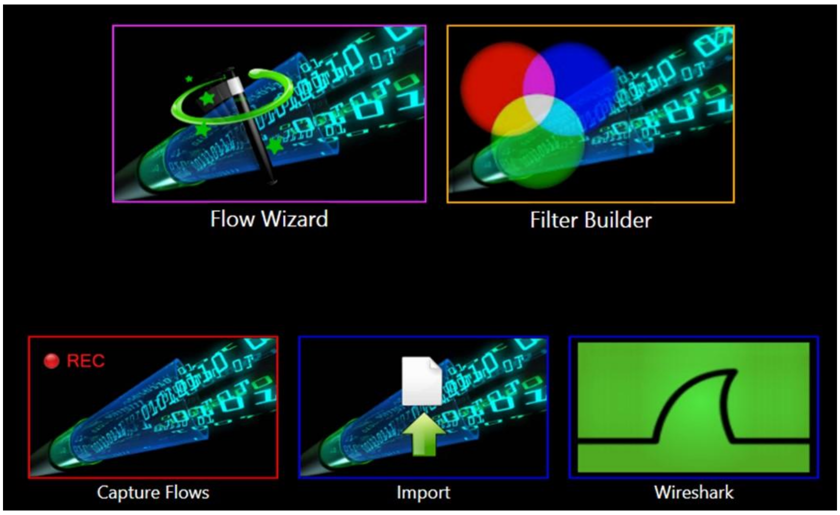
Specific traffic flows can be selected by applying one or more filters to the incoming traffic.

- To access Flow Filters click on **Select Flows** as shown below.



Fixed Delay and Jitter (µs):
Available: 80000000.0
Used: 0.0

The Flow Filter Launch window shown below will appear giving access to various functions.



From this Launch Window 5 functions can be launched;

- **Flow Wizard**
  Flow Wizard is a tool that automatically detects traffic flows in the incoming Ethernet signal and presents these flows to the user for easy creation of filters based on those detected flows. Flow wizard operates on “all packet” capture of the incoming traffic. If

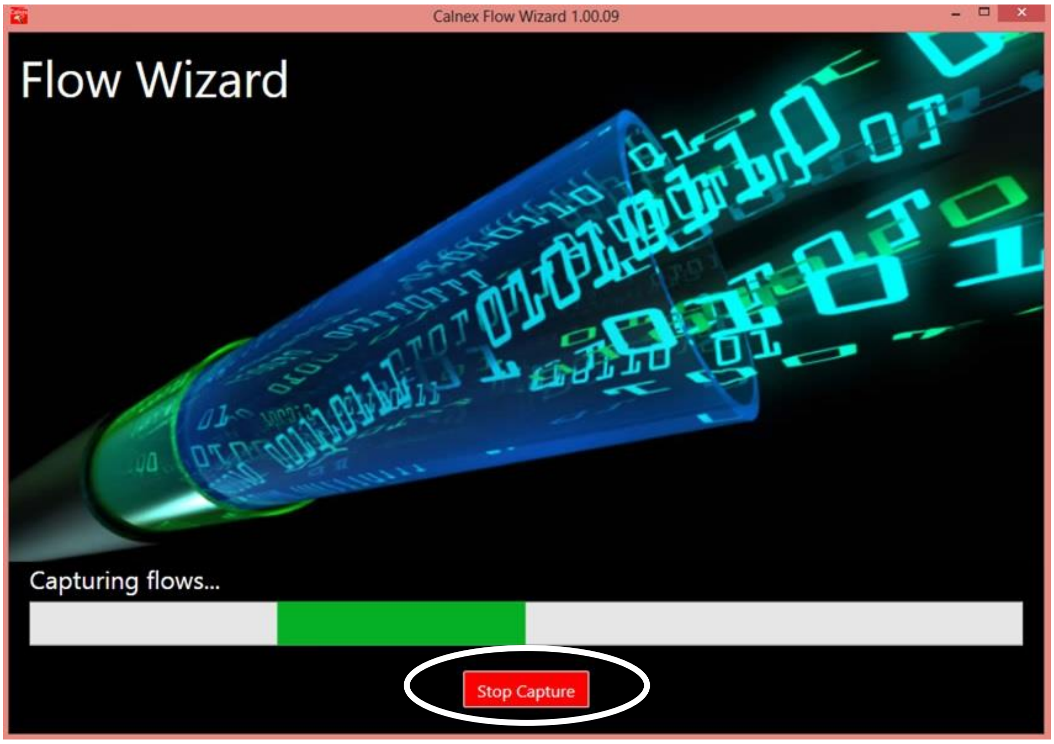
capture data is not currently held in memory a new data capture will be automatically started when Flow Wizard is selected.

- **Filter Builder**
  Filter Builder provides a manual method to create filters based on user input to select protocol structure and the value of key fields for example IP Source and IP Destination addresses.
- **Capture Flows**
  Initiates an “all packet” capture. This captures all packets being received at the Ethernet ports. Capture files can be saved using File->Export or analysed using Wireshark.
- **Import**
  Allows the user to import previously saved “all packet” capture files (.cpd) for protocol and network delay analysis, or to import PCAP files to quickly set Flow Filters based on the previously captured traffic. Previously saved Flow Filter files can also be imported. Import/Export of Flow Filters is described in Appendix 3 - Other Features and Functions.
- **Wireshark**
  Opens the Wireshark application software and automatically decodes the current capture file held in memory. If an “all packet” capture is not currently held in memory, a new capture will automatically start.

There are 3 methods to create Flow Filters; these are **Flow Wizard**, **Filter Builder** and **Import from PCAP** (these are described briefly above). All 3 methods can be used individually or in any combination to create the desired list of Flow Filters. The total size of all filters must not exceed 128 Bytes. Each filter must be set within the first 256 Bytes of the Ethernet packets.

Using Flow Wizard to Create and Set Filters

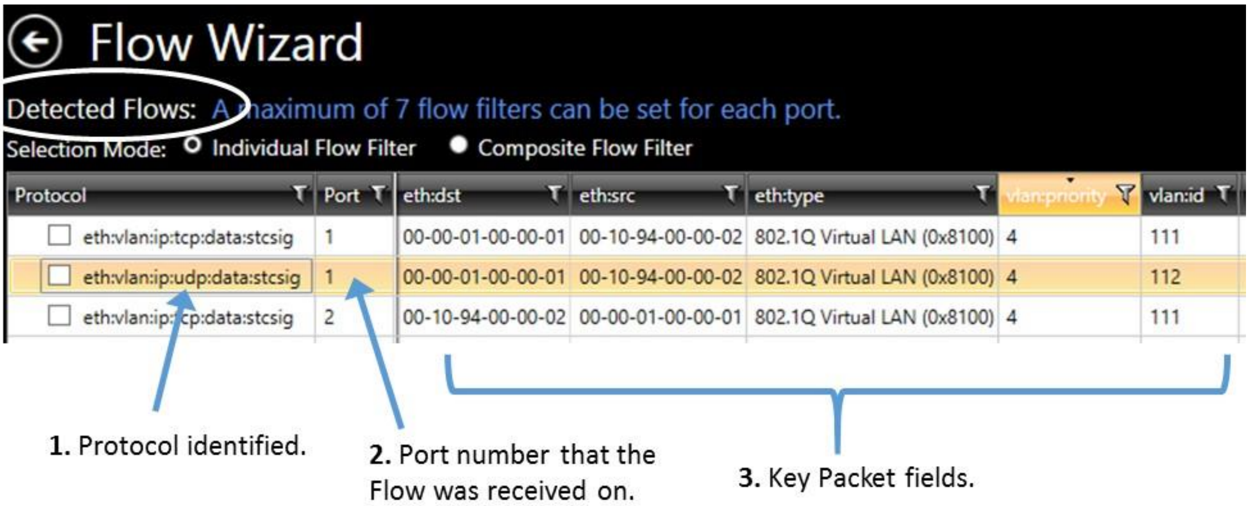
- Click on **Flow Wizard** shown encircled in the graphic on the previous page to start an All Packet Capture, then click on the **Stop Capture** button (shown encircled below) after a few seconds.



- During this capture period the Paragon-X will capture all packets of the traffic on its active ports. Once the capture has been stopped a “Packet Capture Data File” (or PCAP file) is generated.

Note: If a capture has been previously run Flow Wizard will analyse that data rather than start a new capture. To force a new capture of data, click on **Capture Flows**.

The captured traffic and detected protocols will be extracted from the PCAP file and displayed automatically in the format shown below.



Flow Wizard

Detected Flows: A maximum of 7 flow filters can be set for each port.

Selection Mode: ○ Individual Flow Filter ● Composite Flow Filter

Protocol	Port	eth:dst	eth:src	eth:type	vlan:priority	vlan:id
□ eth:vlan:ip:tcp:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	4	111
□ eth:vlan:ip:udp:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	4	112
□ eth:vlan:ip:tcp:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	802.1Q Virtual LAN (0x8100)	4	111

The Flow Wizard window is split in to two panes; **Detected Flows** of captured traffic are listed in the table in the upper pane of the window as shown above. Key packet information fields are provided for each detected flow to allow the user to identify the traffic type and its characteristics making it easier to set the appropriate filter criteria. The lower pane lists **Flow Filters** that the user has selected, or **Configured,** from the upper pane. The lower pane is shown on the next page in Figure 4.1

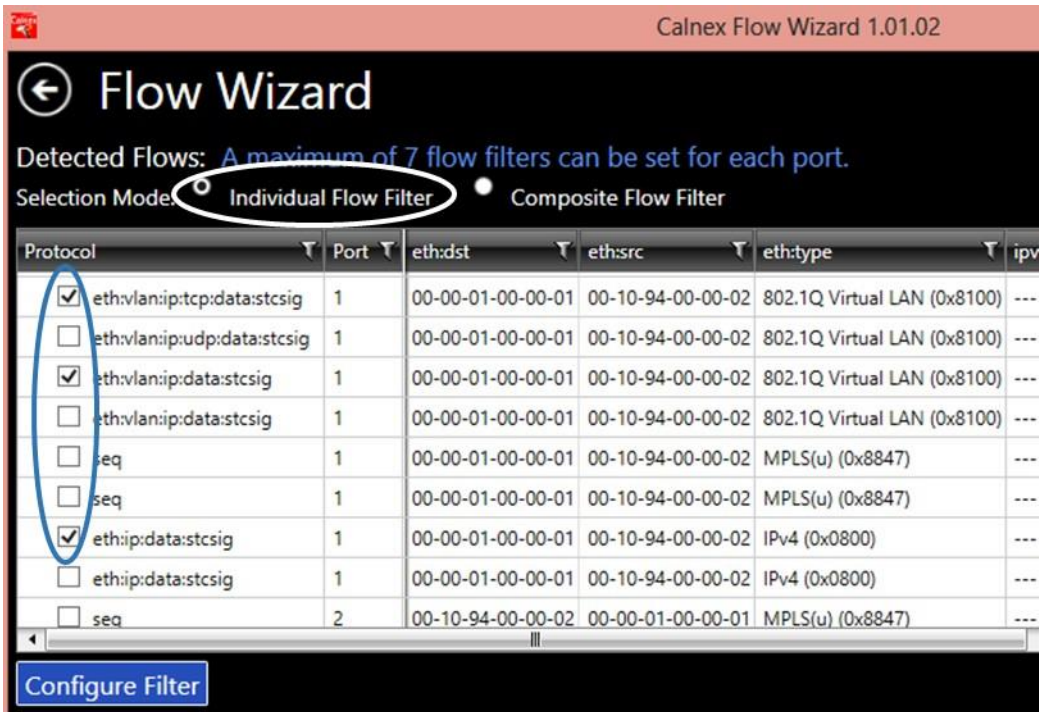
Note: The window split between upper and lower panes can be adjusted by clicking and dragging the grey window divider. Additional windows features are included to optimise viewing the Flow Wizard tables. These are explained in Appendix 2 – Optimizing Flow Wizard Window Viewing Features.

1. The protocol identified for each Flow adopts the Wireshark naming convention.
   For example **eth:ip:data** represents an Ethernet packet containing an Internet Protocol header with a Data Payload.
2. The instrument port number that the Detected Flow was received on indicates the direction of each flow.
3. The Key Packet fields provide the byte values detected in each key field of the packet.
   Where applicable a “decode” of the bytes is also included.
   For example **IPv4 (0x0800)**.
   The Key Packet fields are dynamically displayed depending on the protocol detected.
   For example fields like **vlan:id** and **vlan:priority** are only displayed if a **vlan** protocol is detected within the captured traffic. This reduces the overall number of fields displayed allowing the user to easily locate fields of interest.

There are 2 Modes of selecting Flow Filters; An **Individual Flow Filter** can be created by selecting any one detected flow while a **Composite Flow Filter** can be created from several detected flows. Any combination of Individual Flow Filters and Composite Flow Filters can be created (or “Set”) up to an overall total of 7 for each port. Each Filter that is set is given an associated user configurable Impairment Profile.
Note: the number of available Filters/Profiles per port is dependent on the options fitted.

Setting Individual Filters

- To set an **Individual Flow Filter** click on ○ Individual Flow Filter then click on the checkbox of the Flow(s) to be chosen. Example shown below.



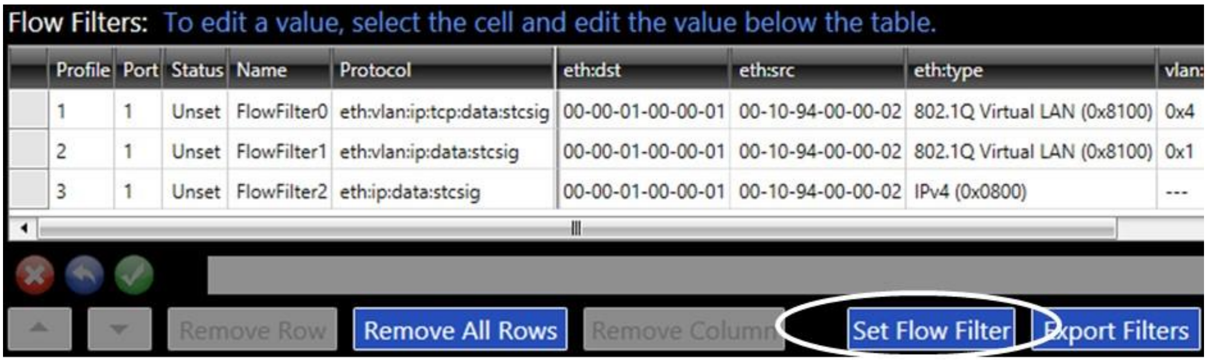
Detected Flows: A maximum of 7 flow filters can be set for each port.

Selection Mode: ○ Individual Flow Filter ● Composite Flow Filter

	Protocol	Port	eth:dst	eth:src	eth:type	ipv
☑	eth:vlan:ip:tcp:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---
□	eth:vlan:ip:udp:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---
☑	eth:vlan:ip:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---
□	eth:vlan:ip:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---
□	seq	1	00-00-01-00-00-01	00-10-94-00-00-02	MPLS(u) (0x8847)	---
□	seq	1	00-00-01-00-00-01	00-10-94-00-00-02	MPLS(u) (0x8847)	---
☑	eth:ip:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---
□	eth:ip:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---
□	seq	2	00-10-94-00-00-02	00-00-01-00-00-01	MPLS(u) (0x8847)	---

- Now click on Configure Filter .

- The selected Flow Filters appear in the lower pane of the Flow Wizard window as shown below. Other Filters can be added using FilterBuilder and/or Importing from a PCAP file (see page 22 for full details).



Flow Filters: To edit a value, select the cell and edit the value below the table.

Profile	Port	Status	Name	Protocol	eth:dst	eth:src	eth:type	vlan:
1	1	Unset	FlowFilter0	eth:vlan:ip:tcp:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	0x4
2	1	Unset	FlowFilter1	eth:vlan:ip:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	0x1
3	1	Unset	FlowFilter2	eth:ip:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---

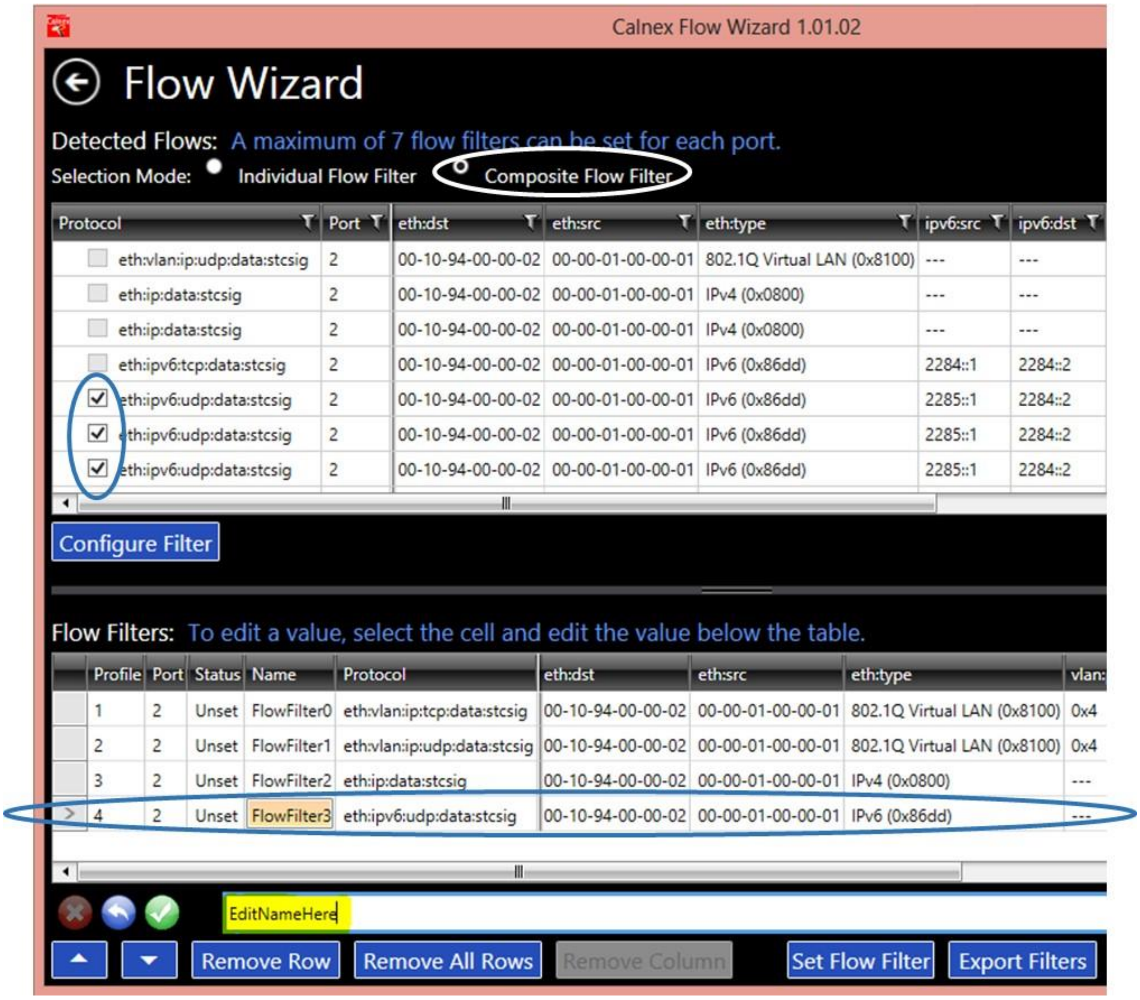
Figure 4.1

- The packet characteristics, or criteria, of each filter is detailed in the various field columns as shown in Figure 4.1 on the previous page. These are the fields/values that incoming traffic will be matched against once the filters are set in the instrument hardware.
- When all desired Filters have been configured. Click on Set Flow Filter as shown in Figure 4.1 on the previous page. The Filters in the instrument hardware will now be set.
  Note: Filters can be configured using Flow Wizard, Filter Builder or Import from PCAP. It is only necessary to **Set Flow Filter** once after all Filters have been configured.

Setting Composite Filters

To set a **Composite Flow Filter** click on ○ Composite Flow Filter then select a combination of flows by clicking on the appropriate checkboxes. Note that only flows of the same packet structure can be combined to create a Composite Flow Filter. For example multiple IP flows can be used to create a Composite Filter, but an IP flow and VLAN flow cannot be combined.

- Now click on Configure Filter .
- The new Composite Flow Filter is appended to the list of Flow Filters in the lower pane of the Flow Wizard window as shown encircled below. Repeat to add more Composite Filters as required.



Detected Flows: A maximum of 7 flow filters can be set for each port.

Selection Mode: ● Individual Flow Filter ○ Composite Flow Filter

Protocol	Port	eth:dst	eth:src	eth:type	ipv6:src	ipv6:dst
□ eth:vlan:ip:udp:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	802.1Q Virtual LAN (0x8100)	---	---
□ eth:ip:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	IPv4 (0x0800)	---	---
□ eth:ip:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	IPv4 (0x0800)	---	---
□ eth:ipv6:tcp:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	IPv6 (0x86dd)	2284::1	2284::2
☑ eth:ipv6:udp:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	IPv6 (0x86dd)	2285::1	2284::2
☑ eth:ipv6:udp:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	IPv6 (0x86dd)	2285::1	2284::2
☑ eth:ipv6:udp:data:stcsig	2	00-10-94-00-00-02	00-00-01-00-00-01	IPv6 (0x86dd)	2285::1	2284::2

Flow Filters: To edit a value, select the cell and edit the value below the table.

	Profile	Port	Status	Name	Protocol	eth:dst	eth:src	eth:type	vlan:
	1	2	Unset	FlowFilter0	eth:vlan:ip:tcp:data:stcsig	00-10-94-00-00-02	00-00-01-00-00-01	802.1Q Virtual LAN (0x8100)	0x4
	2	2	Unset	FlowFilter1	eth:vlan:ip:udp:data:stcsig	00-10-94-00-00-02	00-00-01-00-00-01	802.1Q Virtual LAN (0x8100)	0x4
	3	2	Unset	FlowFilter2	eth:ip:data:stcsig	00-10-94-00-00-02	00-00-01-00-00-01	IPv4 (0x0800)	---
>	4	2	Unset	FlowFilter3	eth:ipv6:udp:data:stcsig	00-10-94-00-00-02	00-00-01-00-00-01	IPv6 (0x86dd)	---

EditNameHere

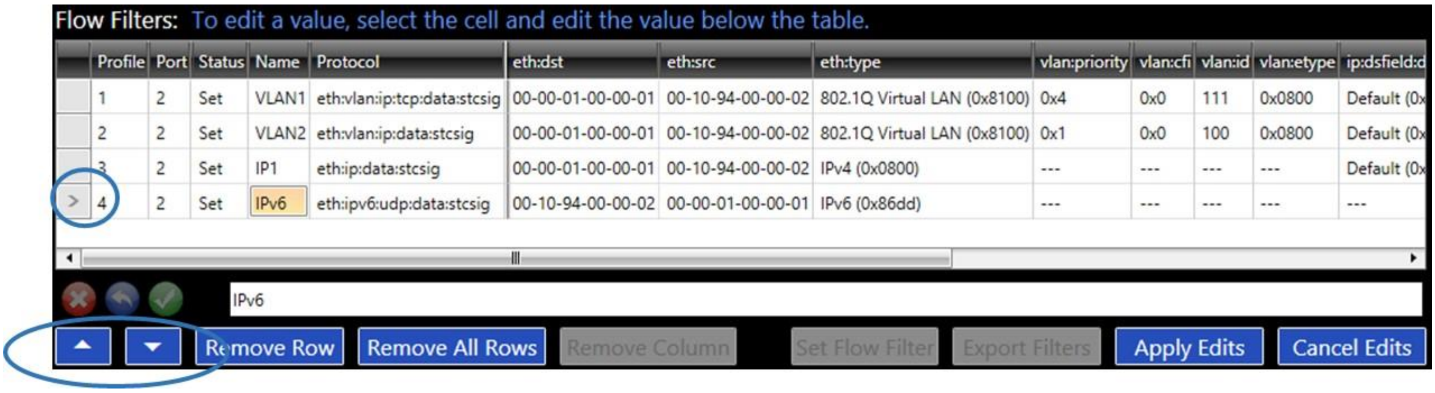
- When all desired Filters have been configured. Click on Set Flow Filter .

Naming or Editing a Profile

- To name a Profile click on the **Name** field then edit the default name in the "Edit Line" shown highlighted in yellow above. Now click on ✓ to complete the change or click on ↶ to undo the change. Profile names are limited to 12 characters (Alphanumeric and underscore, no spaces allowed).
- Each Profile can be named, for example we could name Profiles 1 -4; VLAN1, VLAN2, IP1 and IPv6 respectively as shown in the graphic below.
- Other fields, such as IP Destination Address, can be edited in the same way as the Name field.
- The Port (or direction) that the filter applies to can be edited in the same way as above.

Setting the Priority of Filters

The Flow Filters are listed in priority order (Profile 1 is highest priority). The priority can be raised or lowered by clicking on the left-hand side of a specific filter row (shown encircled below) then using the ▲ ▼ buttons to increase or decrease the priority of that filter.



Flow Filters: To edit a value, select the cell and edit the value below the table.

	Profile	Port	Status	Name	Protocol	eth:dst	eth:src	eth:type	vlan:priority	vlan:cfi	vlan:id	vlan:etype	ip:dsfield:d
	1	2	Set	VLAN1	eth:vlan:ip:tcp:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	0x4	0x0	111	0x0800	Default (0x
	2	2	Set	VLAN2	eth:vlan:ip:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	0x1	0x0	100	0x0800	Default (0x
	3	2	Set	IP1	eth:ip:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---	---	---	---	Default (0x
>	4	2	Set	IPv6	eth:ipv6:udp:data:stcsig	00-10-94-00-00-02	00-00-01-00-00-01	IPv6 (0x86dd)	---	---	---	---	---

IPv6

Note that there are 2 separate orders of priority, one for Port 1 Filters and another for Port 2 Filters.

- Once all edits to the Flow Filters are complete click on the Apply Edits button to update the filter settings in the instrument hardware.

Removing Filters

A single Filter can be removed by clicking on the Filter row in the Flow Filters Table, then clicking on the **Remove Row** button. All Filters can be removed by clicking on the **Remove All Rows** button. The location of these buttons is shown in the graphic above.

Removing a Field from a Filter

Note: the following operation is not reversible;
To remove an individual field from a filter. Click on the field to be removed and then click on ☒ This has the effect of "widening" the filter allowing more traffic to pass through the associated Profile.

Removing Columns from the Set Filters table

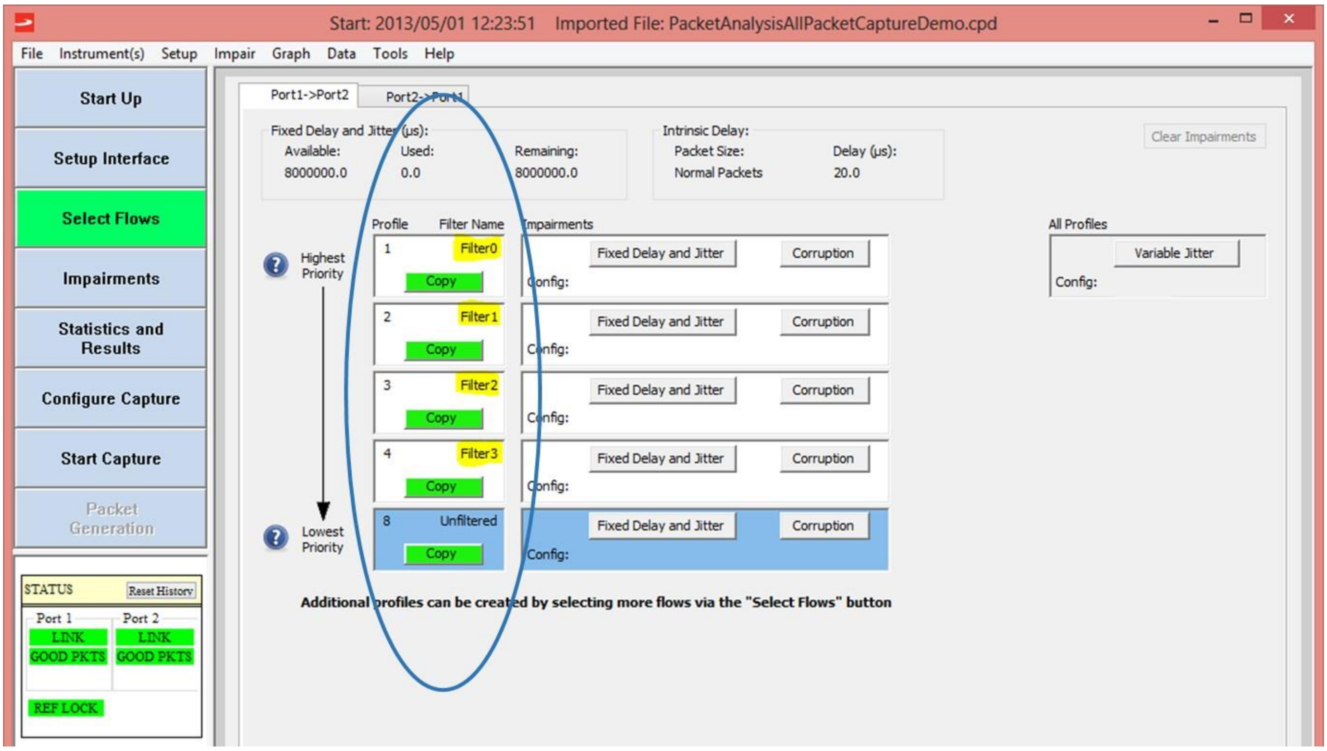
It is possible to remove a column from the table by right-clicking the mouse on the column. This pops-up a button as shown which can be clicked to remove the column. Remove Column

After all the desired Filters have been **Configured** and **Set** it is not necessary to close the Flow Wizard window, but if the window is closed it can be re-opened if subsequently required by clicking on **Select Flows**, then clicking on **Flow Wizard**.

Note: It is possible to open the Wireshark application to view the protocol decode of traffic at any time after the "all packet" capture has completed. It is also possible to have both Wireshark and Flow Wizard applications open at the same time.

Note: Additional filters can be added retrospectively by returning to **Flow Wizard, Filter Builder** or **Import**.

- Return to the Network Emulation window to see a summary of the Filters and Profiles set as shown below.



Start: 2013/05/01 12:23:51 Imported File: PacketAnalysisAllPacketCaptureDemo.cpd

Fixed Delay and Jitter (µs):
Available: 8000000.0
Used: 0.0
Remaining: 8000000.0

Intrinsic Delay:
Packet Size: Normal Packets
Delay (µs): 20.0

Profile	Filter Name	Impairments
1	Filter0	Fixed Delay and Jitter, Corruption
2	Filter1	Fixed Delay and Jitter, Corruption
3	Filter2	Fixed Delay and Jitter, Corruption
4	Filter3	Fixed Delay and Jitter, Corruption
8	Unfiltered	Fixed Delay and Jitter, Corruption

All Profiles: Variable Jitter

Additional profiles can be created by selecting more flows via the "Select Flows" button

The summary above illustrates the Priority of Profiles (highest = Profile 1), and the Filters associated with each Profile. Profile 8 represents all traffic received that does not match any of the set Filters on Profiles 1 through 4.

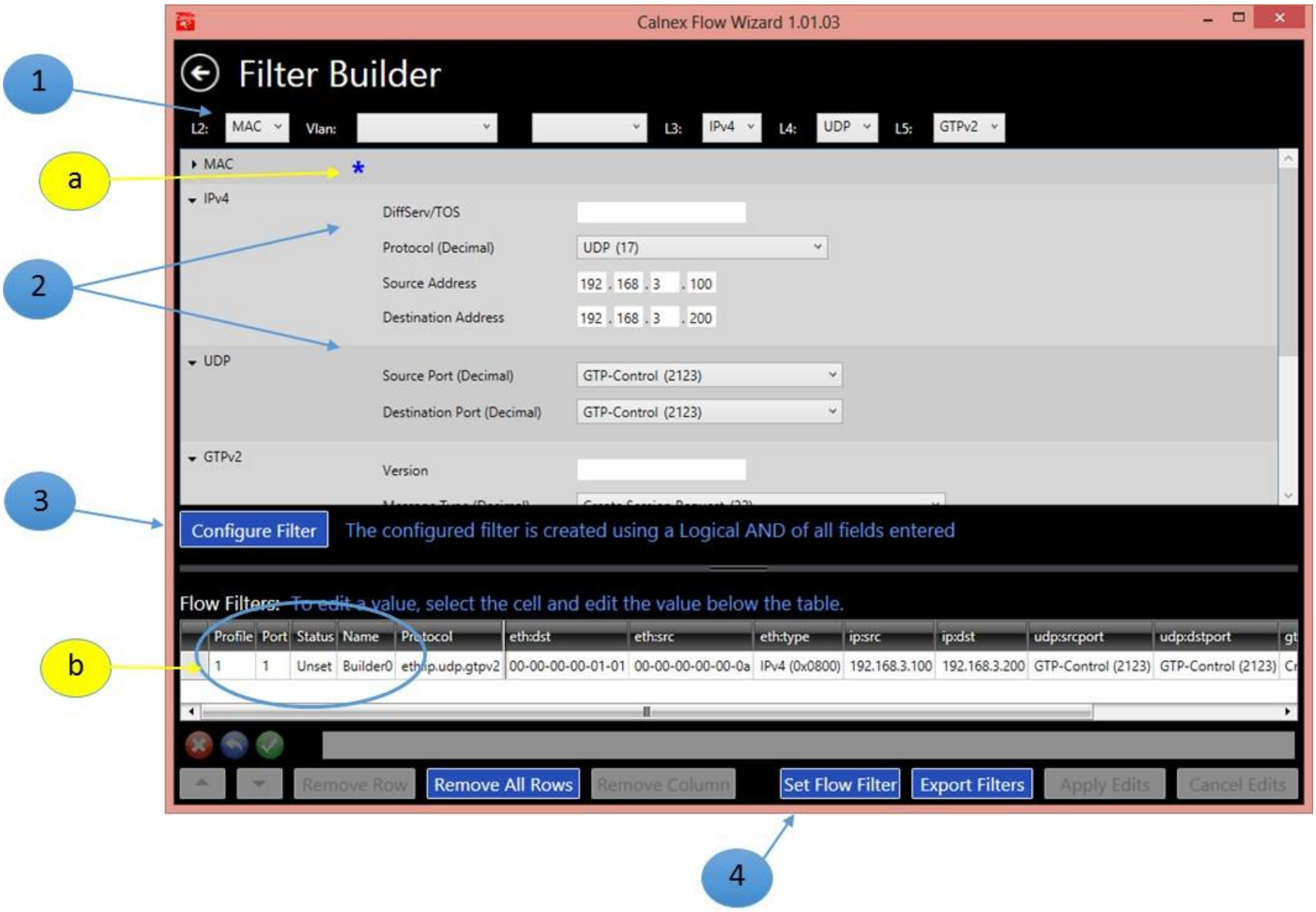
The Filter Names (highlighted in yellow above) are set in Flow Wizard. It is possible to return to Flow Wizard and edit the names to make the Filters and Profiles easy to identify, or to change the priority of the profiles.
Note: To access Flow Wizard click on **Select Flows**.

The graphic above illustrates the Profiles set in direction Port1->Port2. Click on the Port2->Port1 tab to see the Profiles set in the opposite direction.

Using Filter Builder to Create Filters

Creating Filters using **Filter Builder** involves manually configuring the expected protocol structure, then selecting and defining values for key fields.

- Click on **Select Flows**, then select **Filter Builder**. The following window is displayed;



Calnex Flow Wizard 1.01.03

Filter Builder

L2: MAC Vlan: L3: IPv4 L4: UDP L5: GTPv2

MAC *

IPv4
- DiffServ/TOS:
- Protocol (Decimal): UDP (17)
- Source Address: 192 . 168 . 3 . 100
- Destination Address: 192 . 168 . 3 . 200

UDP
- Source Port (Decimal): GTP-Control (2123)
- Destination Port (Decimal): GTP-Control (2123)

GTPv2
- Version:

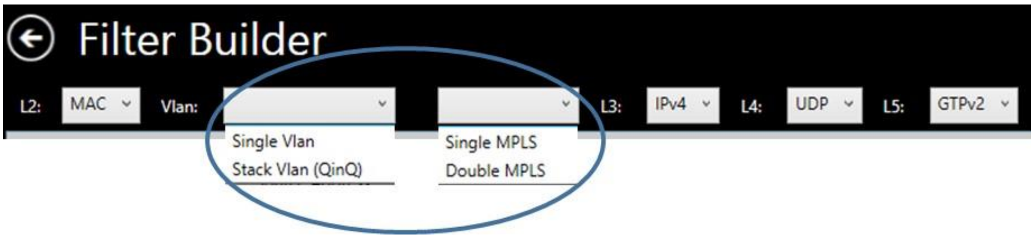
Configure Filter The configured filter is created using a Logical AND of all fields entered

Flow Filters: To edit a value, select the cell and edit the value below the table.

Profile	Port	Status	Name	Protocol	eth:dst	eth:src	eth:type	ip:src	ip:dst	udp:srcport	udp:dstport	gt
1	1	Unset	Builder0	eth.ip.udp.gtpv2	00-00-00-00-01-01	00-00-00-00-00-0a	IPv4 (0x0800)	192.168.3.100	192.168.3.200	GTP-Control (2123)	GTP-Control (2123)	Cr

Remove Row Remove All Rows Remove Column Set Flow Filter Export Filters Apply Edits Cancel Edits

1. First set the Layers in the protocol stack using the drop-lists across the top of the **Filter Builder** window. It is important to set whether or not VLANs and/or MPLS labels are present in the structure (as shown below) as this affects the starting byte position of Layer 3.

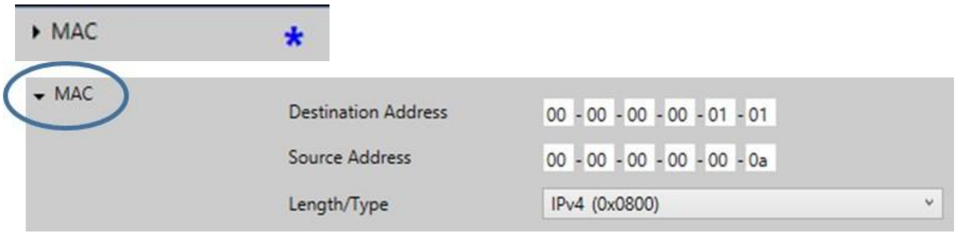


Filter Builder

L2: MAC Vlan: L3: IPv4 L4: UDP L5: GTPv2

Note that setting VLAN or MPLS in the drop-lists shown above does not set the Length/Type field. This needs to be set manually in Step 2 below.

2. Now enter the field details to be filtered. Fields can be expanded and collapsed by clicking on the Field Header (MAC example shown encircled below).

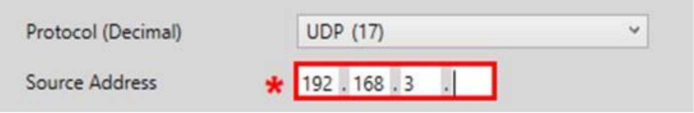


MAC *

MAC
- Destination Address: 00 - 00 - 00 - 00 - 01 - 01
- Source Address: 00 - 00 - 00 - 00 - 00 - 0a
- Length/Type: IPv4 (0x0800)

A blue asterisk indicates that a collapsed Field Header has an entry – example shown below and annotated "a" on the previous page.

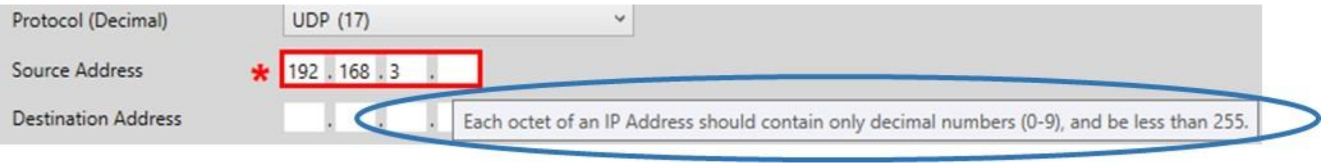
If an invalid, incomplete or out-of-range value is entered in any field a red asterisk is displayed as shown below.



Protocol (Decimal) UDP (17)

Source Address * 192 . 168 . 3 .

Hovering the mouse over the field displays the value range information as shown encircled below.



Protocol (Decimal) UDP (17)

Source Address * 192 . 168 . 3 .

Destination Address . . .

Each octet of an IP Address should contain only decimal numbers (0-9), and be less than 255.

3. Click on **Configure Filter**. The Filter created is the logical AND of all fields entered.
   (Repeat to add more Filters. You can also add Filters from Flow Wizard).
   The Filter direction (Port) can be edited – annotated “b” on the previous page.

4. Click on **Set Flow Filter** when all desired filters have been configured.
   When the filters are Set the status field changes from ”Unset” to “Set”.
   Filters created using Filter Builder are given default names “Builder0” etc to distinguish them from those created using Flow Wizard.

Filter Builder protocol field definitions, ranges and units are shown below.

Header	**Field Name**	**Definition**	**Range (units)**
MAC	Source Address Destination Address Length/Type	6 One-byte fields 6 One-byte fields Drop-List	00 to ff (hex) 00 to ff (hex) 0x0 to 0xffff (hex)
VLAN	Priority VLAN ID Type (TPID)	Value Value Value	0x0 to 0x7 (hex) 0 to 4095 (decimal) 0x0 to 0xffff (hex)
MPLS	Label	Value	0x0 to 0xfffff (hex)
IPv4	DiffServ/TOS Protocol Source Address Destination Address	Value Drop-List 4 fields 4 fields	0x0 to 0xff (hex) 0 to 255 (decimal) 0-255 (decimal) 0-255 (decimal)
IPv6	Source Address Destination Address	8 x 2-byte fields 8 x 2-byte fields	00 to ff (hex) 00 to ff (hex)
TCP/UDP	Source Port Destination Port	Drop-List Drop-List	0 to 65535 (decimal) 0 to 65535 (decimal)
GTPv2	Version Message Type Tunnel Endpoint ID	Value Drop-List Value	0x0 to 0x7 (hex) 0 to 255 (decimal) 0x0 to 0xffffffff (hex)
Custom Byte Offsets	L2 Offset L3 Offset 1 Byte Mask 4 Byte Mask 1 Byte Value 4 Byte Value	Value Value Byte Mask Byte Mask Byte Value Byte Value	0 to 31 (decimal) 0 to 225 (decimal) 0x0 to 0xff (hex) 0x0 to 0xffffffff (hex) 0x0 to 0xff (hex) 0x0 to 0xffffffff (hex)

Creating Filters from an Imported PCAP file

Filters can be created by importing a previously captured PCAP file.

- Click on **Select Flows**, then select **Import**.
- Now select the desired PCAP file and click **Open**.
- The flow information from the PCAP file is automatically displayed in Flow Wizard upper pane.
- Now follow the process for Flow Wizard (page 17) to set the desired Filters.

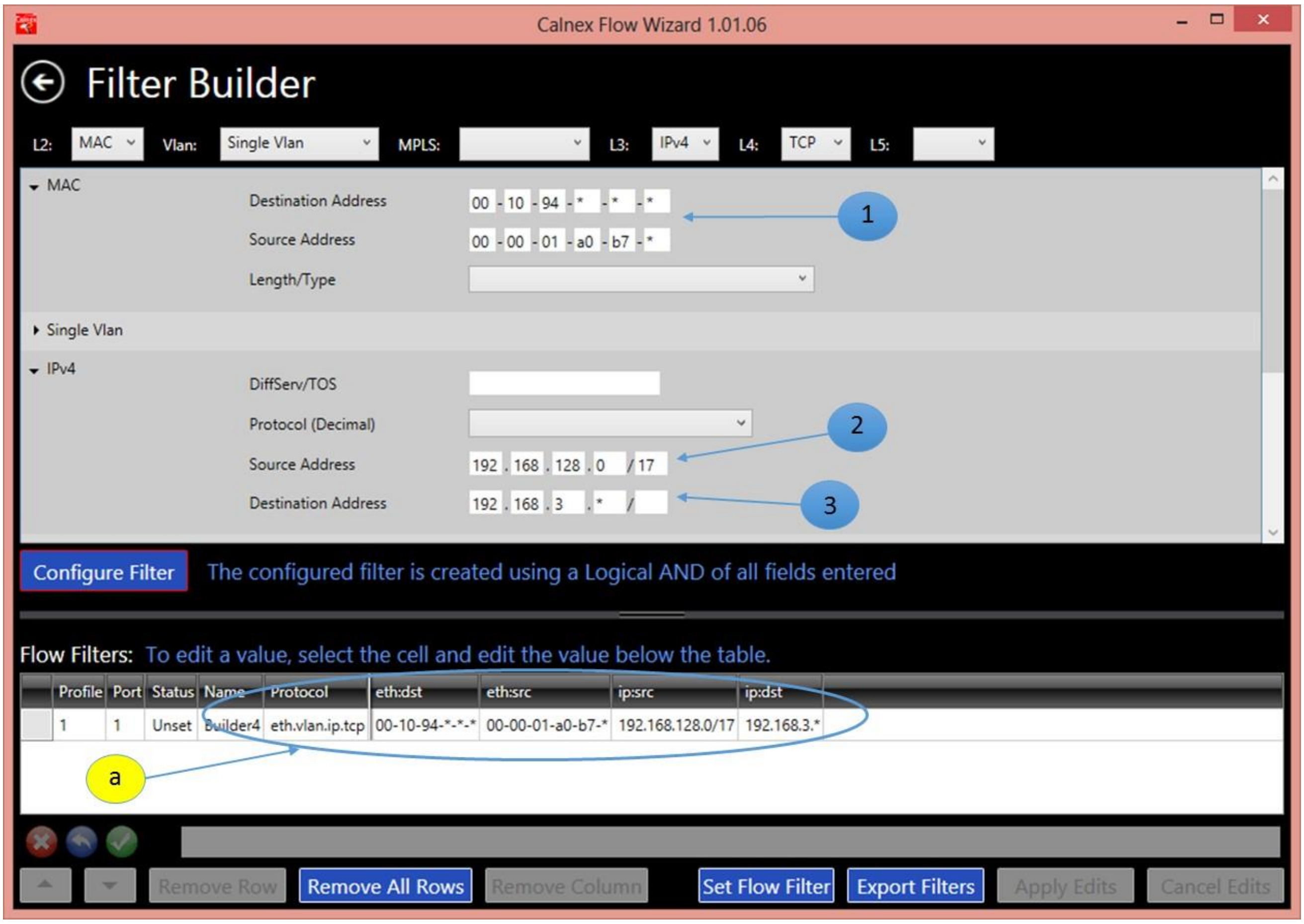
Filters created using Filter builder or from Imported PCAP files can be edited in the same way as described in the previous section on Flow Wizard.

Filters set using Filter builder or from Imported PCAP files appear in the Profile Summary in the same way as those created using Flow Wizard.

Filter Ranges and Wildcards

Filters created by Flow Wizard or Filter Builder, or by importing a PCAP, can include ranges and wildcards expanding the filter criteria to match a wider range of traffic. One example is to filter on a range of IP addresses (or a subnet of IP addresses). Another example is to filter on a contiguous range of VLAN ID’s or a non-contiguous range of IP addresses.

Entering a subnet range of IP addresses and entering wildcards using Filter Builder



L2: MAC Vlan: Single Vlan MPLS: L3: IPv4 L4: TCP L5:

MAC
Destination Address 00 - 10 - 94 - * - * - *
Source Address 00 - 00 - 01 - a0 - b7 - *
Length/Type

Single Vlan

IPv4
DiffServ/TOS
Protocol (Decimal)
Source Address 192 . 168 . 128 . 0 / 17
Destination Address 192 . 168 . 3 . * /

The configured filter is created using a Logical AND of all fields entered

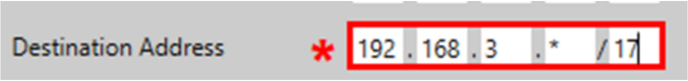
Flow Filters: To edit a value, select the cell and edit the value below the table.

	Profile	Port	Status	Name	Protocol	eth:dst	eth:src	ip:src	ip:dst
	1	1	Unset	Builder4	eth.vlan.ip.tcp	00-10-94-*-*-*	00-00-01-a0-b7-*	192.168.128.0/17	192.168.3.*

1. Annotation “1” above illustrates how to enter **wildcards** in the MAC Destination and Source Address fields. A wildcard is entered using the ***** character (asterisk). It can be entered in any combination of MAC address fields. Each wildcard matches any byte value for that part of the address field.
2. Annotation “2” illustrates how to enter a **range** of IPv4 Source Addresses. The address is entered in dot-decimal notation followed by an optional CIDR (Classless Inter-Domain Routing). Entering the address without CIDR will set one unique IP address to be used. Entering with a CIDR value will set a range of IP address values.
The above example illustrates an IP Source Address of 192.168.128.0 with a CIDR value of 17 bits. This will set a range of IP Source Addresses from 192.168.128.0 through to 192.168.255.255 - that is 32,768 contiguous addresses.
A smaller address range can be set by using a <u>bigger</u> CIDR value.
E.g. 192.168.128.0/24 covers the range 192.168.128.0 through 192.168.128.255 (A range of 256 contiguous IP addresses).

3. Annotation “3” on the previous page illustrates how to enter **wildcards** in the IP Destination Address fields. A wildcard is entered using the * character (asterisk). It can be entered in any combination of IP address fields. Each wildcard matches any byte value for that part of the address field.

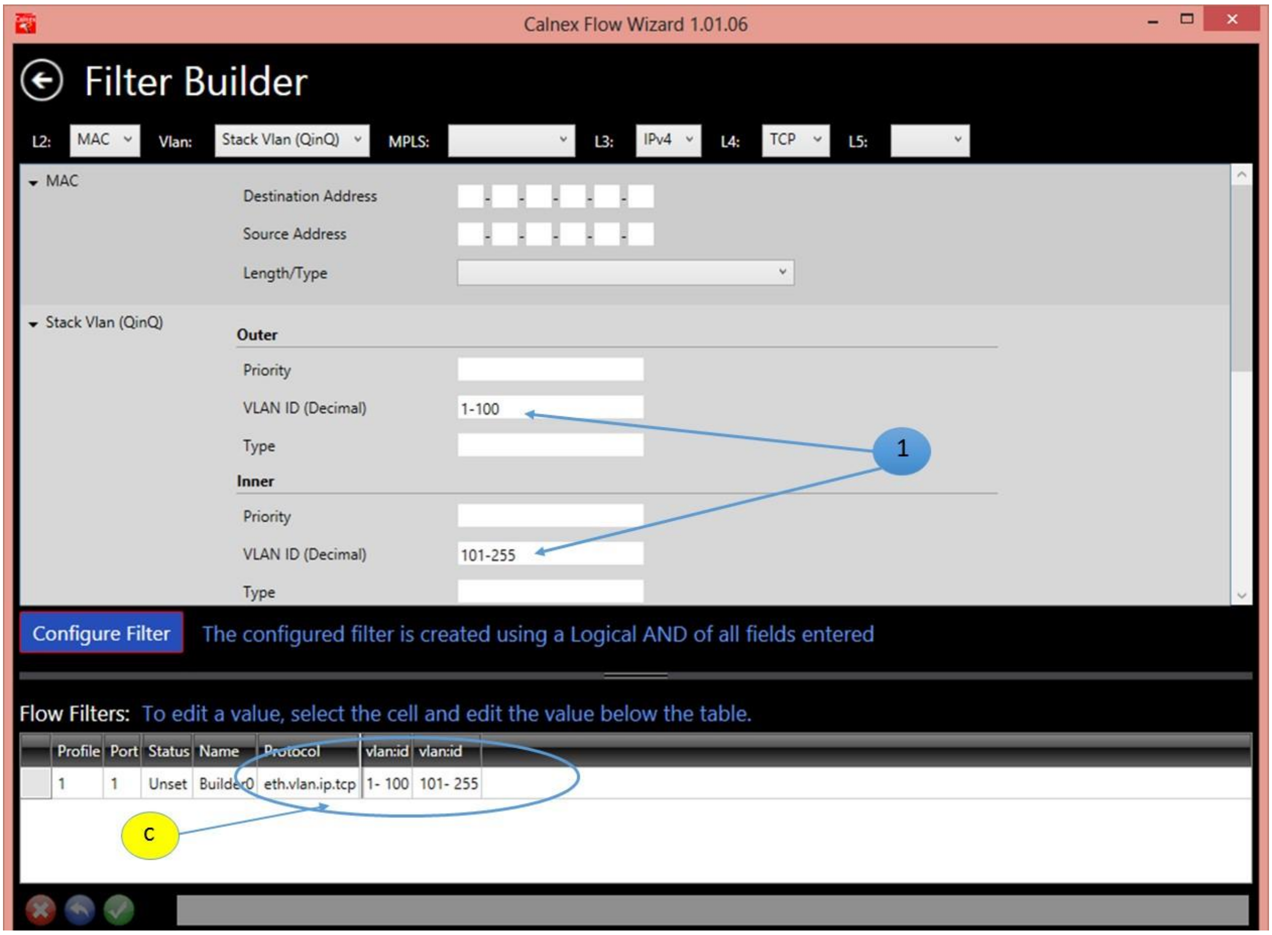
   Note that wildcards and CIDRs are mutually exclusive on the same IP Address field; for example 192.168.3.*/17 is not allowed.



Destination Address * 192 . 168 . 3 . * / 17

4. IPv6 Address fields also accept wildcards and CIDR ranges in the same way as IPv4 Address fields.
5. Wildcards and CIDR ranges can also be entered directly into Flow Wizard by editing the Filter fields as shown on the previous page (annotated “a”).
6. Non-contiguous ranges of IP addresses and MAC addresses can also be entered using Flow Wizard. The range is entered using commas to separate the values. The range must be within the same Octet/Byte. (E.g. 192.168.100.1, 192.168.100.5, 192.168.100.255)

Entering a VLAN ID range



Calnex Flow Wizard 1.01.06

Filter Builder

L2: MAC Vlan: Stack Vlan (QinQ) MPLS: L3: IPv4 L4: TCP L5:

MAC
Destination Address
Source Address
Length/Type

Stack Vlan (QinQ)
Outer
Priority
VLAN ID (Decimal) 1-100
Type
Inner
Priority
VLAN ID (Decimal) 101-255
Type

Configure Filter The configured filter is created using a Logical AND of all fields entered

Flow Filters: To edit a value, select the cell and edit the value below the table.

Profile	Port	Status	Name	Protocol	vlan:id	vlan:id
1	1	Unset	Builder0	eth.vlan.ip.tcp	1- 100	101- 255

1. Enter the **VLAN ID** range in Filter Builder using the “-“ character between the min and max values of the contiguous range as shown in the graphic above annotated “1”.
   A non-contiguous range can also be entered using “,” as a separator. (E.g.   1,3,7,100)

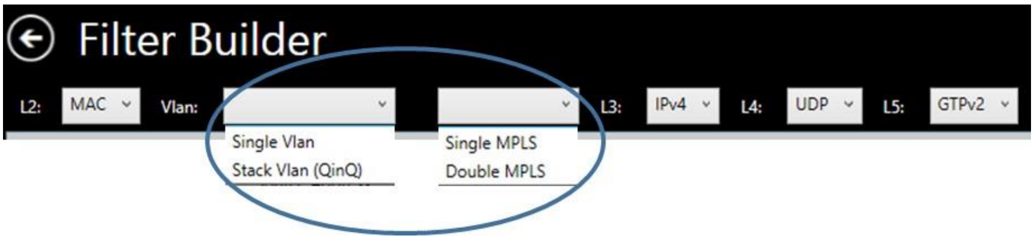
Note that the range must be contiguous and lie within the limits below;
0-255
256-511
512- 767
768-1023
1024-1279
1280-1536
…
…
3583-3838
3839-4095
Any range that crosses over the limit boundaries given above is invalid (e.g. 250-260 is an invalid VLAN ID filter range).

2. A **VLAN ID** range can also be entered directly to Flow Wizard by editing the Filter fields as shown on the previous page (annotated "c").

Custom-Byte Filters

Non-standard protocols can be filtered using Custom Byte Filters. These Filters can match on 1 single byte in the packets or up to 4 consecutive bytes. Up to 5 instances of each type of filter can be created to match on multiple byte locations in the packets.

The Filters are specified by a starting point (Offset from Layer 2 or Layer 3 position), a mask and a value. The Layer 2 or 3 position is determined by the VLAN and MPLS settings along the top line of Filter Builder as shown below.

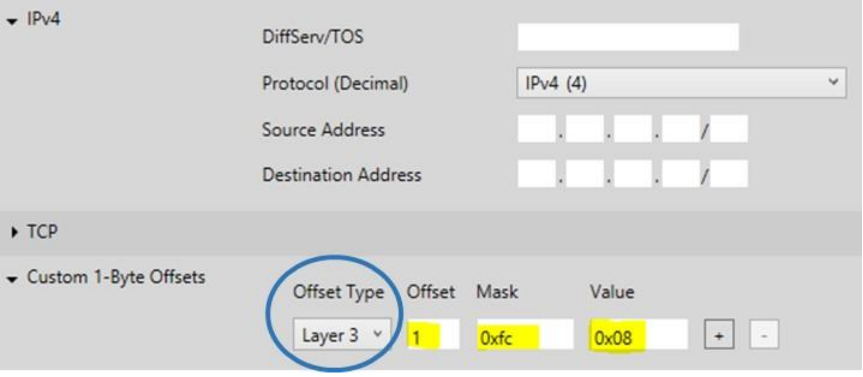


Filter Builder

L2: MAC
Vlan: Single Vlan / Stack Vlan (QinQ) | Single MPLS / Double MPLS
L3: IPv4
L4: UDP
L5: GTPv2

Example Custom-Byte Filter

This example creates a Custom 1-Byte Filter to match a DCSP value of "8" in IPv4 packets.



IPv4
DiffServ/TOS
Protocol (Decimal): IPv4 (4)
Source Address: . . . /
Destination Address: . . . /

TCP

Custom 1-Byte Offsets

Offset Type	Offset	Mask	Value
Layer 3	1	0xfc	0x08

Note that if custom-byte filters are being combined with non-custom-byte filters care should be taken to avoid both types of filter trying to set the same bytes in the filter to different values.

Chapter 5 - Adding Impairments to Selected Traffic

The previous chapter detailed how to set up filters to select specific flows of traffic received at the instrument's Ethernet ports. This chapter describes how to configure and add impairments to the previously selected traffic flows.

Impairments Overview

Paragon-X Network Emulation provides 16 independent Profiles of impairments, 8 in each direction. A combination of impairments can be added to each profile – for example Fixed Delay (latency), Jitter (PDV) and Corruption. The table below shows the valid combinations of impairments that can be applied to each profile (shown in green).

Impairment Matrix	Delay	Jitter (Profile)	Corruptions				Header Overwrite	Physical Corruption	Random Packet Loss	Bandwidth Control	Variable Jitter
			Lost	Errored	Repeat	Misorder					
Delay	🟦	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Jitter (Profile)	🟩	🟦	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟥
Lost	🟩	🟩	🟦	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩
Errored	🟩	🟩	🟩	🟦	🟩	🟩	🟩	🟥	🟩	🟩	🟩
Repeat	🟩	🟩	🟩	🟩	🟦	🟩	🟩	🟥	🟩	🟩	🟩
Misorder	🟩	🟩	🟩	🟩	🟩	🟦	🟩	🟥	🟩	🟩	🟩
Header Overwrite	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟥	🟩	🟩	🟩
Physical Corruption	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟦	🟩	🟩	🟩
Random Packet Loss	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩	🟥
Bandwidth Control	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟦	🟩
Variable Jitter	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟦

Impairments are applied in the following order:

Policer
Lost Packets
Header Overwrite (L2 CRC is recalculated after overwrite)
Errored Packets (L2 CRC is inverted on errored packets)
Misorder Packets
Repeated Packets
Variable Jitter & Random Packet Loss
Delay & Jitter (Profile)
Shaper

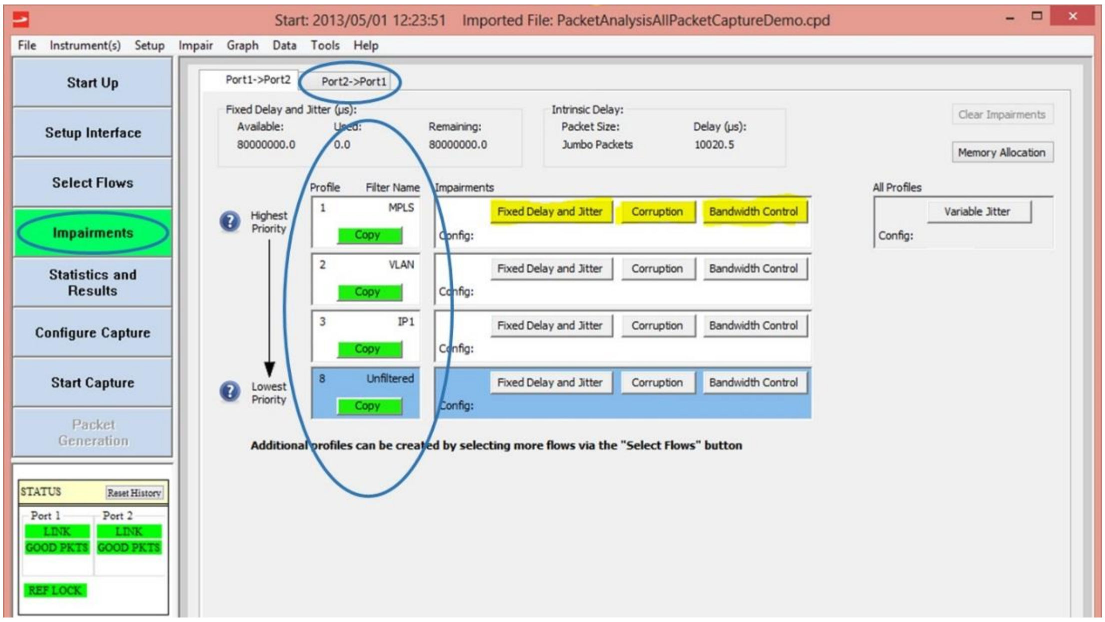
When multiple impairments are applied to the same profile they can affect each other - for example if Errored Packets is combined with Repeated Packets some Errored Packets may also be Repeated.

- Click on the Impairments button as shown encircled below to view a summary of the Profiles that have been set up and to access the impairments configuration.

Figure 5.1 below shows an example where 3 Profiles have been set up for traffic received at the Port 1. The Profiles are numbered 1 to 3 and the associated Flow Filters named as they were during set up in Flow Wizard. Profile 8 represents the remainder of the traffic received at Port 1 that does not match any of the Flow Filter criteria in Profiles 1 through 3.
Note: when there are no Filters set up all traffic flows through Profile 8.

Each Profile has a **Fixed Delay and Jitter, Corruption** and **Bandwidth Control** Impairment element (Profile 1 impairment elements are shown highlighted in yellow in Figure 5.1 below). These elements are used to configure the impairments and to indicate which impairments are enabled/active.

A summary of the Port 2 Profiles can be viewed by clicking on the **Port2->Port1** tab shown encircled below.



Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
80000000.0	0.0	80000000.0

Intrinsic Delay:

Packet Size:	Delay (µs):
Jumbo Packets	10020.5

Profile	Filter Name	Impairments
1	MPLS	Fixed Delay and Jitter, Corruption, Bandwidth Control Config:
2	VLAN	Fixed Delay and Jitter, Corruption, Bandwidth Control Config:
3	IP1	Fixed Delay and Jitter, Corruption, Bandwidth Control Config:
8	Unfiltered	Fixed Delay and Jitter, Corruption, Bandwidth Control Config:

Additional profiles can be created by selecting more flows via the "Select Flows" button

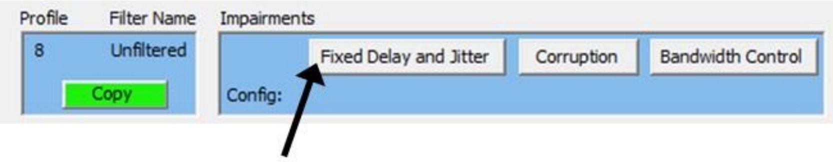
Figure 5.1 Impairments Summary View

Setting the Instrument Intrinsic Delay Value

The instrument hardware processes every packet received at the Ethernet ports. This introduces a small intrinsic delay to the packets while they are buffered within the instrument. To keep this intrinsic delay to a minimum the user is able to set the maximum packet size expected to be received. The user should select small, normal or jumbo packets.

Note that received packets will be dropped if they exceed the selected maximum packet size when set to small or normal packets. Packets exceeding the Jumbo packet size (12000 bytes) are not dropped, but will have intrinsic delay greater than the indicated values.

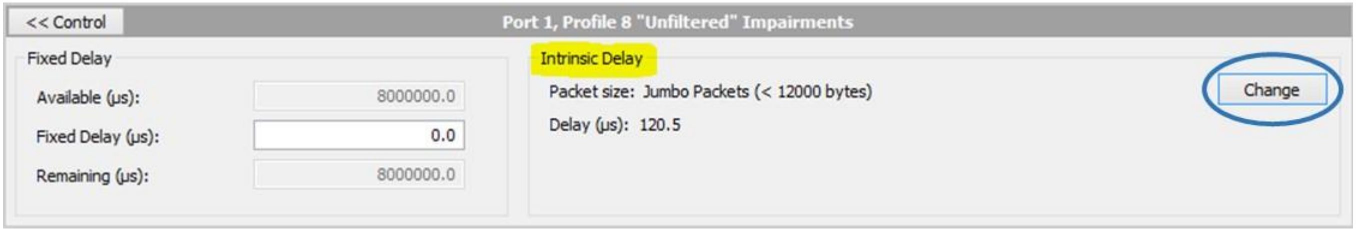
- To change the packet size click on the **Fixed Delay and Jitter** or **Corruption** or **Bandwidth Control** element of any enabled Impairment Profile as shown below.



Profile	Filter Name	Impairments
8	Unfiltered	Config:

Click on **Fixed Delay and Jitter** element.

- Now click on the **Change** button as shown encircled below.



Port 1, Profile 8 "Unfiltered" Impairments

Fixed Delay

Available (μs): 8000000.0

Fixed Delay (μs): 0.0

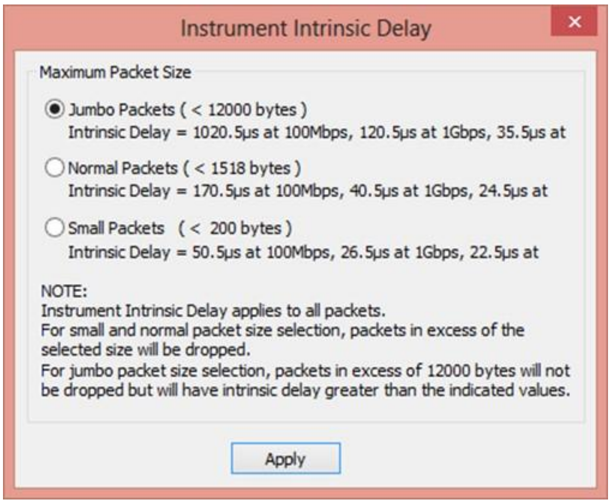
Remaining (μs): 8000000.0

Intrinsic Delay

Packet size: Jumbo Packets (< 12000 bytes)

Delay (μs): 120.5

The following dialog box is then displayed;



Instrument Intrinsic Delay

Maximum Packet Size

● Jumbo Packets (< 12000 bytes)
Intrinsic Delay = 1020.5μs at 100Mbps, 120.5μs at 1Gbps, 35.5μs at

○ Normal Packets (< 1518 bytes)
Intrinsic Delay = 170.5μs at 100Mbps, 40.5μs at 1Gbps, 24.5μs at

○ Small Packets (< 200 bytes)
Intrinsic Delay = 50.5μs at 100Mbps, 26.5μs at 1Gbps, 22.5μs at

NOTE:
Instrument Intrinsic Delay applies to all packets.
For small and normal packet size selection, packets in excess of the selected size will be dropped.
For jumbo packet size selection, packets in excess of 12000 bytes will not be dropped but will have intrinsic delay greater than the indicated values.

Click on the radio button of the appropriate Packet Size then click on **Apply**. The Packet Size and Intrinsic Delay will be updated on screen.

Note that the intrinsic delay values for each packet size are smaller if **Low Intrinsic Mode** is selected. Low Intrinsic Mode is enabled by first clicking on the **Memory Allocation** button. This is discussed in the following section entitled Profile Memory Allocation.

Profile Memory Allocation

Paragon-X Network Emulation provides flexible allocation of its memory block to each Impairment profile. This allows the user to optimise the memory allocation spread across the particular profiles that are in use for the specific application. This section describes the operation in non-Extended Delay Mode.
Extended Delay Mode operation is described in the next section.

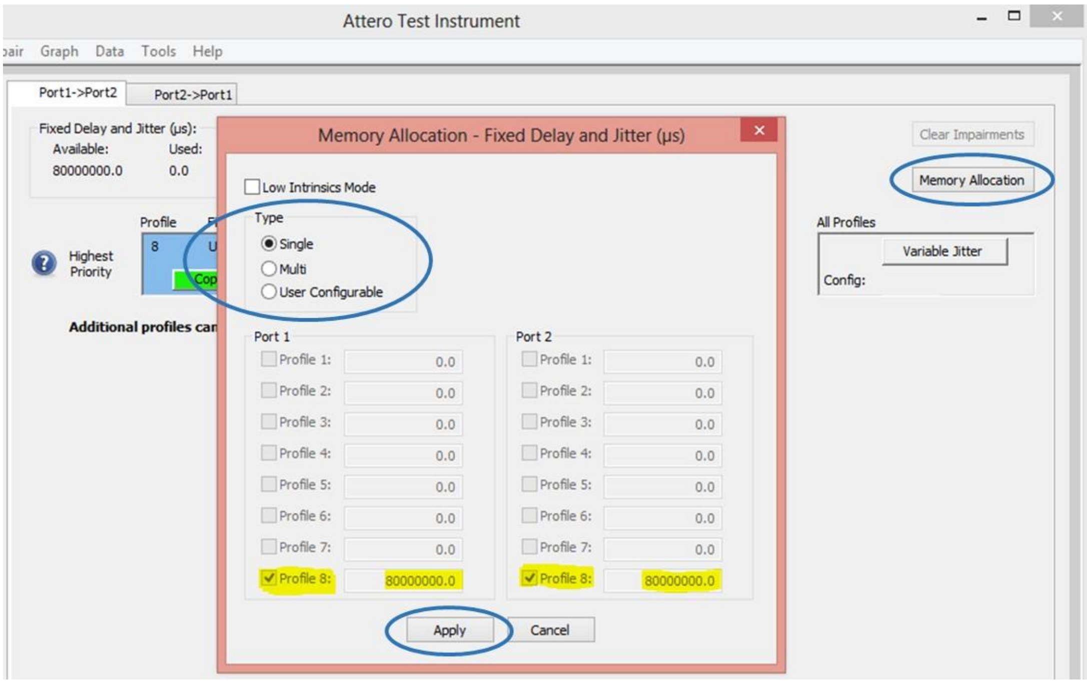
The maximum available memory is 80 seconds per Port (dependent on the Line Rate). Each Profile can be set to any value from zero to maximum, but the sum total of all Profiles cannot exceed the maximum available memory for the Port. Part of the memory allocation is used-up each time Fixed Delay and Jitter are added to an impairment profile.

Note: Max Available memory/delay is dependent on Line Rate (10GbE: 0.8s, 1GbE: 8s, 100MbE: 80s).

The default Memory Allocation Type is **Single,** where all the memory is allocated to a single profile (Profile 8) on both Ports as shown below.

To re-configure the profile memory allocation;

- Click on the **Memory Allocation** button as shown encircled below.



Fixed Delay and Jitter (µs):
Available: 80000000.0
Used: 0.0

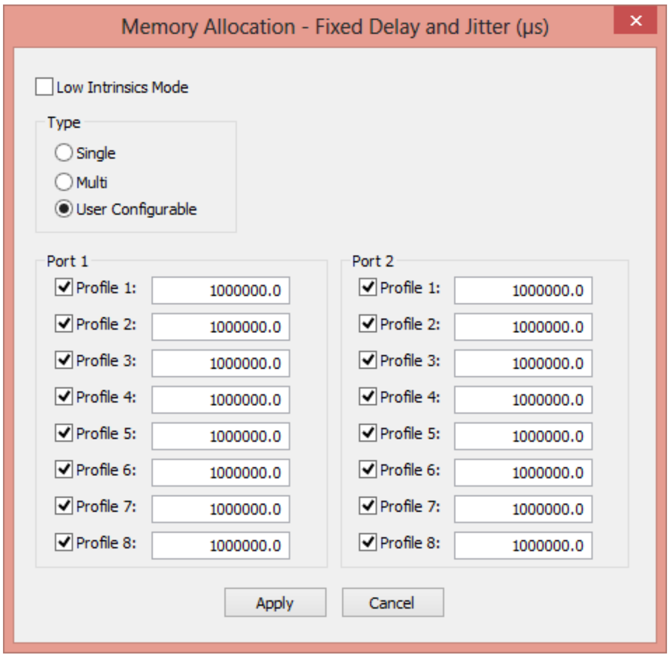
Memory Allocation - Fixed Delay and Jitter (µs)

☐ Low Intrinsics Mode

Type
● Single
○ Multi
○ User Configurable

	Port 1		Port 2
☐ Profile 1:	0.0	☐ Profile 1:	0.0
☐ Profile 2:	0.0	☐ Profile 2:	0.0
☐ Profile 3:	0.0	☐ Profile 3:	0.0
☐ Profile 4:	0.0	☐ Profile 4:	0.0
☐ Profile 5:	0.0	☐ Profile 5:	0.0
☐ Profile 6:	0.0	☐ Profile 6:	0.0
☐ Profile 7:	0.0	☐ Profile 7:	0.0
☑ Profile 8:	80000000.0	☑ Profile 8:	80000000.0

- Choose the required **Type** by selecting from the list of radio buttons as shown encircled above.



Memory Allocation - Fixed Delay and Jitter (µs)

☐ Low Intrinsics Mode

Type

○ Single

○ Multi

● User Configurable

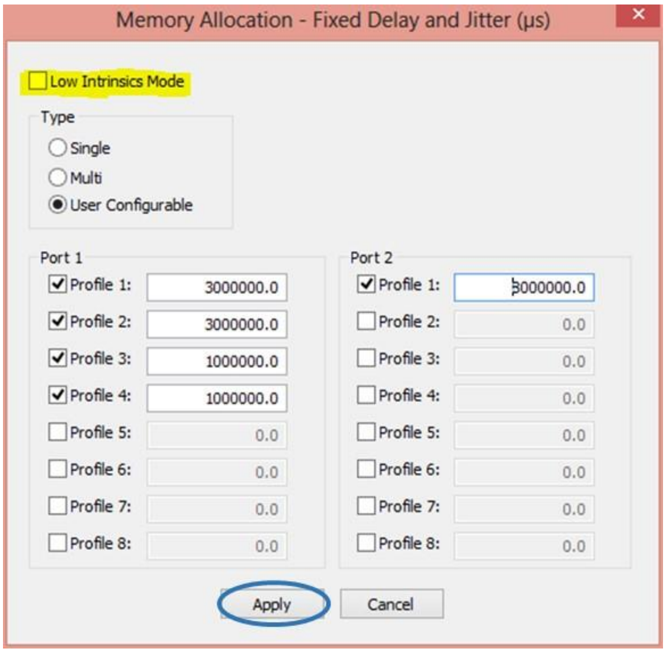
Port 1		Port 2	
☑ Profile 1:	1000000.0	☑ Profile 1:	1000000.0
☑ Profile 2:	1000000.0	☑ Profile 2:	1000000.0
☑ Profile 3:	1000000.0	☑ Profile 3:	1000000.0
☑ Profile 4:	1000000.0	☑ Profile 4:	1000000.0
☑ Profile 5:	1000000.0	☑ Profile 5:	1000000.0
☑ Profile 6:	1000000.0	☑ Profile 6:	1000000.0
☑ Profile 7:	1000000.0	☑ Profile 7:	1000000.0
☑ Profile 8:	1000000.0	☑ Profile 8:	1000000.0

The **Multi** setting shares the memory allocation equally over all profiles.

The **User Configurable** setting allows the user flexibility in allocating memory as desired.

Note: The **User Configurable** default settings are dependent on whether the previous setting was **Single** or **Multi.**

- One typical configuration is as shown below.



Memory Allocation - Fixed Delay and Jitter (µs)

☐ Low Intrinsics Mode

Type

○ Single

○ Multi

● User Configurable

Port 1		Port 2	
☑ Profile 1:	3000000.0	☑ Profile 1:	8000000.0
☑ Profile 2:	3000000.0	☐ Profile 2:	0.0
☑ Profile 3:	1000000.0	☐ Profile 3:	0.0
☑ Profile 4:	1000000.0	☐ Profile 4:	0.0
☐ Profile 5:	0.0	☐ Profile 5:	0.0
☐ Profile 6:	0.0	☐ Profile 6:	0.0
☐ Profile 7:	0.0	☐ Profile 7:	0.0
☐ Profile 8:	0.0	☐ Profile 8:	0.0

In this example for 1GbE interface the total 8 seconds of available memory is split over 4 profiles on Port 1.

On Port 2 the 8s of memory is allocated to one single profile.

- Set the appropriate memory allocation values for the profiles to be used.
- Click Apply when complete.

Low intrinsic Mode (as shown highlighted above) disables all memory providing a low intrinsic delay path through the instrument. Corruption impairments can be added in this mode, but not Fixed Delay or Jitter.

Extended Delay Mode

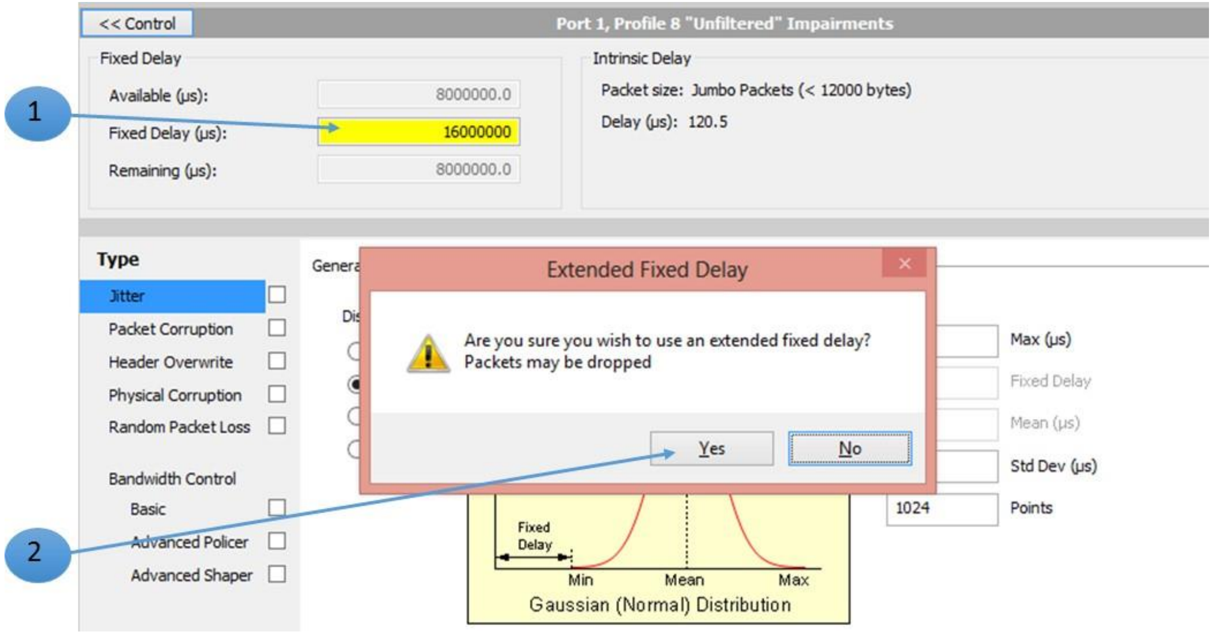
In normal operation, Paragon-X Network Emulation provides a fixed maximum limit of delay that can be flexibly applied across the configured profiles on each port. For example when set to 1Gb/s interface, there is a maximum limit of 8 seconds delay – that could be 8s on one profile, 1s on each of 8 profiles, or any other configuration of delay that adds up to 8s maximum. In this mode of operation, the fixed maximum limit ensures that all packets pass through the instrument right up to the full Line Rate (1Gb/s). No packets are unintentionally dropped.

In scenarios where the full Line rate of traffic is not required, Extended Delay Mode allows the user to add higher levels of delay. This is done at the expense of the maximum rate of traffic that can pass through without dropping packets. For example, in Extended Delay Mode it is possible to set 16 seconds of delay on the 1Gb/s interface (twice the normal limit). The maximum traffic rate possible with this delay setting is 500Mb/s (half the normal limit). At traffic rates higher than 500Mb/s some packets will be unintentionally dropped.

The formula for calculating the Max Delay and Traffic Rate using the 1Gb/s interface is;
Max Delay (seconds) x Traffic Rate (bandwidth in Gb/s) = 8 (constant)
Some examples;

Delay	Bandwidth
400s	20Mb/s
160s	50Mb/s
80s	100Mb/s
16s	500Mb/s
8s	1Gb/s
2s	4Gb/s

Adding Fixed Delay in Extended Delay Mode



Port 1, Profile 8 "Unfiltered" Impairments

Fixed Delay
Available (µs): 8000000.0
Fixed Delay (µs): 16000000
Remaining (µs): 8000000.0

Intrinsic Delay
Packet size: Jumbo Packets (< 12000 bytes)
Delay (µs): 120.5

Extended Fixed Delay

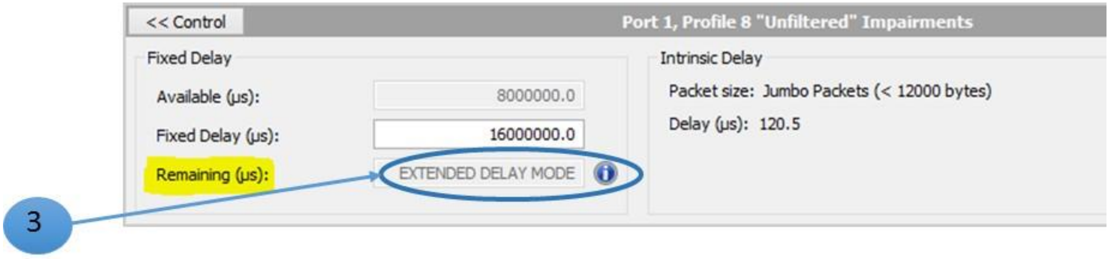
Are you sure you wish to use an extended fixed delay?
Packets may be dropped

1. Enter the value of Fixed Delay required as shown annotated above.

If the value of Fixed Delay entered is greater than the **Available** delay the user will be prompted to confirm a change to Extended Delay Mode. Note that adding Jitter also uses up the **Available** delay which can result in switching to Extended Delay Mode when jitter is selected.

2. To change to Extended Delay Mode click on **Yes**.

3. When in Extended Delay Mode the display of **Remaining** delay changes to an indicator that **Extended Delay Mode** is set as shown illustrated below.



Port 1, Profile 8 "Unfiltered" Impairments

Fixed Delay

Available (µs): 8000000.0

Fixed Delay (µs): 16000000.0

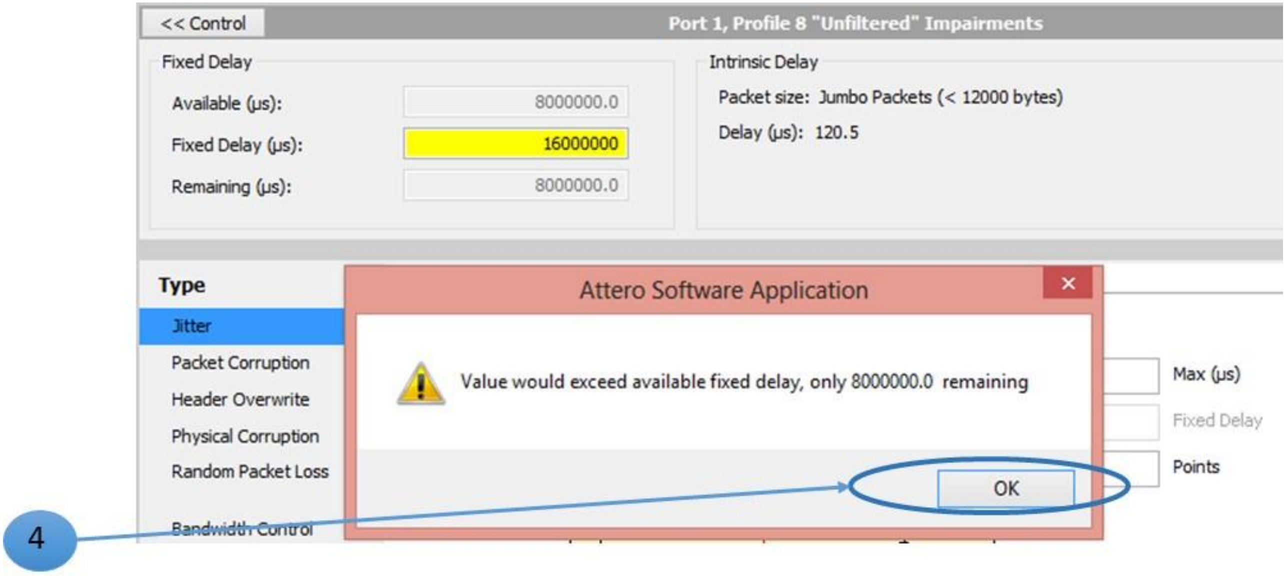
Remaining (µs): EXTENDED DELAY MODE

Intrinsic Delay

Packet size: Jumbo Packets (< 12000 bytes)

Delay (µs): 120.5

4. If the user chooses NOT to enter Extended Delay Mode in step 2 by clicking on **No** the following prompt is displayed and no change is made to the Fixed Delay setting;



Port 1, Profile 8 "Unfiltered" Impairments

Fixed Delay

Available (µs): 8000000.0

Fixed Delay (µs): 16000000

Remaining (µs): 8000000.0

Intrinsic Delay

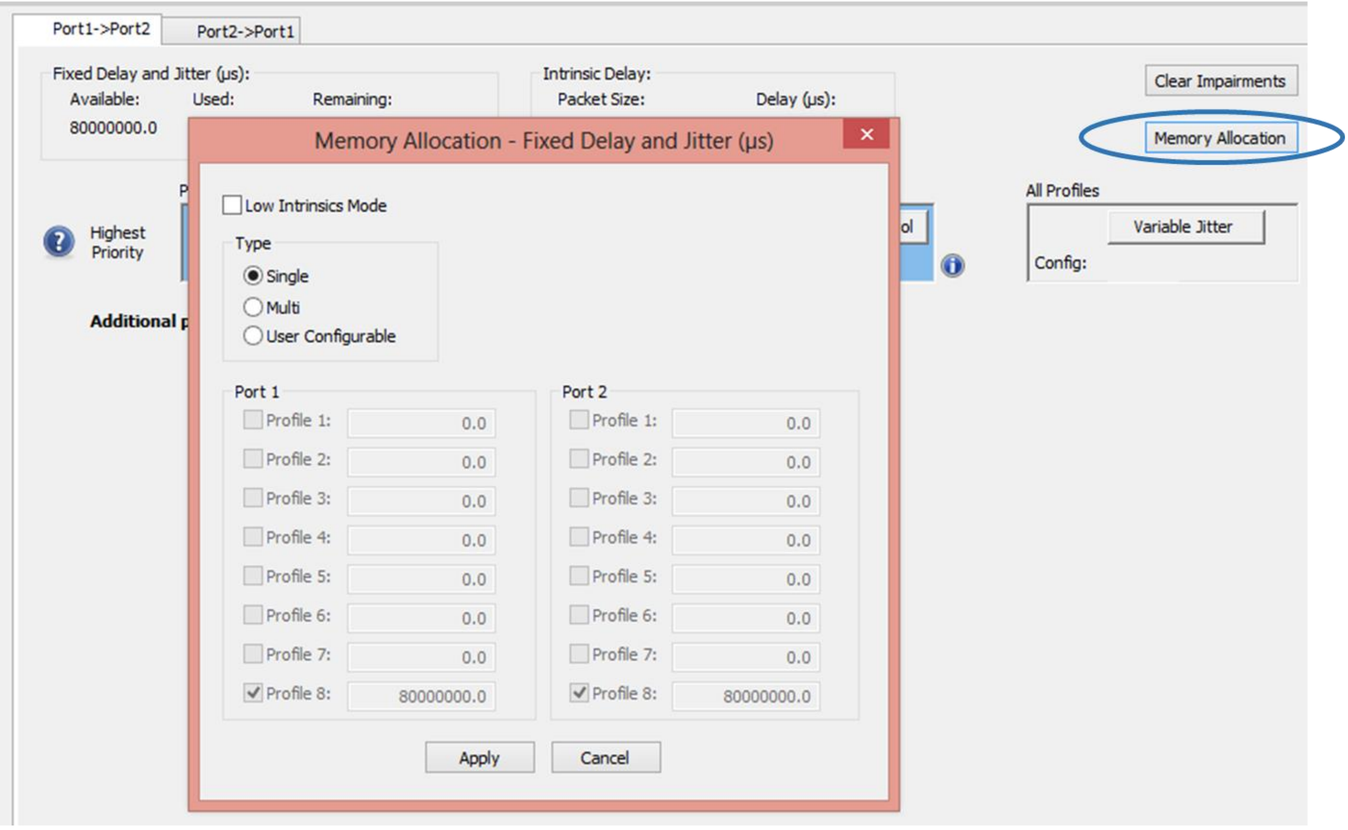
Packet size: Jumbo Packets (< 12000 bytes)

Delay (µs): 120.5

Attero Software Application

Value would exceed available fixed delay, only 8000000.0 remaining

Note that it is possible to re-allocate more memory to a particular profile to achieve more Fixed Delay on that profile without entering Extended Delay Mode. This is done by clicking on the Memory Allocation button shown encircled in the graphic on the next page.



Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
80000000.0		

Intrinsic Delay:

Packet Size:	Delay (µs):

Memory Allocation - Fixed Delay and Jitter (µs)

□ Low Intrinsics Mode

Type

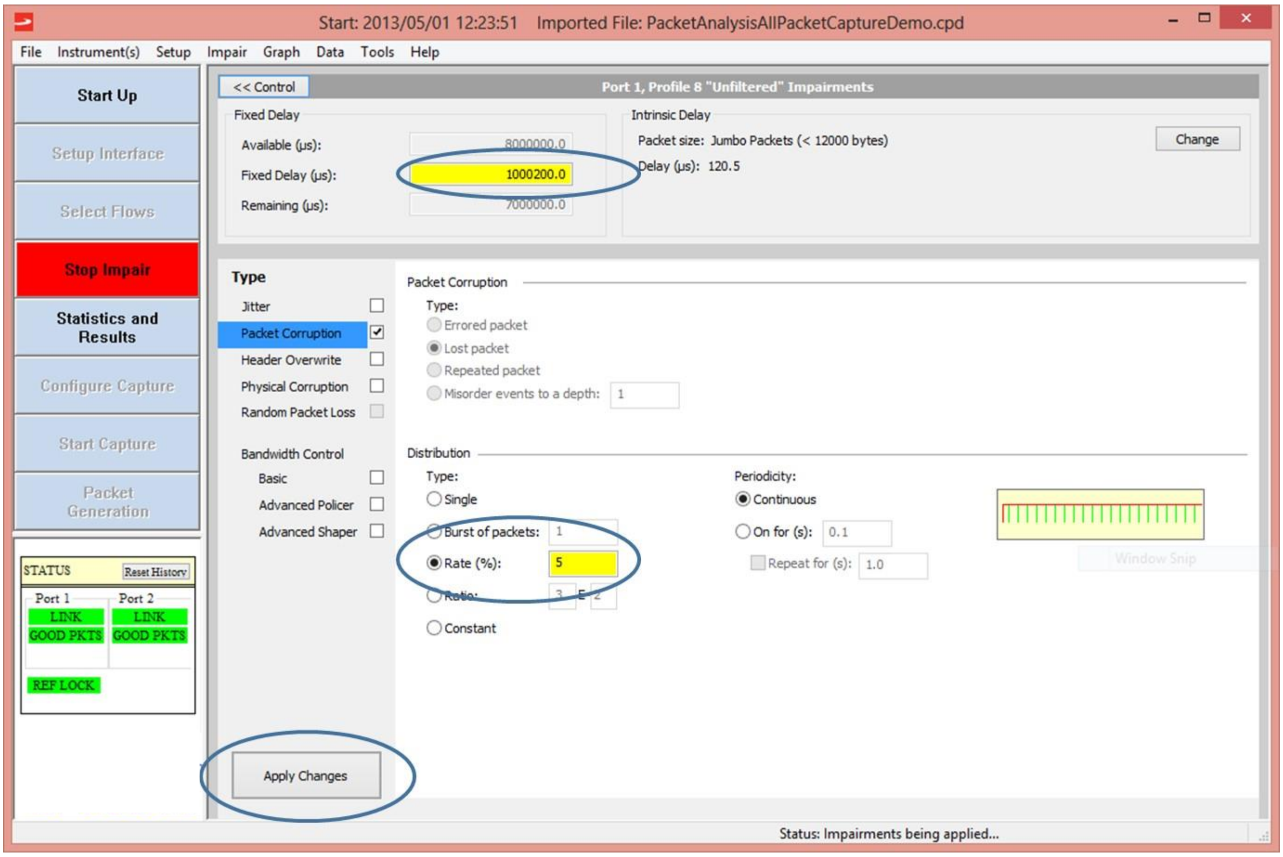
● Single
○ Multi
○ User Configurable

Port 1		Port 2	
□ Profile 1:	0.0	□ Profile 1:	0.0
□ Profile 2:	0.0	□ Profile 2:	0.0
□ Profile 3:	0.0	□ Profile 3:	0.0
□ Profile 4:	0.0	□ Profile 4:	0.0
□ Profile 5:	0.0	□ Profile 5:	0.0
□ Profile 6:	0.0	□ Profile 6:	0.0
□ Profile 7:	0.0	□ Profile 7:	0.0
☑ Profile 8:	80000000.0	☑ Profile 8:	80000000.0

Apply Changes button

Entering impairment configuration values can be completed by pressing the Enter key on your keyboard to make a single field change. To change multiple fields at the same time use the **Apply Changes** button.

When each field value is changed the field background colour changes to yellow as shown encircled below for the **Fixed Delay** and **Packet Corruption Rate** fields. The changes are not activated until the **Apply Changes** button is pressed. This provides a means to change or vary multiple impairments at the same instant while impairments are running.



Start: 2013/05/01 12:23:51   Imported File: PacketAnalysisAllPacketCaptureDemo.cpd

Port 1, Profile 8 "Unfiltered" Impairments

Fixed Delay

Available (µs): 8000000.0

Fixed Delay (µs): 1000200.0

Remaining (µs): 7000000.0

Intrinsic Delay

Packet size: Jumbo Packets (< 12000 bytes)

Delay (µs): 120.5

Type

- Jitter □
- Packet Corruption ☑
- Header Overwrite □
- Physical Corruption □
- Random Packet Loss □
- Bandwidth Control
  - Basic □
  - Advanced Policer □
  - Advanced Shaper □

Packet Corruption

Type:

- ○ Errored packet
- ● Lost packet
- ○ Repeated packet
- ○ Misorder events to a depth: 1

Distribution

Type:

- ○ Single
- ○ Burst of packets: 1
- ● Rate (%): 5
- ○ Ratio: 3 E 2
- ○ Constant

Periodicity:

- ● Continuous
- ○ On for (s): 0.1
  - □ Repeat for (s): 1.0

Status: Impairments being applied...

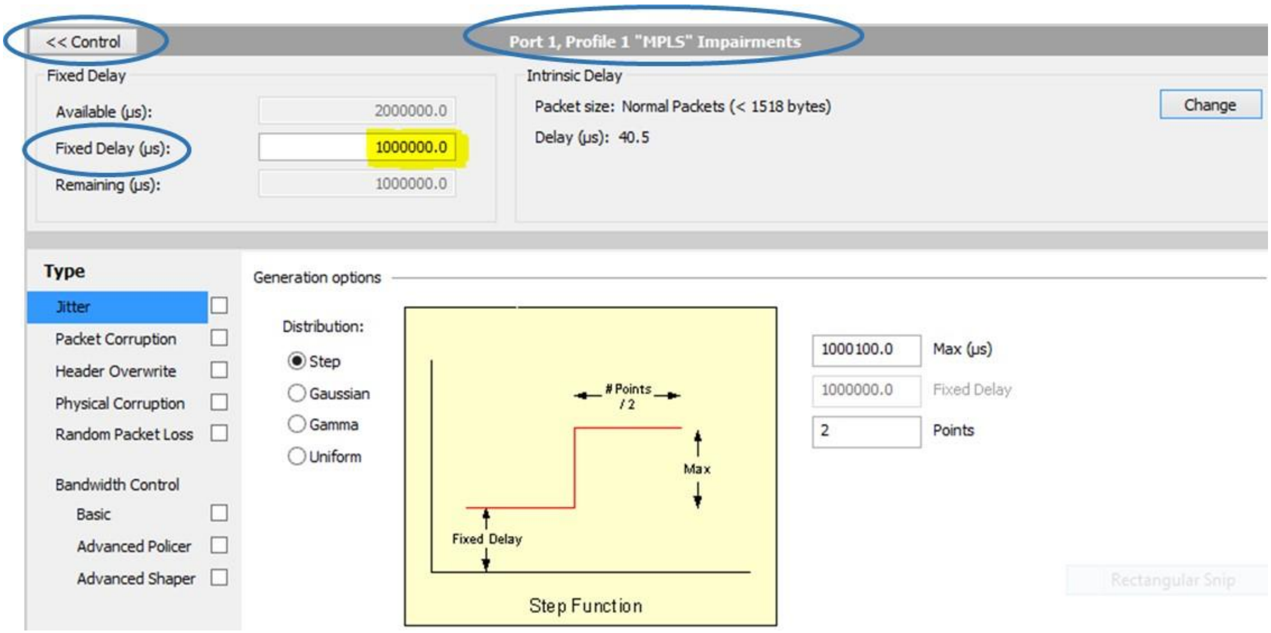
Adding Fixed Delay to an Impairment Profile

- In the Impairments Summary View (see Figure 5.1 for reference) click on the **Fixed Delay and Jitter** element in the Profile to be impaired. This gives access to the Impairment Setup View where various types of impairment are added as shown in Figure 5.2.

The legend, shown encircled, at the top right of Figure 5.2 identifies which Filter the impairments profile relates to. In this case “Port: 1 Filter Name: MPLS”.

- Enter the required Delay setting for this Profile in the **Fixed Delay** field shown highlighted in yellow below. The combined value entered cannot be greater than that displayed in the **Remaining** Field.

The **Available (µS)** field displays the amount of memory allocated to this Profile. More memory can be allocated using the Memory Allocation function – see page 32. Adding a Fixed Delay impairment will reduce the remaining memory resource and this will be reflected in the **Remaining (µS)** value displayed.



Port 1, Profile 1 "MPLS" Impairments

Fixed Delay

Available (µs): 2000000.0

Fixed Delay (µs): 1000000.0

Remaining (µs): 1000000.0

Intrinsic Delay

Packet size: Normal Packets (< 1518 bytes)

Delay (µs): 40.5

Type

- Jitter □
- Packet Corruption □
- Header Overwrite □
- Physical Corruption □
- Random Packet Loss □
- Bandwidth Control
  - Basic □
  - Advanced Policer □
  - Advanced Shaper □

Generation options

Distribution:

- ● Step
- ○ Gaussian
- ○ Gamma
- ○ Uniform

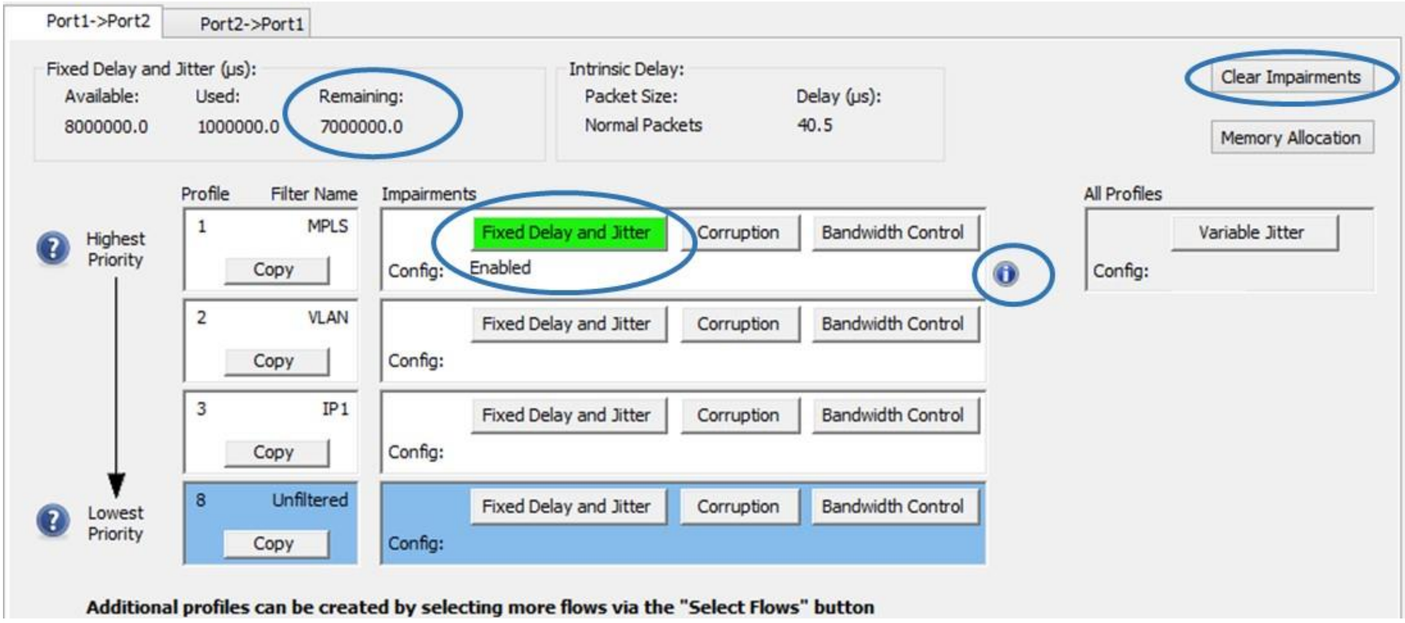
1000100.0 Max (µs)

1000000.0 Fixed Delay

2 Points

Figure 5.2: Impairment Setup View

- Click on **<<Control** to return to the Impairment Summary View.



Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
8000000.0	1000000.0	7000000.0

Intrinsic Delay:

Packet Size:	Delay (µs):
Normal Packets	40.5

Profile	Filter Name	Impairments Config:
1	MPLS	Enabled
2	VLAN	
3	IP1	
8	Unfiltered	

Additional profiles can be created by selecting more flows via the "Select Flows" button

The Impairment Summary View shown above indicates that **Fixed Delay and Jitter** are **Enabled** for Profile 1 (Enabled impairments elements are coloured green for easy identification). A summary of the Remaining Delay that can be configured for other Profiles is also provided.

- Repeat the above procedure to add Fixed Delay to other Profiles as required.

The Information Icon ⓘ positioned at the right-hand side of each Profile gives a quick summary of the impairments configured for each Profile. Hover the mouse over the information icon to see the summary.

To remove a Fixed Delay impairment click on the appropriate Profile and set the values to 0.
Note: The Clear Impairments button can be used to clear all Impairment Profiles simultaneously.

- When all required impairments have been added to the profiles click on ▶ **Impairments** to apply the Impairment Profiles to the traffic flowing through the instrument.

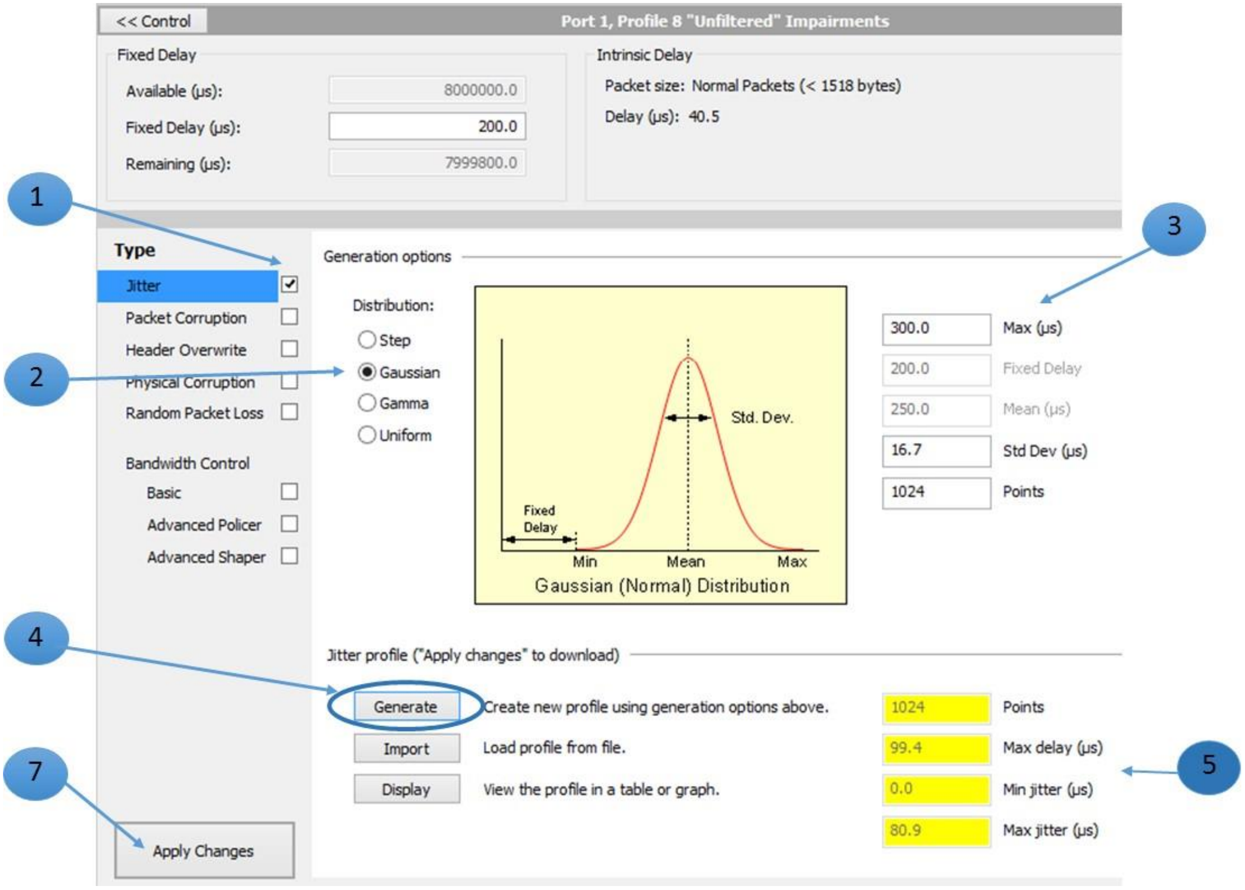
The button will change from ▶ **Impairments** to ■ **Impairments**. The Impairments workflow button will also turn red and say "Stop Impair". Enabled impairment elements will also change from Green to Red to indicate they are being applied to traffic.

Note: Fixed Delay value can be changed dynamically while impairments are still running.

- Click on ■ **Impairments** to stop impairing the traffic.

Adding Jitter to an Impairment Profile

- In the Impairments Summary View (see Figure 5.1 for reference) click on the **Fixed Delay and Jitter** element in the Profile to be impaired. This gives access to the Impairment Setup View where various types of impairment are added as shown below.
  Note that Jitter is mutually exclusive with Variable Jitter and Profile Corruption impairments.
- Jitter is added to an impairment profile by first selecting the distribution type and parameters, then generating a profile of Jitter points that is downloaded to the instrument hardware.
- Follow steps 1 to 7 below to generate and download a Jitter profile to the hardware.



<< Control — Port 1, Profile 8 "Unfiltered" Impairments

Fixed Delay
- Available (µs): 8000000.0
- Fixed Delay (µs): 200.0
- Remaining (µs): 7999800.0

Intrinsic Delay
- Packet size: Normal Packets (< 1518 bytes)
- Delay (µs): 40.5

Type
- Jitter ☑
- Packet Corruption □
- Header Overwrite □
- Physical Corruption □
- Random Packet Loss □
- Bandwidth Control
  - Basic □
  - Advanced Policer □
  - Advanced Shaper □

Generation options

Distribution:
- ○ Step
- ● Gaussian
- ○ Gamma
- ○ Uniform

300.0	Max (µs)
200.0	Fixed Delay
250.0	Mean (µs)
16.7	Std Dev (µs)
1024	Points

Jitter profile ("Apply changes" to download)
- Generate — Create new profile using generation options above.
- Import — Load profile from file.
- Display — View the profile in a table or graph.

1024	Points
99.4	Max delay (µs)
0.0	Min jitter (µs)
80.9	Max jitter (µs)

1. Click on the **Jitter** checkbox.
2. Choose the Jitter **Distribution** type for the profile to be generated by clicking on the appropriate radio button. Each type displays a graph that illustrates the shape of the distribution and also the relationship between the values; Fixed Delay, Mean, Max and Standard Deviation etc.
   Note that the Gaussian distribution is bounded by the Max and Min values (Truncated Gaussian distribution).
3. Enter the parameters to be used to create the Jitter distribution profile.
   Explanation of fields;

   Max (µs) – sets the Maximum Delay value of the Jitter Profile.
   The maximum value that can be set is the Fixed Delay value + 107ms. (Resolution 0.1µs)

Fixed Delay – this field displays the value of Fixed Delay that is set (if any). The jitter profile is superimposed on top of the Fixed Delay.
Mean (µs) – displays the Mean Delay value.
Std Dev (µs) – sets the spread of the jitter distribution.

Points – sets the number of points in the jitter distribution profile (range 2 – 1-024)
For the Jitter Generation option parameters shown on the previous page all packets would have a minimum delay of 200µs (Fixed Delay) and a jitter delay value somewhere between 0µs and 100µs (Max minus Fixed Delay). The Fixed Delay and Jitter values are added together to get the total delay so the actual delay range would be from 200µs to 300µs.

4. Click on the **Generate** button to create the profile of jitter values to be used. (If 1024 "points" was chosen in step 3 then 1024 values will be created in the profile).
*At this point the profile can be displayed in a table, TIE graph or PDF (Probability Density Function) graph by clicking on the **Display** button. When the table of points is displayed click on **Graph->Show Graph** in the Menu Bar to view the generated profile as a Delta Delay (TIE) graph, or click **Tools->Plot PDF/CDF/Histogram** to view a PDF.*
Note that the profile table & graphs do not include any Fixed Delay component. Only the Jitter component is displayed. See Chapter 9 for more general details on Displaying Graphs.
*The Generated profile can also be exported, edited and re-imported. To export ensure the table/graph of generated values is displayed then use **File->Export** from the Menu Bar and save as .csv file. To import click on **Import** and select the required .csv file*
See section on Editing a Jitter Distribution Profile *on page 90 for details on how to manually edit a Jitter Profile.*
To exit the table/graph view click on the **Impairments** button located in the workflow area.
5. Key information about the profile values generated (such as Max Delay, Min Jitter, Max Jitter) is displayed.
6. Steps 3 and 4 can be repeated adjusting the parameters to achieve the desired profile.
7. Click on the Apply button to save the generated jitter profile.

- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments. The Impairments workflow button will also turn red and say "Stop Impair".

Note: Jitter Distribution types and values can be changed dynamically while impairments are still running using the **Generate** and **Apply Changes** buttons.

- Click on ■ Impairments to stop impairing the traffic.

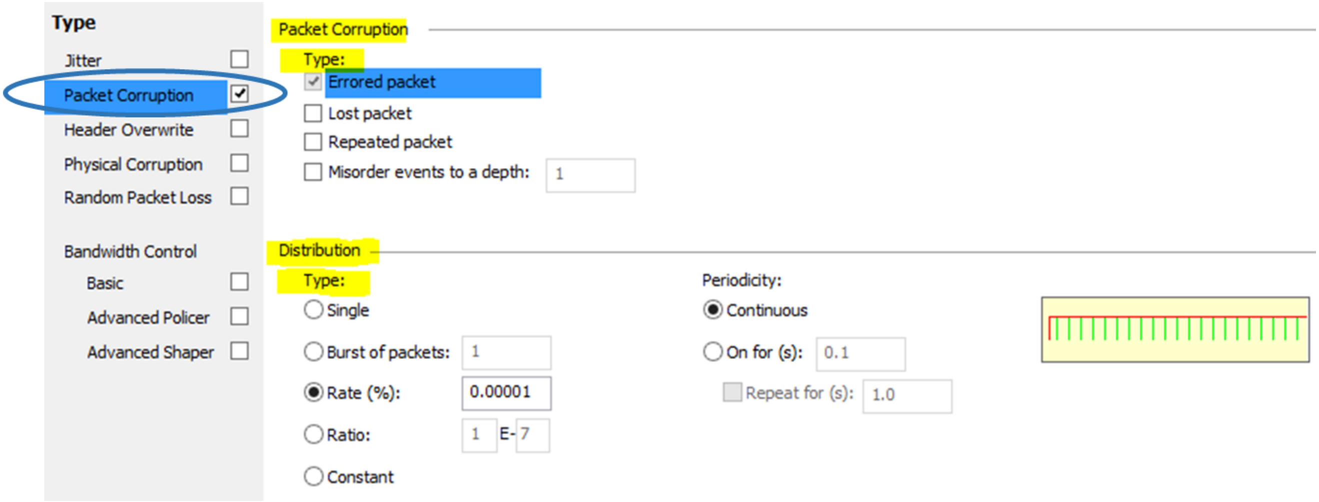
Adding Corruptions to an Impairment Profile

Note that Packet Corruption and Physical Corruption impairments cannot be combined in a single profile.

- In the Impairments Summary View (see Figure 5.1 for reference) click on the **Corruption** element within the Profile to be impaired. This gives access to the Impairment Setup View where various types of impairment can be added as shown below. The following sub-sections describe how to add each type of Corruption.

Adding Packet Corruptions

- Click on the **Packet Corruption** checkbox as shown encircled below.
- Choose the **Type(s)** of Packet Corruption required from the list provided as shown highlighted in yellow below. Click on the appropriate checkbox to select it. At least one Type must be selected. By default **Errored Packet** is selected.
  Note that multiple Packet Corruption types can be applied at the same time.



Type

Jitter ☐

Packet Corruption ☑

Header Overwrite ☐

Physical Corruption ☐

Random Packet Loss ☐

Bandwidth Control

Basic ☐

Advanced Policer ☐

Advanced Shaper ☐

Packet Corruption

Type:

☑ Errored packet

☐ Lost packet

☐ Repeated packet

☐ Misorder events to a depth: 1

Distribution

Type:

○ Single

○ Burst of packets: 1

● Rate (%): 0.00001

○ Ratio: 1 E- 7

○ Constant

Periodicity:

● Continuous

○ On for (s): 0.1

☐ Repeat for (s): 1.0

Packet Corruption Type descriptions;

Packet Corruption Type	Description
Errored Packet	An Ethernet Frame Check Sum value is Errored on a packet selected at random.
Lost Packet	An Ethernet Packet is dropped. The Packet to be dropped is selected at random.
Repeated Packet	An Ethernet Packet is repeated. The Packet to be repeated is selected at random. Repeat Range: 1 to 10,000 in steps of 1 packet.
Mis-order Events to a depth.	Packets are transmitted out-of-sequence. The depth value represents the relative deviation of the packet from its proper position in the sequence. For example a depth of 3 would move the affected packet from sequence position 4 to sequence position 7. Depth Range: 1 to 32 in steps of 1 packet.

- Choose the desired **Distribution** for each Packet Corruption type by clicking on the Packet Corruption text (highlighted in blue) then choosing the distribution from the selections provided. Repeat for each Packet Corruption type required.
  See the table below for a description of the settings. Click on the appropriate radio button to select.
  Note that a different Distribution can be selected for each Packet Corruption Type.

Distribution Type	**Description**	**Periodicity**
Single	One single event of the corruption is applied to the packets.	Continuous
Burst of packets	One single burst of packets. Range 1 to 10,000 packets in steps of 1 packet.	Continuous
Rate (%)	The rate at which the corruption occurs within the packets. Range 0.00001% to 99.99999% in steps of 0.00001%	Continuous or on/off repeat
Ratio	The ratio at which the corruption occurs within the packets. Range 1E-7 to 9E-1. Mantissa 1 to 9 in steps of 1. Exponent -7 to -1 in steps of 1.	Continuous or on/off repeat
Constant	The Corruption event is always active.	Continuous or on/off repeat

- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments. The Impairments workflow button will also turn red and say “Stop Impair”.

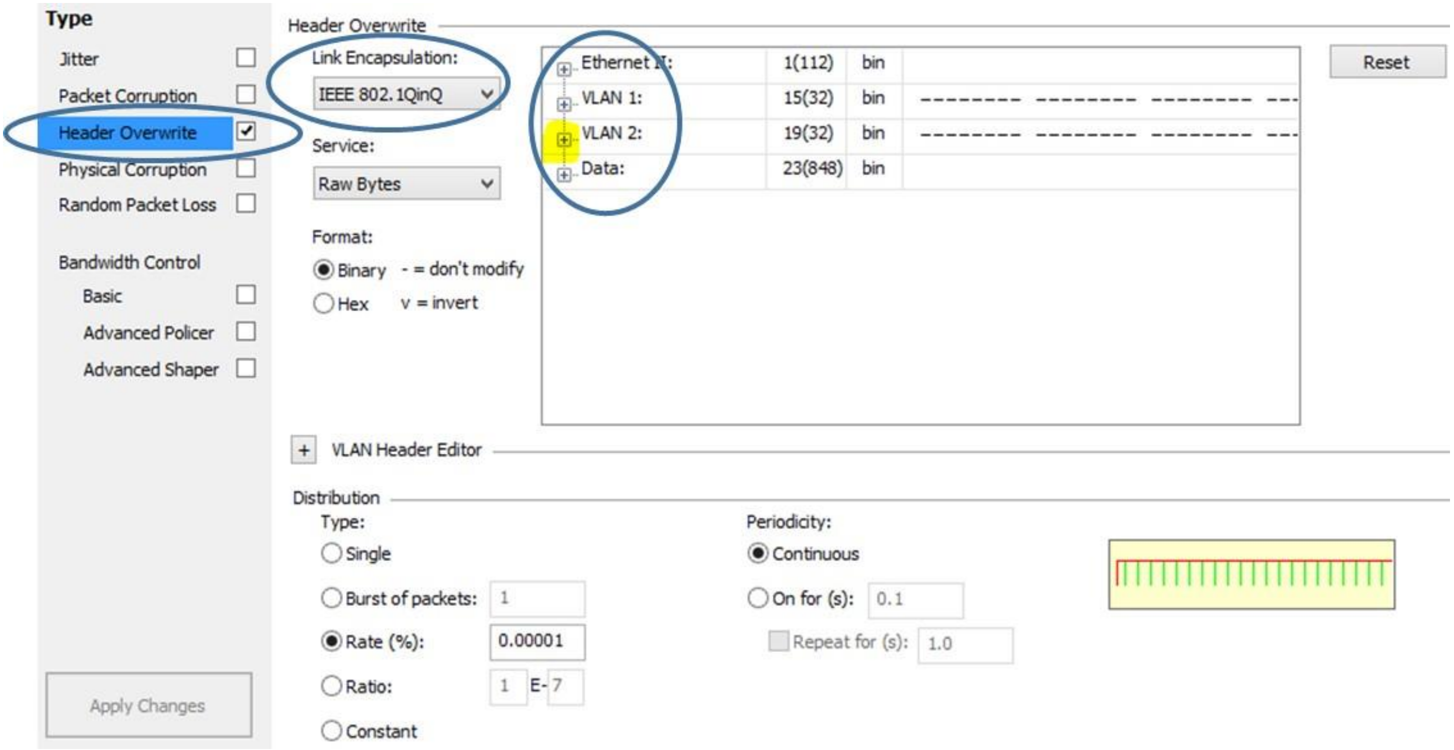
Note: Corruption Distribution types and values can be changed dynamically while impairments are still running.

- Click on ■ Impairments to stop impairing the traffic.

Header Overwrite

Paragon-X Network Emulation can overwrite any or all bytes within the first 128 bytes of each packet. This usually covers the header(s) and part of the data portion of a packet.

- Click on the **Header Overwrite** checkbox as shown encircled below.



Link Encapsulation: IEEE 802.1QinQ

Service: Raw Bytes

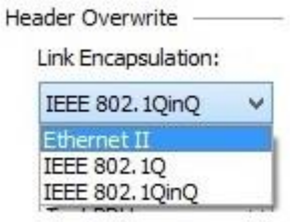
Format: ● Binary ○ Hex   - = don't modify   v = invert

⊞ Ethernet II:	1(112)	bin
⊞ VLAN 1:	15(32)	bin
⊞ VLAN 2:	19(32)	bin
⊞ Data:	23(848)	bin

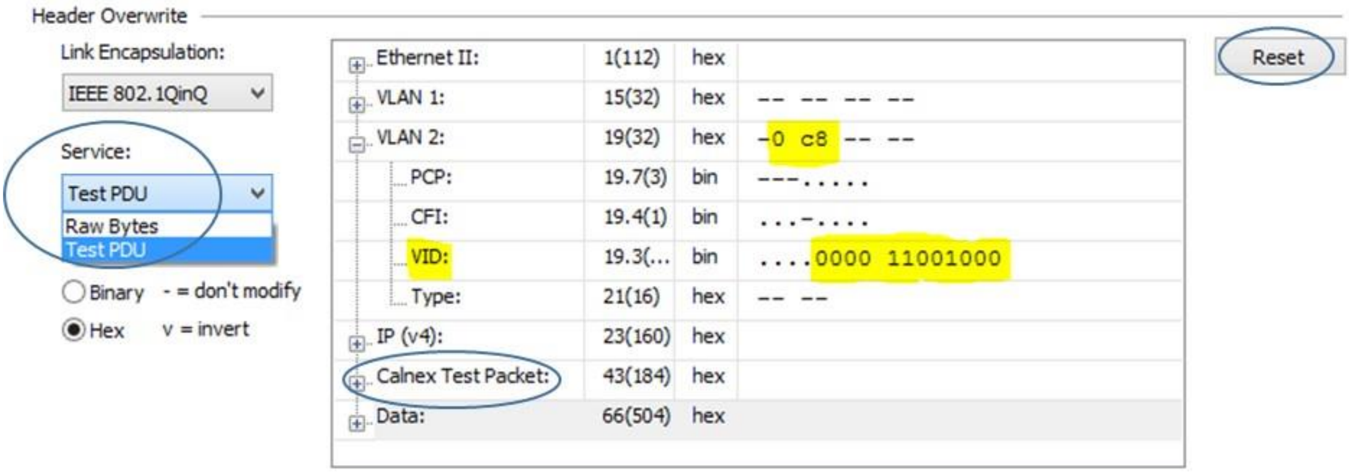
Type: ○ Single ○ Burst of packets: 1 ● Rate (%): 0.00001 ○ Ratio: 1 E- 7 ○ Constant

Periodicity: ● Continuous ○ On for (s): 0.1 □ Repeat for (s): 1.0

- Click on the **Link Encapsulation** Drop-Down Button (encircled above) and select the appropriate Link Encapsulation protocol from the Drop-Down List as shown below. The selected protocol should be set to match the particular profile that is being configured. (IEEE 802.1Q is the Network Standard that specifies the support of VLANs. IEEE 802.1QinQ is the Network Standard that specifies the support of stacked VLANs)



- Click on ⊞ as shown encircled and highlighted in yellow on the right hand side of the above graphic to expand the packet byte structure as shown on the next page.



Header Overwrite

Link Encapsulation: IEEE 802.1QinQ

Service: Test PDU

Raw Bytes
Test PDU

○ Binary - = don't modify

● Hex v = invert

Reset

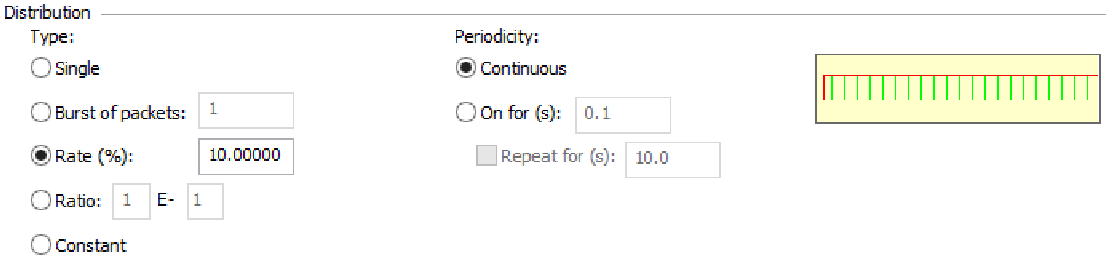
Ethernet II:	1(112)	hex	
VLAN 1:	15(32)	hex	-- -- -- --
VLAN 2:	19(32)	hex	-0 c8 -- --
PCP:	19.7(3)	bin	---.....
CFI:	19.4(1)	bin	...-....
VID:	19.3(...	bin	....0000 11001000
Type:	21(16)	hex	-- --
IP (v4):	23(160)	hex	
Calnex Test Packet:	43(184)	hex	
Data:	66(504)	hex	

- Click on the **Service** Drop-Down Button and select **Raw Bytes** or **Test PDU** as shown above. Selecting **Test PDU** will insert a Calnex Test Packet Data Unit into the Data field of the selected packet(s) as shown encircled above. The overall packet size will remain unchanged.

The packet byte values can be modified by editing the fields on the right-hand side of the packet byte structure shown above. To edit a value click on the bit or byte twice, then enter the value in the appropriate format (Hex or Binary). The graphic above shows **VLAN 2 ID** being overwritten with the value **C8 (Hex)**. This could also have been entered as **binary 0000 1100 1000**. Either of these methods will overwrite the VLAN ID with value 200 (Decimal). See the section entitled "Using the VLAN Header Editor" on the next page for help calculating and entering the packet byte values.

Bytes can also be inverted by entering **v** for the byte value or bytes can be left unmodified from the original packet values by entering **–** (dash). Any changes can quickly be undone by clicking on the **Reset** button as shown encircled above.

- Choose the desired **Distribution Type** and **Periodicity** for the Header Overwrite from the selections provided as shown below. Click on the appropriate radio buttons to select.



Distribution

Type:

○ Single

○ Burst of packets: 1

● Rate (%): 10.00000

○ Ratio: 1 E- 1

○ Constant

Periodicity:

● Continuous

○ On for (s): 0.1

□ Repeat for (s): 10.0

Note: The distribution types available are the same as for Packet Corruption described in the section entitled "Adding Packet Corruptions", page 42.

- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments. The Impairments workflow button will also turn red and say "Stop Impair".

Note: Header Overwrite Distribution types and values can be changed dynamically while impairments are still running.

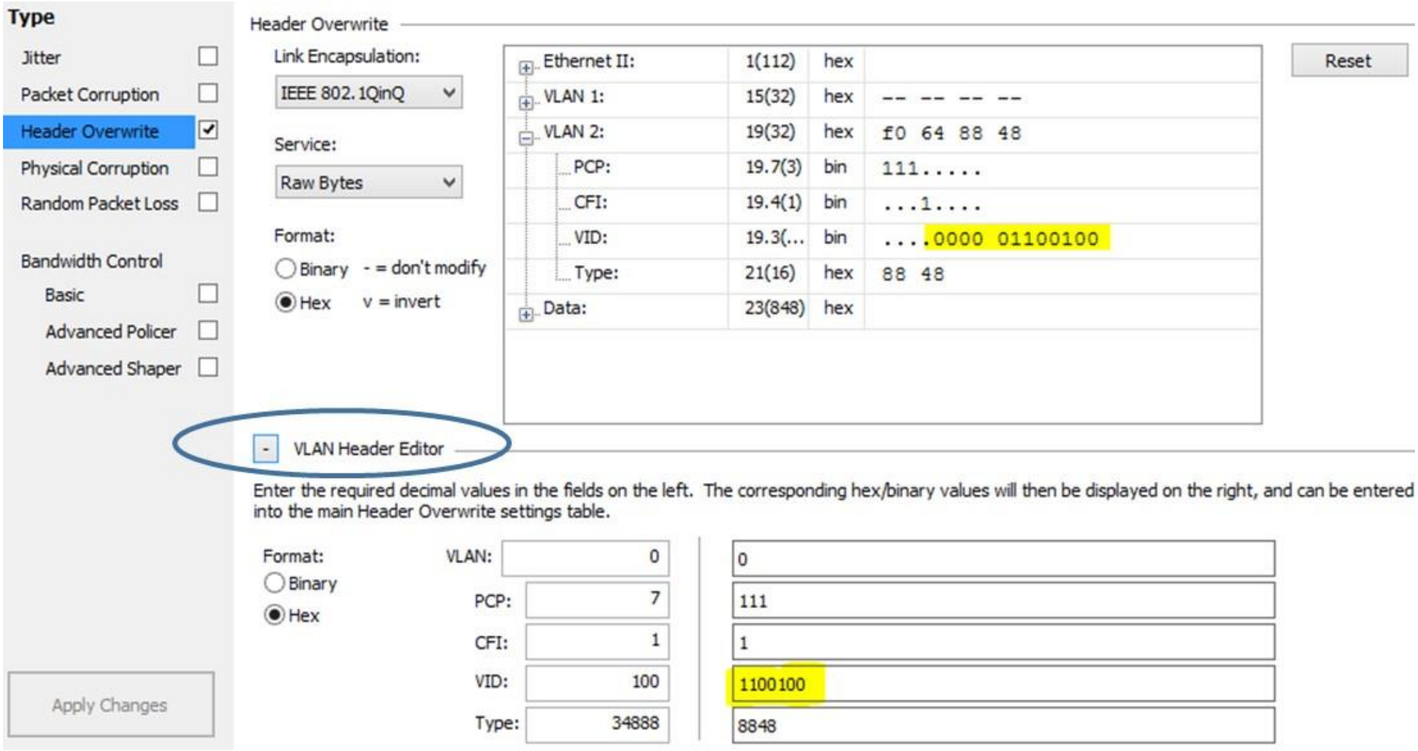
- Click on ■ Impairments to stop impairing the traffic.

Using the VLAN Header Editor

A tool is included to help translate byte values from Decimal to Hex and Binary. To access this tool click on the **VLAN Header Editor** button shown encircled below.

In the example below a VLAN ID value of 100 (Decimal) has been entered in the Editor field. The translated binary value (1100100) is shown highlighted both in the Editor tool and also where it should be entered manually in the VLAN ID field.

Hex or Binary format can be selected. Note that this only applies to the VLAN and Type fields. All other fields are always displayed in Binary format.



Link Encapsulation: IEEE 802.1QinQ

Service: Raw Bytes

Format: ○ Binary ● Hex   - = don't modify   v = invert

⊞ Ethernet II:	1(112)	hex	
⊞ VLAN 1:	15(32)	hex	-- -- -- --
⊟ VLAN 2:	19(32)	hex	f0 64 88 48
PCP:	19.7(3)	bin	111.....
CFI:	19.4(1)	bin	...1....
VID:	19.3(...	bin	....0000 01100100
Type:	21(16)	hex	88 48
⊞ Data:	23(848)	hex	

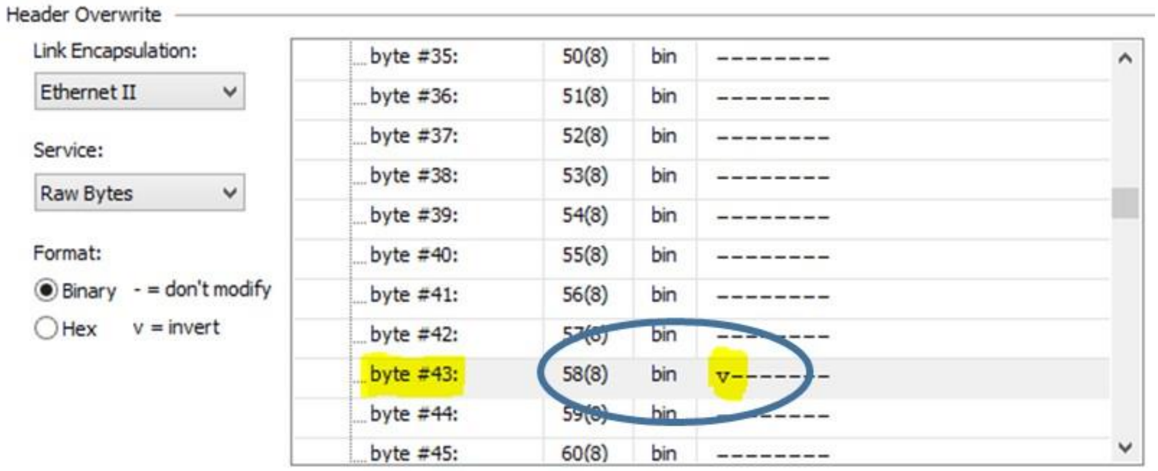
Enter the required decimal values in the fields on the left. The corresponding hex/binary values will then be displayed on the right, and can be entered into the main Header Overwrite settings table.

Format: ○ Binary ● Hex

VLAN:	0	0
PCP:	7	111
CFI:	1	1
VID:	100	1100100
Type:	34888	8848

Adding Bit Errors to Packets

Paragon-X Network Emulation can simulate adding Bit Errors by inverting a bit in the Data portion of the Frame as shown below. A range of Bit Errored Packets can be set using the normal Distribution selections (e.g. Single, Ratio etc.).



Header Overwrite

Link Encapsulation: Ethernet II

Service: Raw Bytes

Format:
● Binary - = don't modify
○ Hex v = invert

byte #35:	50(8)	bin	--------
byte #36:	51(8)	bin	--------
byte #37:	52(8)	bin	--------
byte #38:	53(8)	bin	--------
byte #39:	54(8)	bin	--------
byte #40:	55(8)	bin	--------
byte #41:	56(8)	bin	--------
byte #42:	57(8)	bin	--------
byte #43:	58(8)	bin	v-------
byte #44:	59(8)	bin	--------
byte #45:	60(8)	bin	--------

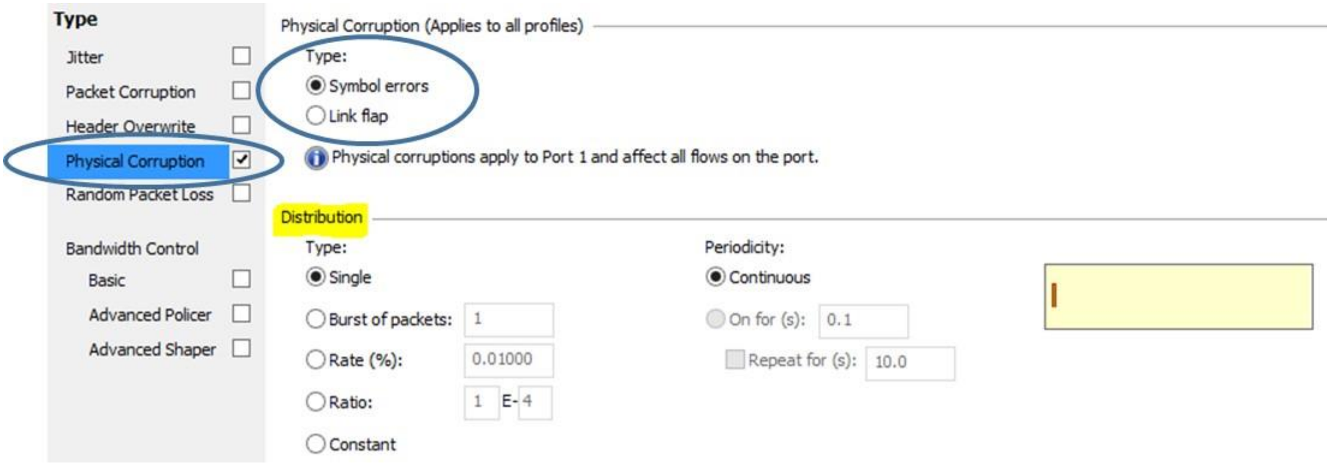
Physical Corruptions

Two types of Physical Corruptions can be added;

- **Symbol Errors**
  This feature inserts Symbol Errors by violating the Line Coding of the signal on the physical interface. Symbol Errors are not generated during Start Frame De-limiter (SFD), Idle Symbols or Auto-negotiation Symbols.
- **Link Flap**
  This feature allows the instrument ports to be cycled off/on to simulate Link Flapping. Both ports can be set to operate simultaneously for Failover Testing. In this mode the time difference between ports switching off is < 1ms

Note: Physical Corruptions are applied to all Profiles on the selected port simultaneously. They cannot be applied to individual Profiles. Also Physical Corruption impairments cannot be combined with Packet Corruption or Header Overwrite impairments.

- Click on the **Physical Corruption** checkbox and select the Type of corruption to be applied (Symbol or Link Flap) as shown encircled below.



Type
Jitter □
Packet Corruption □
Header Overwrite □
Physical Corruption ☑
Random Packet Loss □

Bandwidth Control
Basic □
Advanced Policer □
Advanced Shaper □

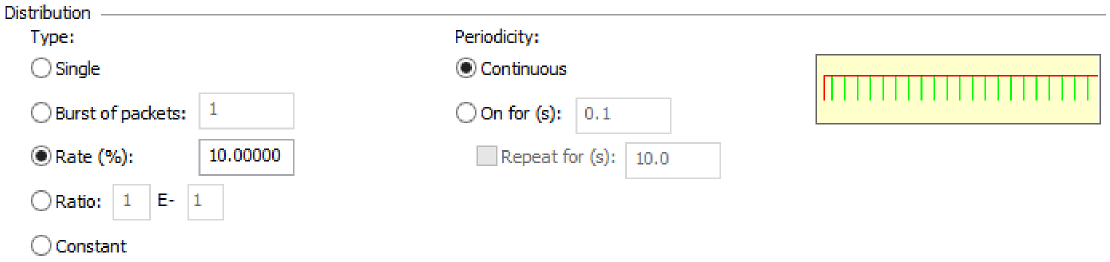
Physical Corruption (Applies to all profiles)
Type:
● Symbol errors
○ Link flap

Physical corruptions apply to Port 1 and affect all flows on the port.

Distribution
Type:
● Single
○ Burst of packets: 1
○ Rate (%): 0.01000
○ Ratio: 1 E- 4
○ Constant

Periodicity:
● Continuous
○ On for (s): 0.1
□ Repeat for (s): 10.0

- Choose the desired **Distribution Type** and **Periodicity** for the Physical Corruption from the selections provided as shown below. Click on the appropriate radio buttons to select.



Distribution

Type:

○ Single

○ Burst of packets: 1

● Rate (%): 10.00000

○ Ratio: 1 E- 1

○ Constant

Periodicity:

● Continuous

○ On for (s): 0.1

□ Repeat for (s): 10.0

Note: The distribution types available are the same as for Packet Corruption described in the section entitled Adding Packet Corruptions, page 42.

- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments. The Impairments workflow button will also turn red and say “Stop Impair”.

Note: Physical Corruption Distribution types and values can be changed dynamically while impairments are still running.

- Click on ■ Impairments to stop impairing the traffic.

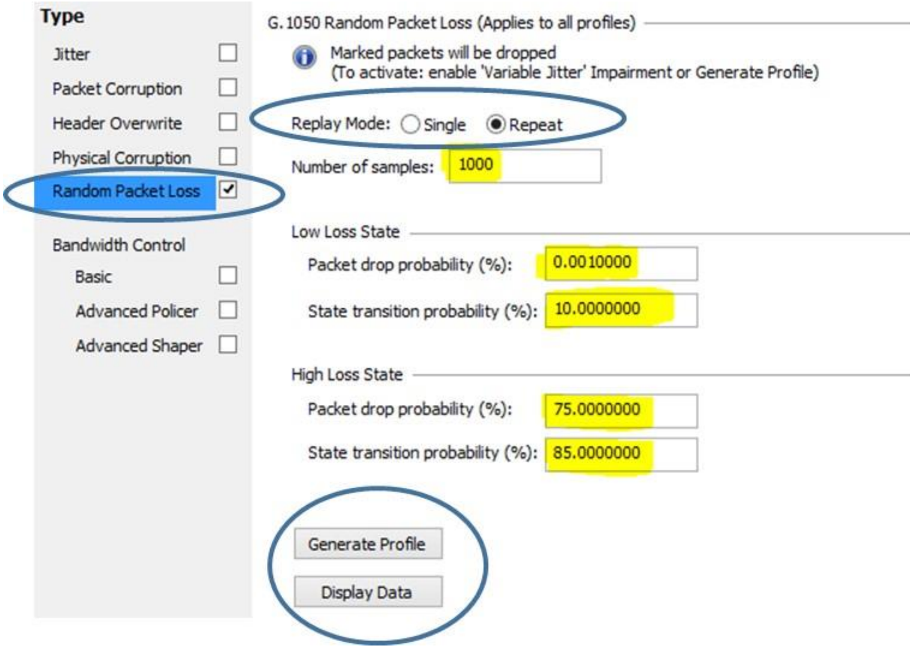
Random Packet Loss (G.1050)

This feature allows packets to be dropped with a randomised pattern according to the Markov chains theory. This is described in G.1050 Appendix II as the Gilbert-Elliott model. The model describes 2 states, a low error rate state and a high error rate state. Within each state there is a probability that the next packet will be dropped. There is also a probability that the state will change to the other state. The distribution of errors and state changes is randomised. The Random Packet Loss feature “replays” a randomly generated profile that “marks” which packets passing through the instrument will be dropped.

Notes:

1. Generating a Random Packet Loss profile will overwrite any existing Variable Jitter Profile that has been set up. The user is alerted before the profile is overwritten.
2. It is not possible to add Variable Jitter impairments while generating a Random Packet Loss impairment.
3. Random Packet Loss is added to all profiles simultaneously.
4. Packets are dropped using the **Delay per packet** setting in Variable Jitter. The **Delay per Time Window** setting is disabled with the Random Packet Loss function.

- Click on the **Random Packet Loss** checkbox as shown encircled on the next page.
- Select the desired **Replay Mode; Single** Mode provides a “one-shot” replay of the dropped packet profile while **Repeat** replays the dropped packet profile continuously.



G.1050 Random Packet Loss (Applies to all profiles)

Marked packets will be dropped
(To activate: enable 'Variable Jitter' Impairment or Generate Profile)

Replay Mode: ○ Single ● Repeat

Number of samples: 1000

Low Loss State

Packet drop probability (%): 0.0010000

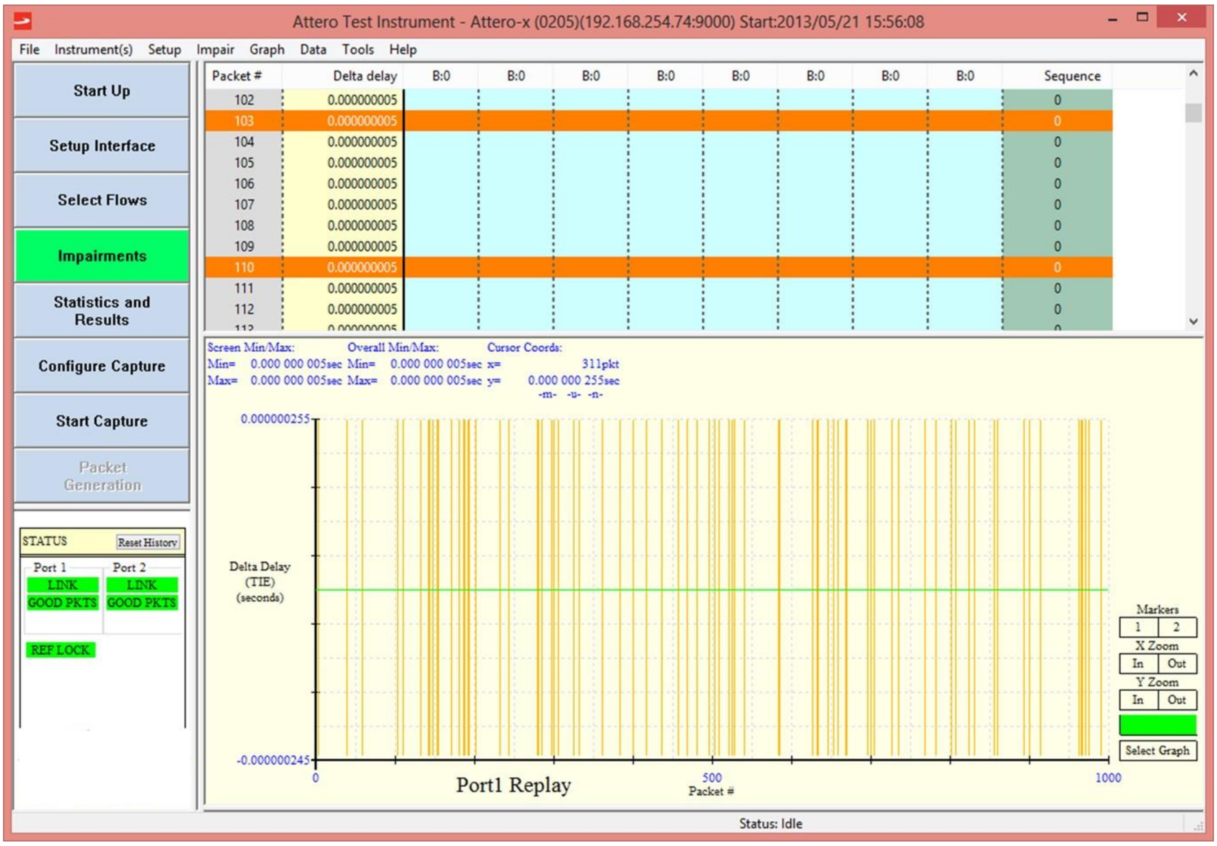
State transition probability (%): 10.0000000

High Loss State

Packet drop probability (%): 75.0000000

State transition probability (%): 85.0000000

- Once the probability parameters have been entered (example probability settings are shown highlighted in yellow above) the dropped packet profile is generated by clicking on the **Generate Profile** button.
- Click on the Display Data button (shown encircled above) to view the generated profile. The dropped packets are displayed as orange markers as shown below.
  To enable the graph click on **Graph -> Show Graph** in the Menu Bar.



Attero Test Instrument - Attero-x (0205)(192.168.254.74:9000) Start:2013/05/21 15:56:08

Packet #	Delta delay	B:0	B:0	B:0	B:0	B:0	B:0	B:0	B:0	Sequence
102	0.000000005									0
103	0.000000005									0
104	0.000000005									0
105	0.000000005									0
106	0.000000005									0
107	0.000000005									0
108	0.000000005									0
109	0.000000005									0
110	0.000000005									0
111	0.000000005									0
112	0.000000005									0

```
Screen Min/Max:          Overall Min/Max:          Cursor Coords:
Min=  0.000 000 005sec   Min=  0.000 000 005sec    x=          311pkt
Max=  0.000 000 005sec   Max=  0.000 000 005sec    y=  0.000 000 255sec
                                                        -m-  -u-  -n-
```

Status: Idle

Note: The action of clicking on the **Generate Profile** button will automatically enable Variable Jitter and the Variable jitter checkbox will be ticked. The user should not change any Variable Jitter settings at this time.

- Click on the **Impairments** button in the workflow area.
- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments. The Impairments workflow button will also turn red and say “Stop Impair”.

Note: Random Packet Loss settings cannot be edited while they are running. Click on ■ Impairments to stop, then edit the settings as required.

Bandwidth Control Overview

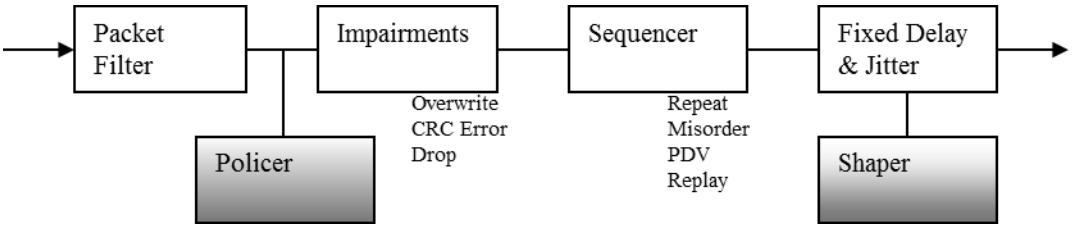
Bandwidth Control provides Policing and Shaping functions to emulate the effects of congestion in a switch or low speed link access to a network. The characteristics of Policing and Shaping is described below.

	Policing	Shaping
Objective	Drop excess packets	Buffer and queue excess packets
Applicable	Inbound traffic	Outbound traffic
Bursts	Propagates Burst. Does not alter incoming burst rate.	Controls burst by smoothing the output data (alters incoming bursts)
Delay	No additional delay introduced.	Smoothing effect is achieved by delaying traffic.

Traffic Policing drops packets that exceed the committed bit rate or the committed burst tolerance. It therefore has a limiting effect on the traffic bandwidth, but it does not alter the incoming burst characteristic of the traffic.

Traffic Shaping queues packets that exceed the committed bit rate or the committed burst tolerance. These “excess” packets are queued in a FIFO buffer, then re-scheduled for later transmission to “smooth out” the burst rate of the traffic.

Policing & Shaping Model



“Advanced Policer”

The Policer is positioned immediately after the Filtering of the inbound data (before any corruptions are added to the traffic). Policing is based on the model described in the MEF Bandwidth Profiles for Ethernet Services White Paper. This model classifies packets as Green (conformant with the Committed Rate), Yellow (not conformant with the Committed Rate, but conformant with the Excess Rate), or Red (not conformant with either Committed or Excess Rates).

The Policing model is implemented using a two token bucket algorithm (Green = Committed, Yellow = Excess). The buckets are “topped up” at the arrival of each packet.

E.g. Green bucket top up quantity = Time (time since last packet) * CIR (Committed Rate)

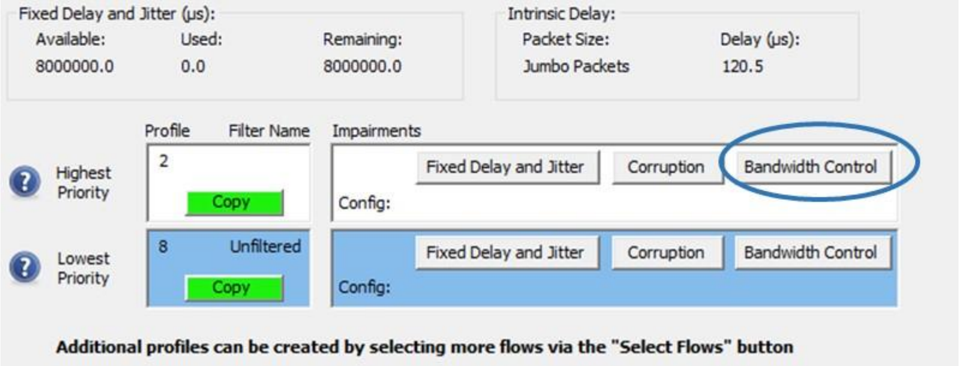
The Committed Burst Tolerance is normally set to TCP default window size (64000 bytes) or 3 times the max size of packets expected in the traffic stream.

“Advanced Shaper”

The Shaper is positioned immediately before the traffic egresses the instrument. This is after any corruptions are added to the traffic. In the Shaper algorithm the token buckets are “topped up” at fixed intervals (CBS/CIR) rather than at the instant new packets arrive. When all tokens have been used up any further packets are queued in the instrument Shaping buffer. The Shaper and Fixed Delay functions share the same FIFO buffer. If the buffer fills completely, no more incoming packets can be accommodated and they will be dropped. If the incoming traffic rate reduces the buffer starts to empty and incoming packets are no longer dropped.

Adding Bandwidth Control to a Profile

- Click on the Bandwidth Control element for the profile to be impaired; example shown encircled below.



Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
8000000.0	0.0	8000000.0

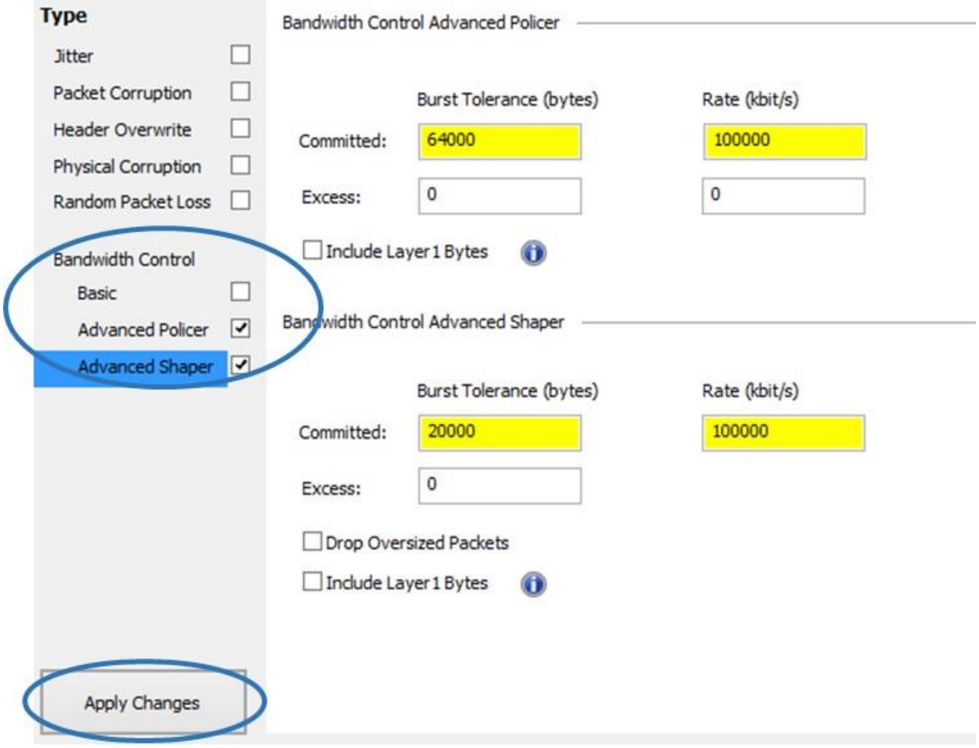
Intrinsic Delay:

Packet Size:	Delay (µs):
Jumbo Packets	120.5

	Profile	Filter Name	Impairments
Highest Priority	2		Fixed Delay and Jitter / Corruption / Bandwidth Control Config:
Lowest Priority	8	Unfiltered	Fixed Delay and Jitter / Corruption / Bandwidth Control Config:

Additional profiles can be created by selecting more flows via the "Select Flows" button

- Select Advanced Policer and/or Advanced Shaper as displayed below.



Type

- Jitter □
- Packet Corruption □
- Header Overwrite □
- Physical Corruption □
- Random Packet Loss □

Bandwidth Control

- Basic □
- Advanced Policer ☑
- Advanced Shaper ☑

Bandwidth Control Advanced Policer

	Burst Tolerance (bytes)	Rate (kbit/s)
Committed:	64000	100000
Excess:	0	0

□ Include Layer 1 Bytes

Bandwidth Control Advanced Shaper

	Burst Tolerance (bytes)	Rate (kbit/s)
Committed:	20000	100000
Excess:	0	

□ Drop Oversized Packets

□ Include Layer 1 Bytes

- Enter the desired values in the “Committed” fields as shown highlighted above. Then click on Apply Changes. The fields are explained on the following page.

Advanced Policer Settings

Setting	Description	Range
Committed Rate	Sets the Profile Bandwidth. Packets conforming to the Committed Rate are counted as “Green Packets” in Statistics & Results.	Zero to maximum set Line Rate.
Committed Burst Tolerance	Specifies the maximum packet size that will be allowed to pass through the Policer. Larger packets will be dropped.	64 bytes to 16M bytes in 1 byte steps.
Excess Rate	Sets the Profile Excess Bandwidth. Packets that exceed the Committed Rate, but fall within the Excess Rate are allowed to pass through the Policer. These packets are counted as “yellow packets” in Statistics & Results. Packets that exceed both the committed and the excess rates are dropped. These are counted as “red packets”.	Zero to maximum set Line Rate.
Excess Burst Tolerance	Specifies the maximum packet size that will be allowed to pass through the Policer as “excess” or “yellow packets”. Larger packets will be counted as “red packets” and dropped.	64 bytes to 16M bytes in 1 byte steps.
Include Layer 1 Bytes	When enabled all fields above are assumed to include L1 Bytes. That is they include each packet's preamble (8B) and minimum IPG (12B)	N/A

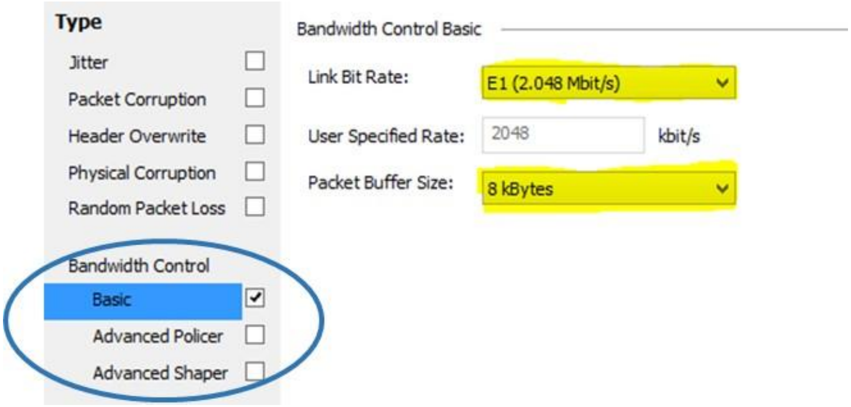
Advanced Shaper Settings

Setting	Description	Range
Committed Rate	Sets the average rate of the Traffic egressing the instrument.	Zero to maximum set Line Rate.
Committed Burst Tolerance	Specifies the maximum allowed packet burst size of traffic egressing the instrument.	64 bytes to 16M bytes in 1 byte steps.
Excess Burst Tolerance	Specifies the maximum number of bytes that can be “saved” during periods of low volume traffic, then re-used when traffic volume exceeds the Committed Burst Tolerance.	64 bytes to 16M bytes in 1 byte steps.
Include Layer 1 Bytes	When enabled all fields above are assumed to include L1 Bytes. That is they include each packet's preamble (8B) and minimum IPG (12B)	N/A
Drop Oversized Packets	When enabled, packets bigger than the Committed Burst Tolerance are dropped.	N/A

Basic Mode

In Basic mode the same Policer and Shaper algorithms are used as in the Advanced mode, but some of the settings are automatically set making bandwidth control quicker and easier to set-up. If you want to see the full details of what you have set up in Basic Mode, simply switch to Advanced Mode after completing your set-up and the all the advanced settings details are displayed. These can then be fine-tuned if required.

- Select Basic Bandwidth Control as shown on the next page (note that selecting Basic mode will deactivate the Advanced Policer and Advanced Shaper).



Type

- Jitter □
- Packet Corruption □
- Header Overwrite □
- Physical Corruption □
- Random Packet Loss □

Bandwidth Control

- Basic ☑
- Advanced Policer □
- Advanced Shaper □

Bandwidth Control Basic

Link Bit Rate: E1 (2.048 Mbit/s)

User Specified Rate: 2048 kbit/s

Packet Buffer Size: 8 kBytes

- Select the Link Bit Rate from the drop-list (this is equivalent to the Committed Rate in the Advanced Policer).
- Select the Packet Buffer Size from the drop-list (this is equivalent to the Committed Burst Tolerance in the Shaper).
- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ **Impairments** to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ **Impairments** to ■ **Impairments**. The Impairments workflow button will also turn red and say "Stop Impair".

Note: Bandwidth Control values can be changed dynamically while impairments are still running.

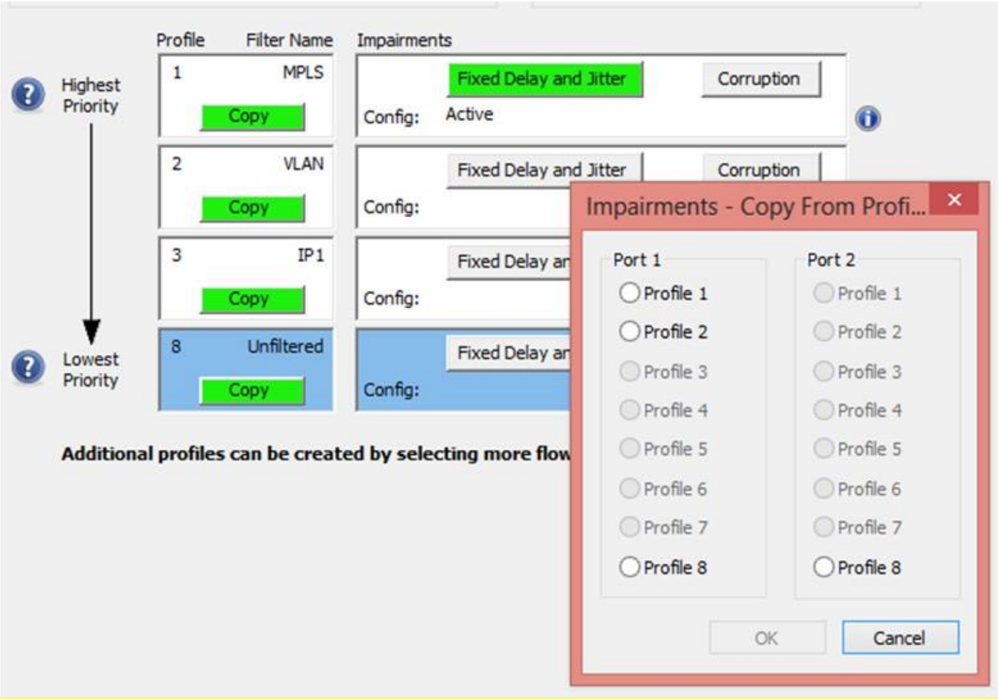
- Click on ■ **Impairments** to stop impairing the traffic.

The effects of Bandwidth Control on network traffic flowing through the instrument can be monitored using the information provided on the Statistics & Results page of the Network Emulation Application. This is detailed in Chapter 6 – Statistics and Results.

Copying Impairments from another Profile

For convenience it is possible to copy impairments from another profile. Once copied the impairment profile can be edited to make further changes.

- To copy impairments from another Profile click on the **Copy** button of the Profile the impairment is to be copied to. Then choose which **Profile** to copy from in the dialog box as shown below.



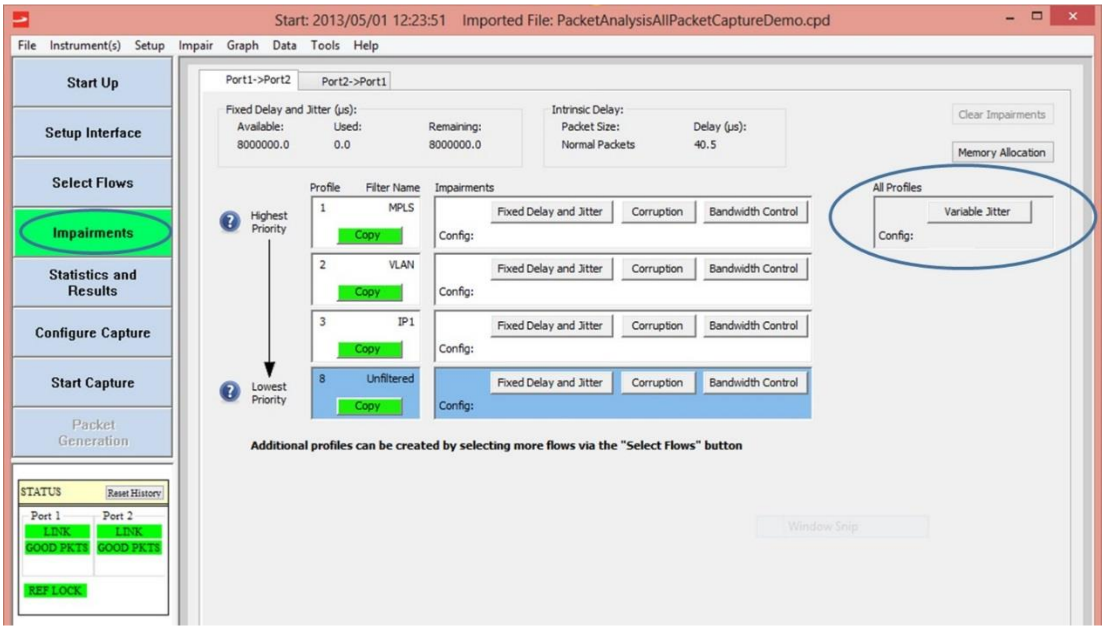
Config: Active

Additional profiles can be created by selecting more flow

Adding Variable Jitter Impairment

Variable Jitter is added across all Impairment Profiles simultaneously. It cannot be added to an individual Profile and it is mutually exclusive with **Jitter**.

- To access the Variable Jitter settings click on the Variable Jitter element as shown encircled below. Note that the Variable Jitter element will change colour to green once Variable Jitter is enabled as part of the following steps.



Start: 2013/05/01 12:23:51 Imported File: PacketAnalysisAllPacketCaptureDemo.cpd

Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
8000000.0	0.0	8000000.0

Intrinsic Delay:

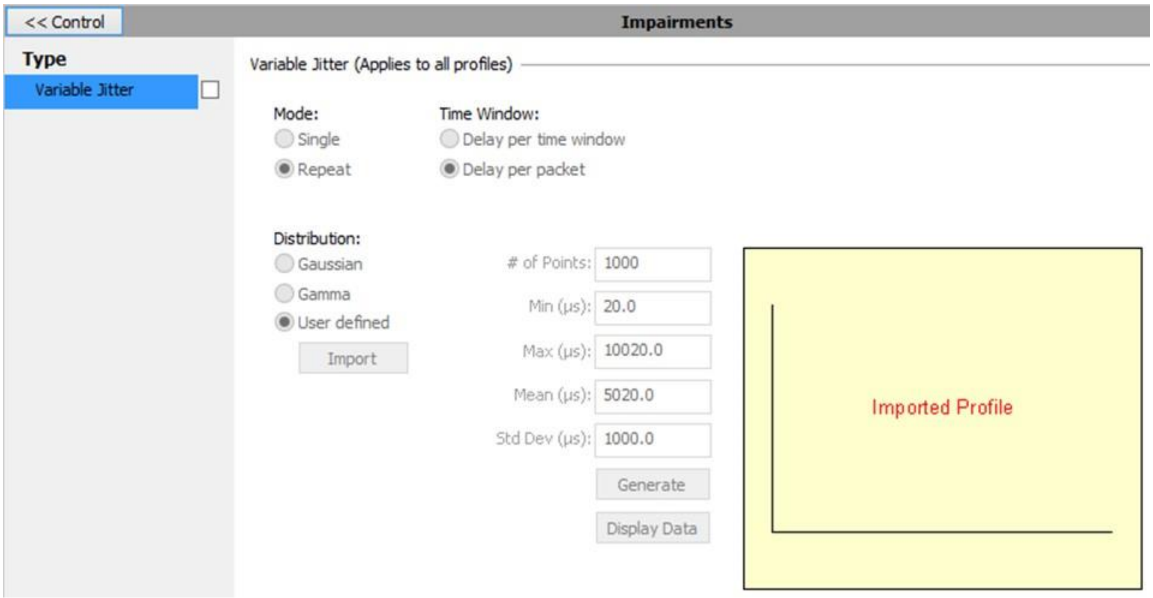
Packet Size:	Delay (µs):
Normal Packets	40.5

Profile	Filter Name	Impairments
1	MPLS	Fixed Delay and Jitter, Corruption, Bandwidth Control
2	VLAN	Fixed Delay and Jitter, Corruption, Bandwidth Control
3	IP1	Fixed Delay and Jitter, Corruption, Bandwidth Control
8	Unfiltered	Fixed Delay and Jitter, Corruption, Bandwidth Control

All Profiles: Variable Jitter

Additional profiles can be created by selecting more flows via the "Select Flows" button

The Variable Jitter Impairment View is now displayed as shown below allowing the Variable Jitter settings to be configured.



Variable Jitter (Applies to all profiles)

Mode: ○ Single ● Repeat

Time Window: ○ Delay per time window ● Delay per packet

Distribution: ○ Gaussian ○ Gamma ● User defined

# of Points: 1000

Min (µs): 20.0

Max (µs): 10020.0

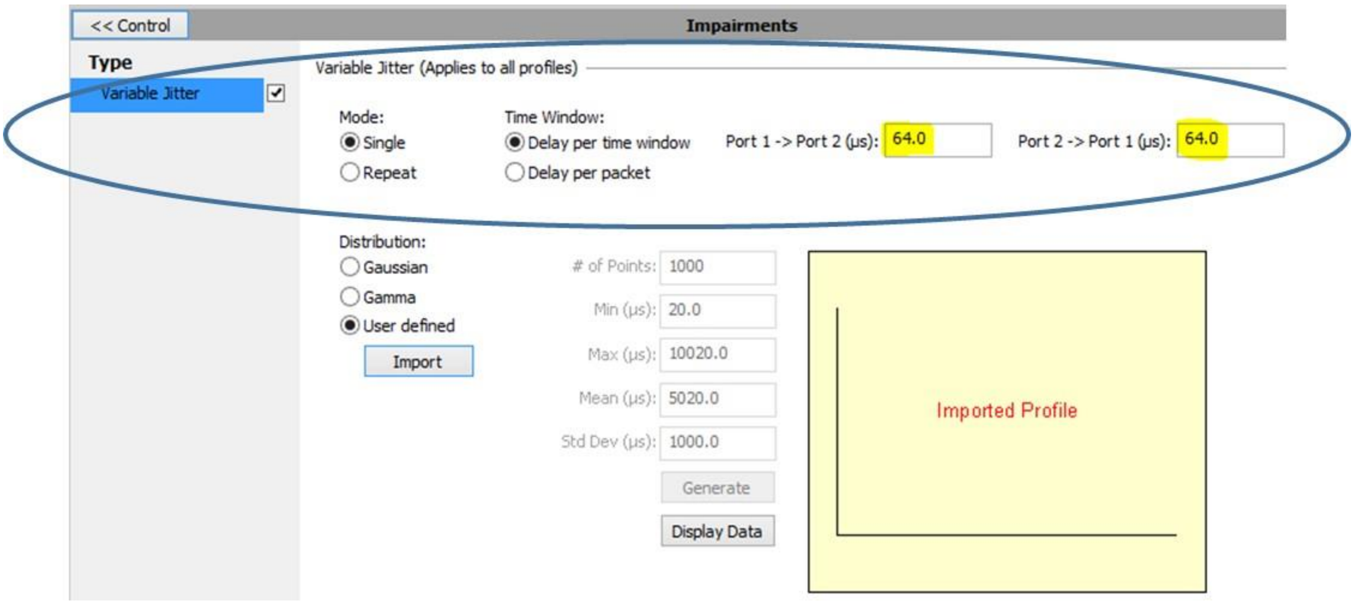
Mean (µs): 5020.0

Std Dev (µs): 1000.0

Variable Jitter is created using many discrete packet delay values, normally randomly generated to lie within a pre-defined distribution curve (for example a Gaussian distribution). Traffic entering the ports of the instrument have unique delay or PDV characteristics. The delay or Packet Delay Variation (PDV) added by the instrument is superimposed onto the traffic passing through. The original traffic delay (PDV) is not removed prior to this operation.

Overall Packet delay = original packet delay + Fixed Delay + Variable Jitter + instrument Intrinsic Delay.

- Click on the **Variable Jitter** checkbox as shown encircled below.
- Click on the **Mode** required:
  - **Single** - provides a **"**single-shot" of a pre-defined Jitter Profile.
  - **Repeat –** provides continuous repeat of the jitter profile.
- Select the **Time Window** required. This selects how the Variable Jitter profile is superimposed onto the packets when there are multiple flows passing through the instrument.



Variable Jitter ☑

Variable Jitter (Applies to all profiles)

Mode: ● Single ○ Repeat

Time Window: ● Delay per time window ○ Delay per packet

Port 1 -> Port 2 (µs): 64.0

Port 2 -> Port 1 (µs): 64.0

Distribution: ○ Gaussian ○ Gamma ● User defined

Import

# of Points: 1000

Min (µs): 20.0

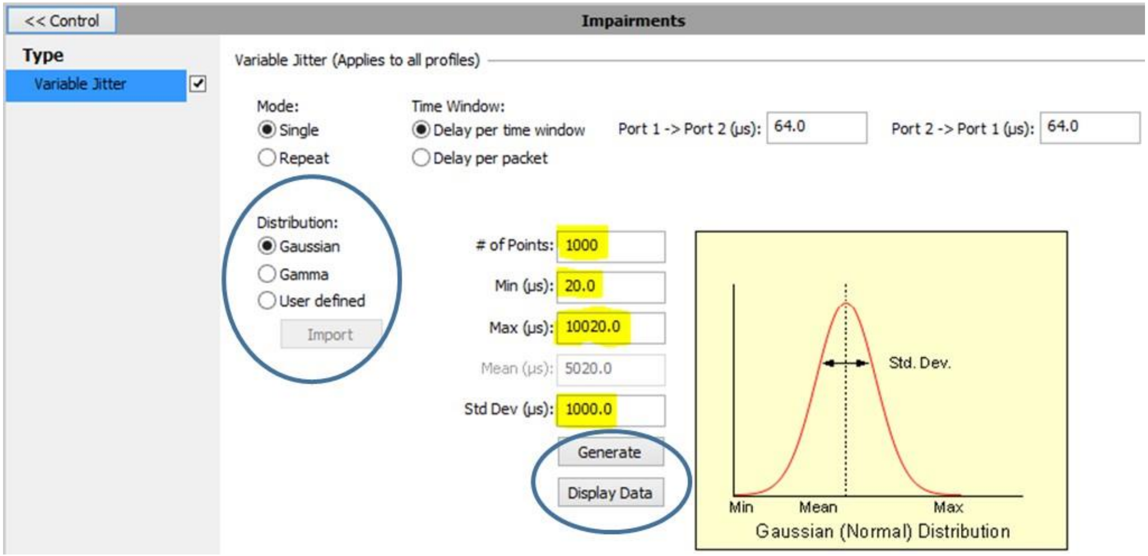
Max (µs): 10020.0

Mean (µs): 5020.0

Std Dev (µs): 1000.0

- **Delay per packet** – The jitter profile is applied to the packets in a "round robin" fashion across all traffic flows. Discrete jitter values are applied to packets in the order that they are transmitted regardless of which flow the packets originated from.
  The jitter profile is therefore distributed over multiple flows rather than applied to each flow individually.
- **Delay per time window –** The jitter profile is applied in a "time-slice" fashion. All packets transmitted in the first "time-slice" are "jittered" using the same discrete value of jitter applied from the pre-defined Jitter profile. In the second "time-slice" all packets are "jittered" using the next discrete jitter value from the jitter profile and so forth. The time slice (Time Window) period is set by the user. In this mode it is not possible to combine Corruptions along with the Variable Jitter impairment.

- Choose the Variable Jitter Distribution profile from the list of **Gaussian**, **Gamma** or **User Defined** as shown encircled below.



Variable Jitter ☑

Variable Jitter (Applies to all profiles)

Mode: ● Single ○ Repeat

Time Window: ● Delay per time window ○ Delay per packet

Port 1 -> Port 2 (µs): 64.0

Port 2 -> Port 1 (µs): 64.0

Distribution: ● Gaussian ○ Gamma ○ User defined

# of Points: 1000

Min (µs): 20.0

Max (µs): 10020.0

Mean (µs): 5020.0

Std Dev (µs): 1000.0

- Enter the parameters of the Jitter Distribution profile in the fields provided as shown highlighted above. The Tables below show the Range/Resolution for the fields.

Gaussian Distribution Parameter Range and Resolution

Parameter	Range (10Gb Interface)	Resolution
Number of packets	1,000 to 10,000,000	1
Min (µS)	15 to 2,000,015 *	0.1
Max (µS)	25 to 3,000,015 *	0.1
Mean (µS)	n/a	n/a
Std Dev (µS)	0 to 3,000,000	0.1

*These values vary slightly for 100Mb and 1Gb interfaces and for the set Intrinsic Delay.

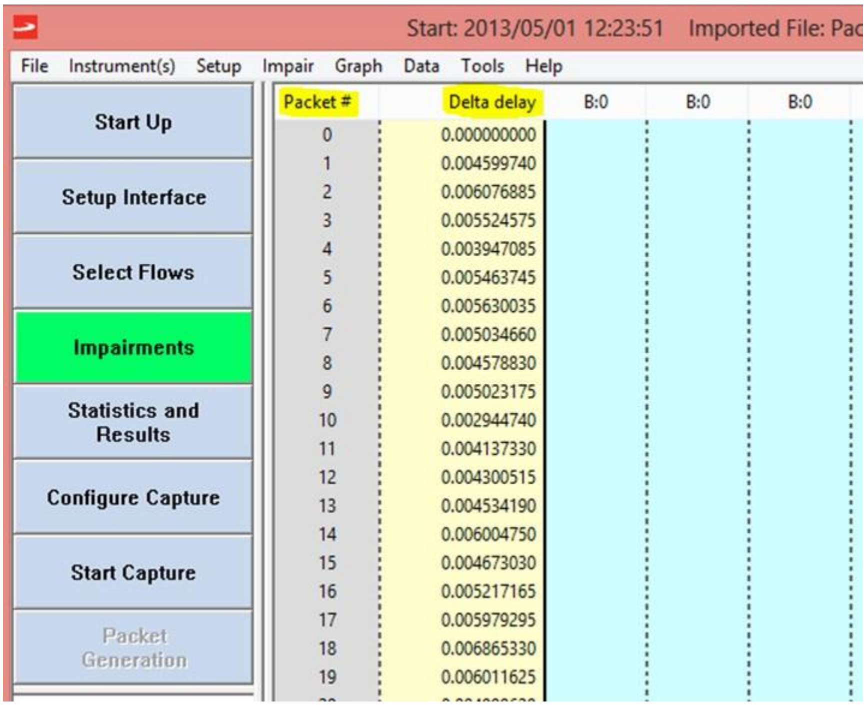
- Mean (µS) – this field indicates the Mean value of jitter given the current user settings. This field is not editable.
- The Standard Deviation defines the spread of the distribution over the range. A small value will result in jitter values close to the mean while a bigger value will spread the jitter values over a wider range.

Gamma Distribution Parameter Range and Resolution

Parameter	Range	Resolution
Number of packets	1,000 to 10,000,000	1
Min (µS)	15 to 2,000,015 *	0.1
Max (µS)	25 to 3,000,015 *	0.1
Alpha (Shape parameter)	1 to 5	0.00001
Beta (Rate parameter)	Fixed at 1	n/a

*These values vary slightly between 100Mb and 1Gb interfaces.

- If Gaussian or Gamma Variable Jitter has been selected, click on the **Generate** button shown encircled on the previous page. This generates the Jitter PDV Profile using the previously set Jitter Distribution parameters.
- The PDV profile can be displayed by clicking on the “Display Data” button. Example shown below.



Packet #	Delta delay	B:0	B:0	B:0
0	0.000000000			
1	0.004599740			
2	0.006076885			
3	0.005524575			
4	0.003947085			
5	0.005463745			
6	0.005630035			
7	0.005034660			
8	0.004578830			
9	0.005023175			
10	0.002944740			
11	0.004137330			
12	0.004300515			
13	0.004534190			
14	0.006004750			
15	0.004673030			
16	0.005217165			
17	0.005979295			
18	0.006865330			
19	0.006011625			

- To view the above PDV Profile on a graph, click on **Graph -> Show Graph** in the Menu Bar.
- Click on the **Impairments** button in the Workflow area of the Network Emulation Application then click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments. The Impairments workflow button will also turn red and say "Stop Impair".

Note: Impairments cannot be edited while they are running. Click on ■ Impairments to stop, then edit the Impairments as required.

For **User defined** Jitter profile;

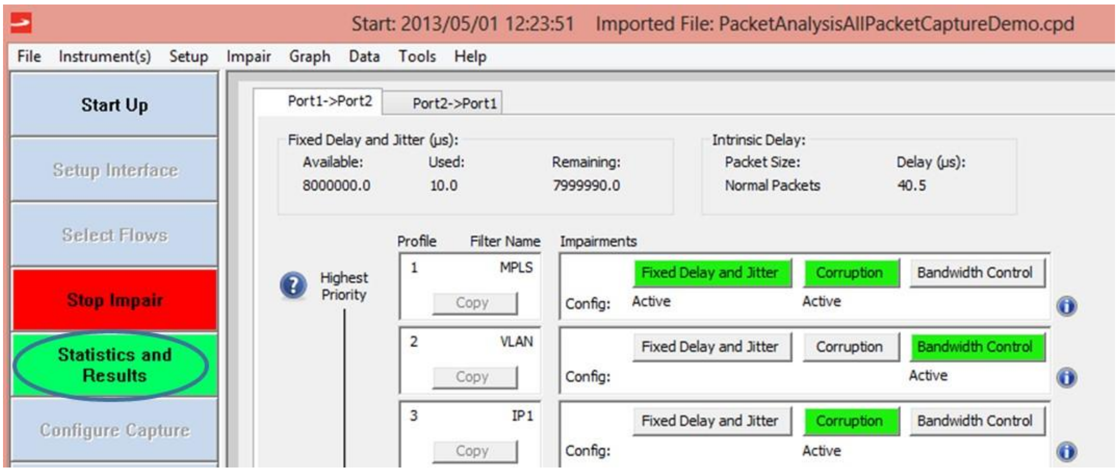
- Click on the **User Defined** radio button then click on the **<Import>** button.
- The user is now prompted for the name and location of the File to be imported.
- Either a .csv or .cpd file type can be imported.
- The file should contain the PDV to be applied as the Jitter Profile.

More details on how to replay a User Defined jitter profile is given in Chapter 7– Capture/Replay of Real Network PDV Profiles.

Chapter 6 – Statistics and Results

The Statistics and Results window displays both port and profile based statistics providing traffic and impairment rates/counts. It also displays packet rates and counts before and after Policing and Shaping as provided in Bandwidth Control.

- Click on the **Statistics and Results** button in the Workflow area as shown encircled below. Note: The Statistics and Results can be viewed while the Impairments are running.



Start: 2013/05/01 12:23:51 Imported File: PacketAnalysisAllPacketCaptureDemo.cpd

Fixed Delay and Jitter (µs):

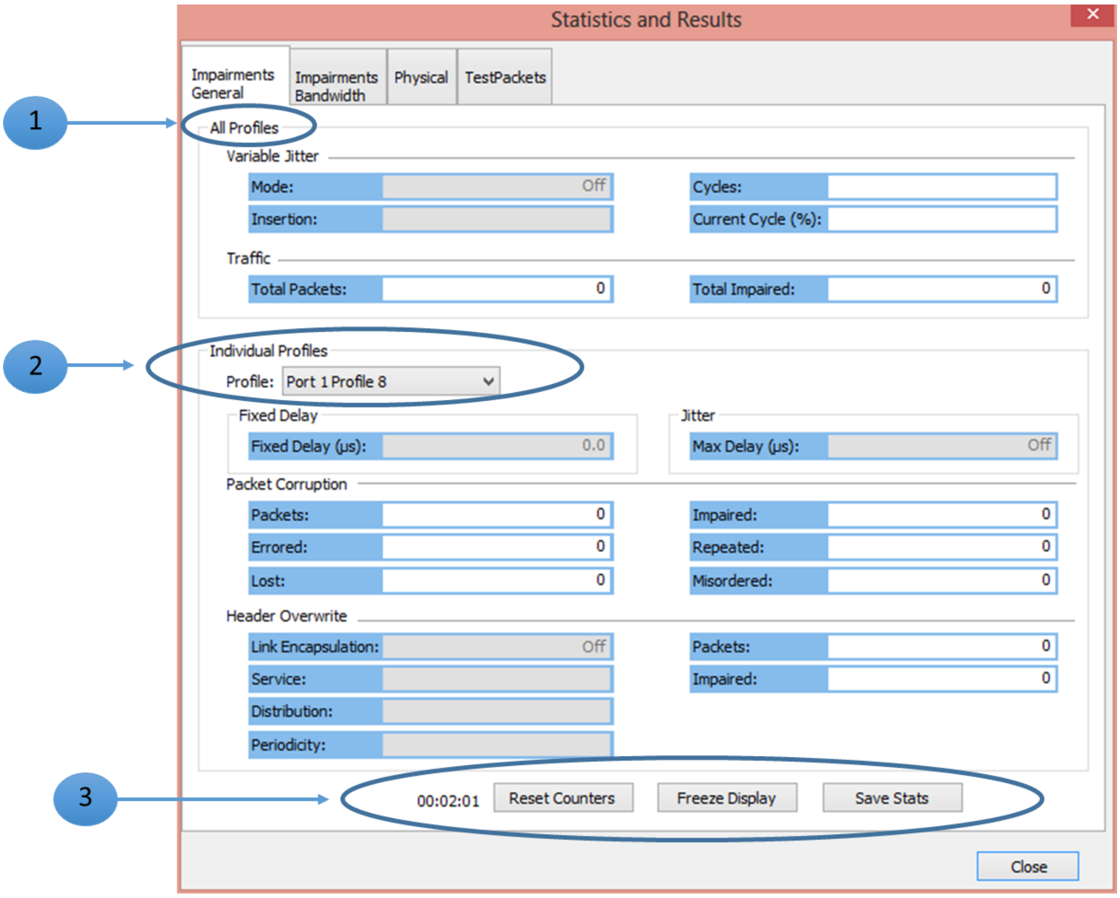
Available:	Used:	Remaining:
8000000.0	10.0	7999990.0

Intrinsic Delay:

Packet Size:	Delay (µs):
Normal Packets	40.5

Profile	Filter Name	Impairments
1	MPLS	Config: Active (Fixed Delay and Jitter), Active (Corruption)
2	VLAN	Config: Active (Bandwidth Control)
3	IP1	Config: Active (Corruption)

The Statistics and Results are displayed as shown below.



All Profiles

Variable Jitter

Mode: Off
Insertion:
Cycles:
Current Cycle (%):

Traffic

Total Packets: 0
Total Impaired: 0

Individual Profiles

Profile: Port 1 Profile 8

Fixed Delay

Fixed Delay (µs): 0.0

Jitter

Max Delay (µs): Off

Packet Corruption

Packets: 0
Errored: 0
Lost: 0
Impaired: 0
Repeated: 0
Misordered: 0

Header Overwrite

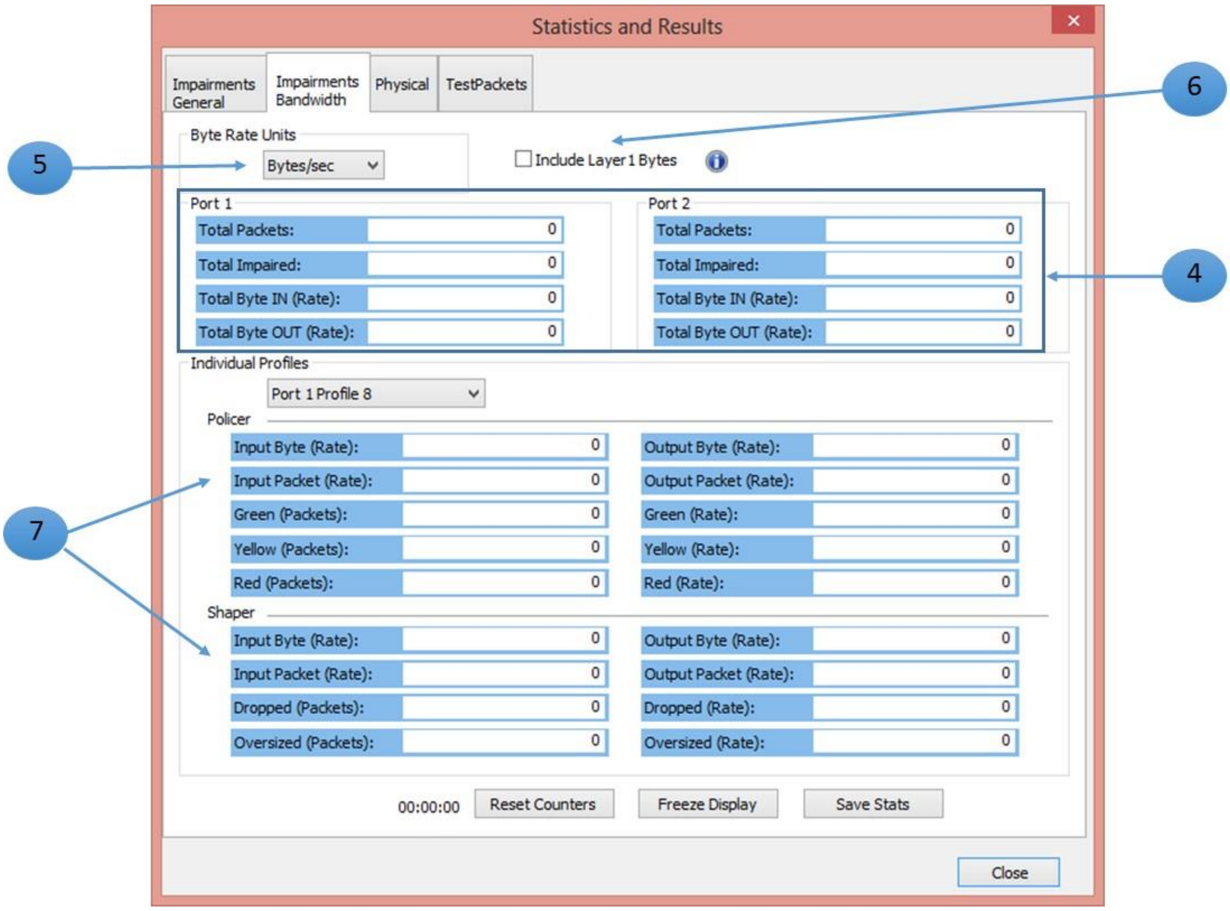
Link Encapsulation: Off
Service:
Distribution:
Periodicity:
Packets: 0
Impaired: 0

00:02:01

The Statistics and Results window has 4 tabs for viewing different pages of results; these are General Impairments, Bandwidth Impairments, Physical and TestPackets. The key features of the General Impairments page are annotated on the graphic shown on the previous page as follows;

1. The top section provides results of impairments that affect all profiles on the instrument ports and also provides a combined total count of all packets received at the ports as well as a total count of how many packets have been impaired.
2. This section provides results on an individual profile basis. The profile of interest is selected from the drop-list.
   Under the Packet Corruption heading there is a count of total packets and impaired packets flowing through each profile. The impaired count is also broken out into each type of impairment (Errored, Lost, Repeated, Misordered).
   Under the Header Overwrite heading the total number of packets flowing through each profile and the count of impaired packets on each profile is displayed.
3. These controls are displayed on all 4 tabs. They provide an Elapsed Time Counter with Reset button, Freeze/Unfreeze Display control and a Save Stats button. More details of operation are given in the bullet points below;
   - The **Elapsed Time Counter** displays the time since the impairments were started, or the time since the **Reset Counter** button was last clicked (whichever is the shortest time). Note that this does not reset the count of cycles completed. Cycle counts are only reset when the **Impairments** button is pressed to start the impairments.
   - The **Freeze/Unfreeze** button freezes all counter displays to make it easier to correlate results. The counters continue running in the background until the **Unfreeze** button is clicked.
   - The **Save Stats** button saves a snapshot of the current results to a CSV file.

The graphic below shows the Bandwidth Impairments results page.



Byte Rate Units: Bytes/sec

□ Include Layer 1 Bytes

Port 1		Port 2	
Total Packets:	0	Total Packets:	0
Total Impaired:	0	Total Impaired:	0
Total Byte IN (Rate):	0	Total Byte IN (Rate):	0
Total Byte OUT (Rate):	0	Total Byte OUT (Rate):	0

Individual Profiles: Port 1 Profile 8

Policer

Input Byte (Rate):	0	Output Byte (Rate):	0
Input Packet (Rate):	0	Output Packet (Rate):	0
Green (Packets):	0	Green (Rate):	0
Yellow (Packets):	0	Yellow (Rate):	0
Red (Packets):	0	Red (Rate):	0

Shaper

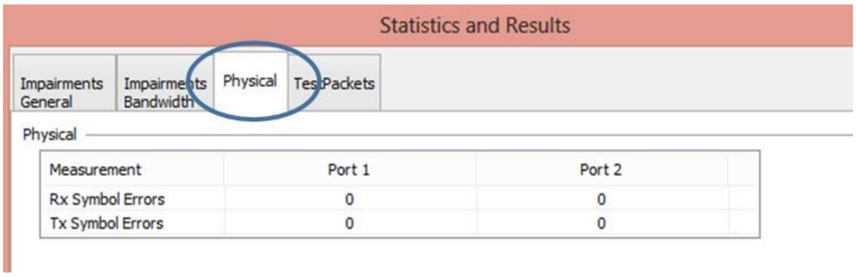
Input Byte (Rate):	0	Output Byte (Rate):	0
Input Packet (Rate):	0	Output Packet (Rate):	0
Dropped (Packets):	0	Dropped (Rate):	0
Oversized (Packets):	0	Oversized (Rate):	0

00:00:00

The key features of the Bandwidth Impairments page are annotated on the graphic shown above as follows;

4. Port level Packet and Byte Rate counters make it easy to see the total number of packets and the byte rate (bandwidth) of the traffic at each port.
5. All results that are “Rate” based can be viewed in either Bytes/sec or Bits/sec by selection from the drop-list shown. For example **Input Byte (Rate)** or **Input Bit (Rate)**.
6. Layer 1 Bytes can be optionally included in “Byte Rate” based results by ticking this checkbox.
7. A count of the Byte Rate and Packet Rate passing through each profile is displayed. The results are viewed one profile at a time. The Profile of interest is selected from the **Individual Profiles** drop-list. These counts are displayed even when no Bandwidth Control impairments are active so they can be viewed at all times.
   When Bandwidth Control impairments are active this display can be used to see the effects and detailed results of Policing and Shaping.

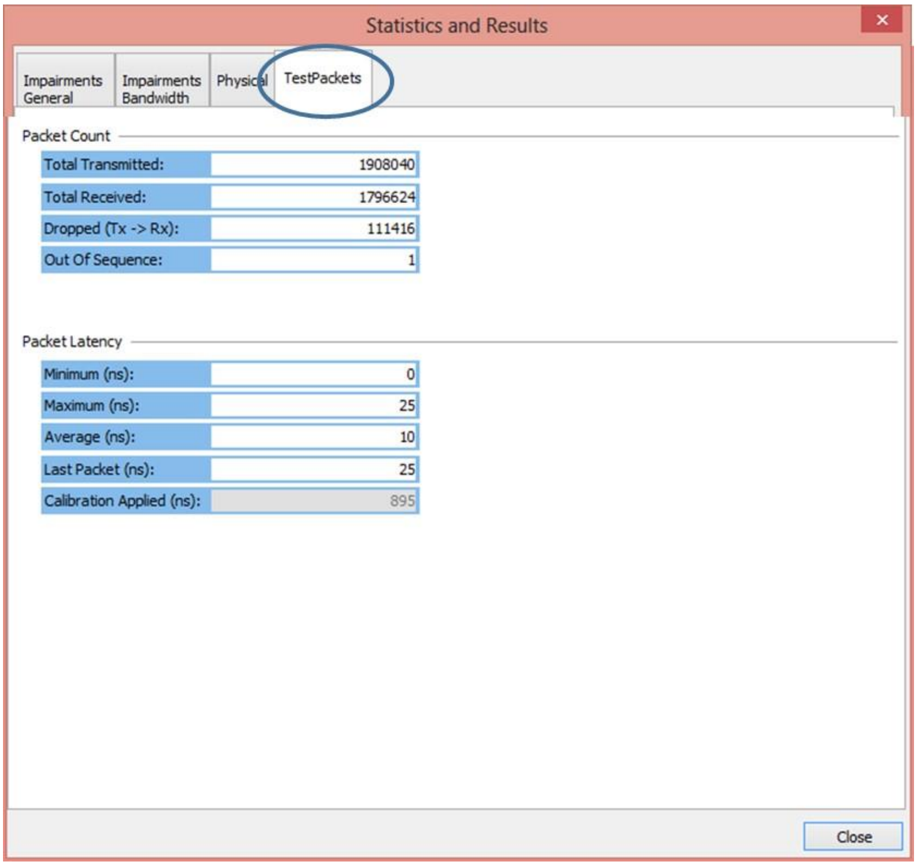
The graphic below shows the Physical Impairments results page. Symbol Errors can be viewed by clicking on the **Physical** tab as shown encircled below.



Physical

Measurement	Port 1	Port 2
Rx Symbol Errors	0	0
Tx Symbol Errors	0	0

When the instrument is set to **Tx + Rx** Mode it can generate Test Packets. In this mode results for Packet Count and Packet Latency can be viewed by clicking on the **TestPackets** tab as shown encircled below.



Packet Count

Total Transmitted:	1908040
Total Received:	1796624
Dropped (Tx -> Rx):	111416
Out Of Sequence:	1

Packet Latency

Minimum (ns):	0
Maximum (ns):	25
Average (ns):	10
Last Packet (ns):	25
Calibration Applied (ns):	895

For more details on TestPacket generation see Appendix 3 - Other Features and Functions.

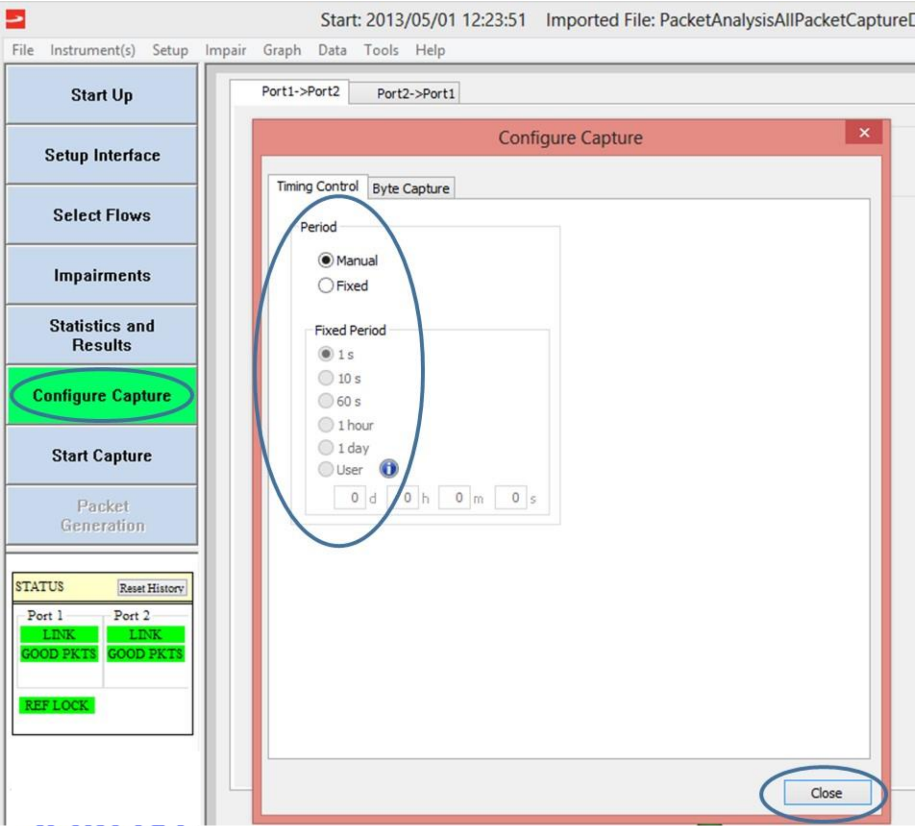
Chapter 7 – Capture/Replay of Real Network PDV Profiles

This chapter describes how to capture real network delay variations creating a Packet Delay Variation profile that can be edited and replayed using Paragon-X Network Emulation. A typical application is to capture real network delay information and save the PDV Profile for playback in the test lab environment.

> **Note:** Capture of Inter-Packet Gap / Packet Delay Variation is for one selected traffic flow only. It is MANDATORY to follow the steps in Chapter 4 – and use Flow Wizard to select a maximum of one flow for capture.

Capturing Real Network PDV Profiles

- Click on the Configure Capture button to configure the capture settings as shown and described below.



Start: 2013/05/01 12:23:51 Imported File: PacketAnalysisAllPacketCaptureD

Period
● Manual
○ Fixed

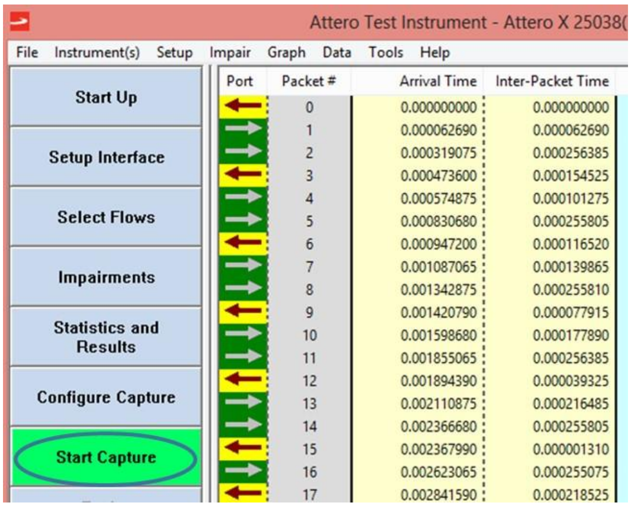
Fixed Period
● 1 s
○ 10 s
○ 60 s
○ 1 hour
○ 1 day
○ User

0 d 0 h 0 m 0 s

On the Timing Control tab shown above the capture period can be set as Manual or Fixed. The Fixed Period sets the capture to run for the chosen pre-set duration. A User-Defined period can also be set. The maximum user-defined period is 3 days. When the capture period is set to manual the capture runs until the user presses the Stop Capture button.

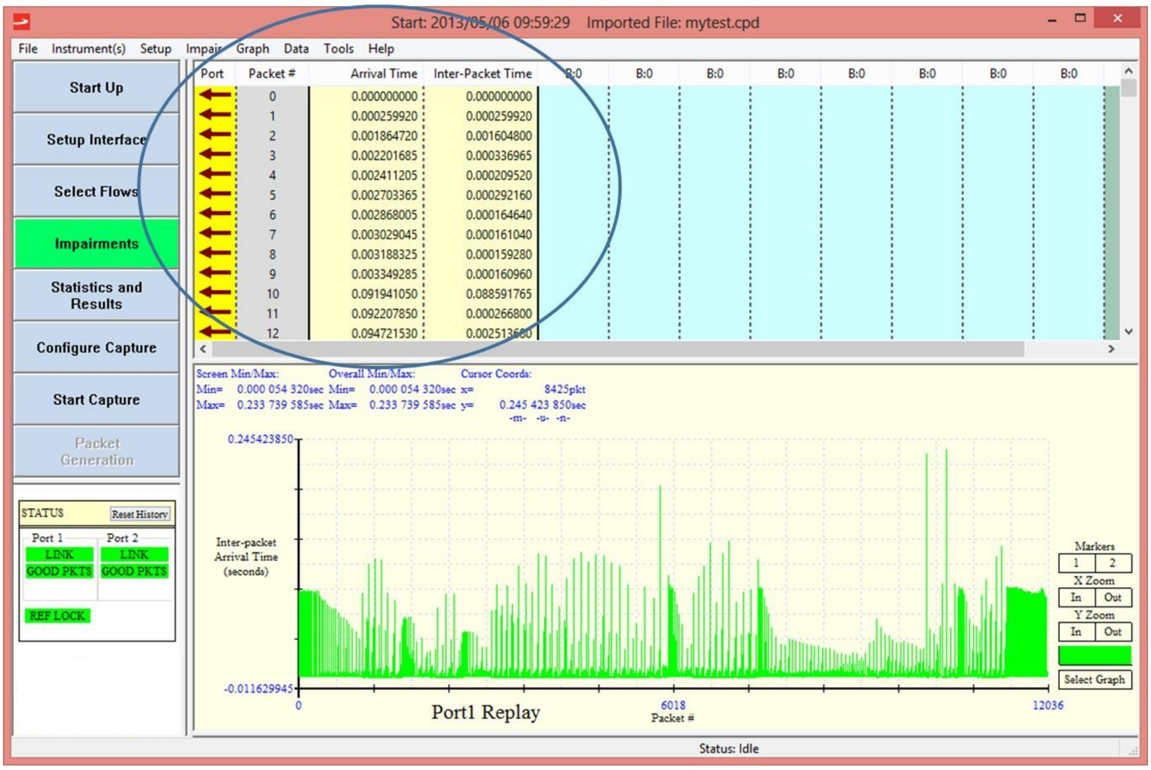
Note: The Capture button is dual purpose. Once the Capture has been started the button changes colour from green to red and becomes the Stop Capture button. Click on this button to stop capturing network delay data when required.

- Click on the Start Capture button as shown encircled below to start capturing.



Port	Packet #	Arrival Time	Inter-Packet Time
←	0	0.000000000	0.000000000
→	1	0.000062690	0.000062690
→	2	0.000319075	0.000256385
←	3	0.000473600	0.000154525
→	4	0.000574875	0.000101275
→	5	0.000830680	0.000255805
←	6	0.000947200	0.000116520
→	7	0.001087065	0.000139865
→	8	0.001342875	0.000255810
←	9	0.001420790	0.000077915
→	10	0.001598680	0.000177890
→	11	0.001855065	0.000256385
←	12	0.001894390	0.000039325
→	13	0.002110875	0.000216485
→	14	0.002366680	0.000255805
←	15	0.002367990	0.000001310
→	16	0.002623065	0.000255075
←	17	0.002841590	0.000218525

The Arrival Time and Inter-Packet Time for each packet will be displayed as shown below. The coloured arrows denote the Port that each packet was received on. An arrow pointing right signifies the packet was received on Port1. An arrow pointing left signifies the packet was received on Port2. A graph plotting the Packet Arrival Time profile is also displayed. The graph is enabled by clicking on **Graph -> Show Graph** in the Menu Bar.



Port	Packet #	Arrival Time	Inter-Packet Time
←	0	0.000000000	0.000000000
←	1	0.000259920	0.000259920
←	2	0.001864720	0.001604800
←	3	0.002201685	0.000336965
←	4	0.002411205	0.000209520
←	5	0.002703365	0.000292160
←	6	0.002868005	0.000164640
←	7	0.003029045	0.000161040
←	8	0.003188325	0.000159280
←	9	0.003349285	0.000160960
←	10	0.091941050	0.088591765
←	11	0.092207850	0.000266800
←	12	0.094721530	0.002513680

```
Screen Min/Max:            Overall Min/Max:           Cursor Coords:
Min=   0.000 054 320sec    Min=   0.000 054 320sec    x=          8425pkt
Max=   0.233 739 585sec    Max=   0.233 739 585sec    y=   0.245 423 850sec
                                                            -m-  -u-  -n-
```

The Arrival Time is the time that a particular packet arrived relative to the arrival time of the first packet. The Inter-Packet Time is the time that a particular packet arrived relative to the time that the previous packet arrived.

The graph provides a readout of the x, y co-ordinates when the cursor is placed on the graph. It also displays the maximum and minimum values for the complete data set and for the currently displayed data. The graph also provides Marker and Zoom features to allow the user to focus in on a specific area and easily read-off the inter-packet delay values.

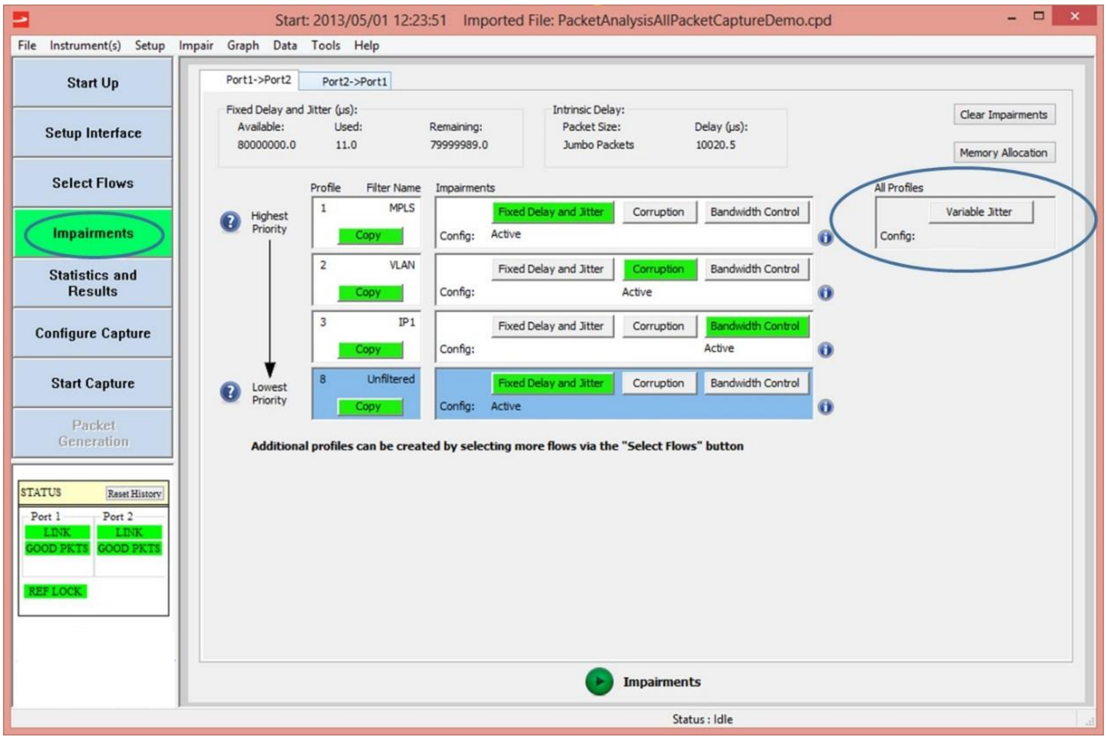
Detailed information on graph features is given in Chapter 9 on page 74.

The PDV Profile can now be saved for subsequent analysis in the lab.

- In the Menu Bar click on **File -> Export** and save the file as type **.cpd** (Calnex Packet Data). Note that the PDV Profile can also be saved as a .csv file. This file type takes up more space, but has the advantage that the PDV content can be edited.

Importing and Re-Playing Packet Delay Variation Profiles

- The PDV profile is extracted from the imported file and superimposed onto the original PDV on all Traffic passing through the instrument. Other impairments can be added simultaneously with the PDV replay. Packets can also be marked to be dropped from the PDV profile. This is detailed later in this chapter.
- Click on the **Impairments** button in the Workflow area as shown encircled below.
- Click on the **Variable Jitter** impairment element as shown encircled below.



Start: 2013/05/01 12:23:51 Imported File: PacketAnalysisAllPacketCaptureDemo.cpd

Fixed Delay and Jitter (µs):

Available:	Used:	Remaining:
80000000.0	11.0	79999989.0

Intrinsic Delay:

Packet Size:	Delay (µs):
Jumbo Packets	10020.5

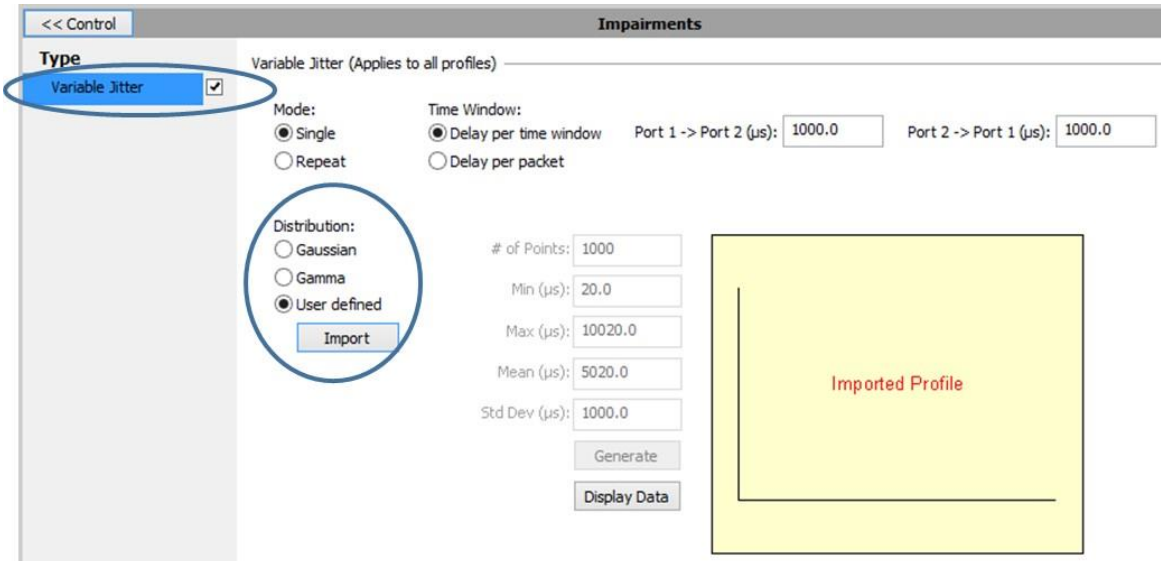
Profile	Filter Name	Impairments	Config:
1	MPLS	Fixed Delay and Jitter	Active
2	VLAN	Corruption	Active
3	IP1	Bandwidth Control	Active
8	Unfiltered	Fixed Delay and Jitter	Active

Additional profiles can be created by selecting more flows via the "Select Flows" button

Status : Idle

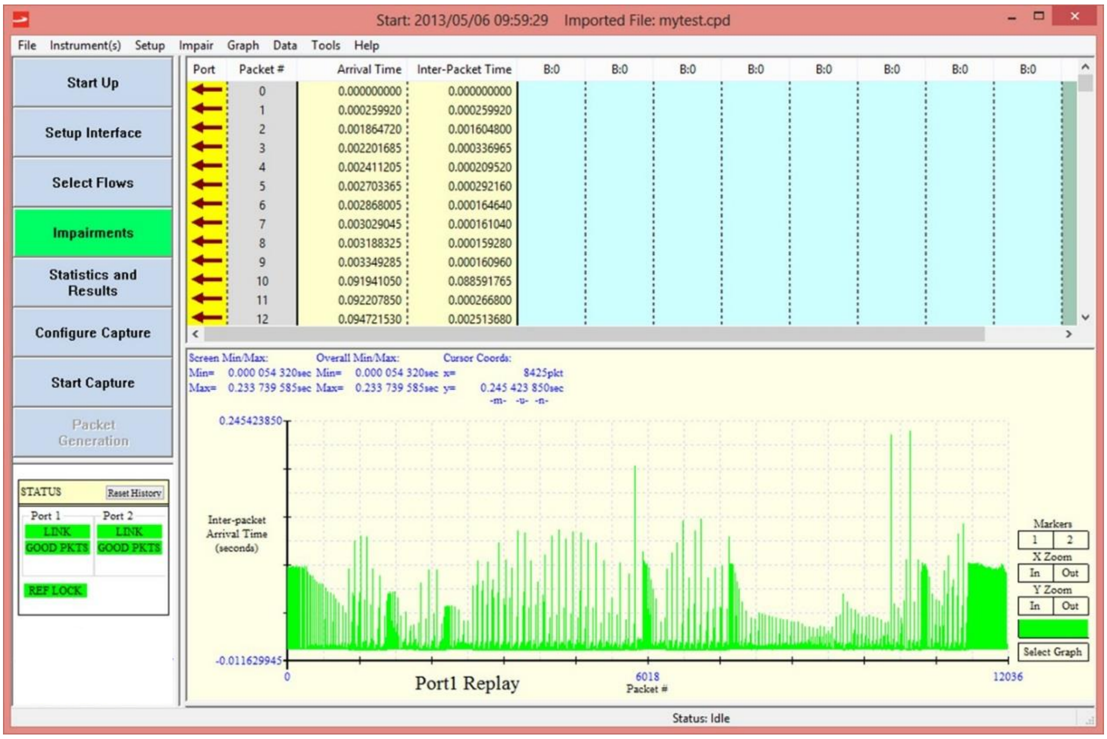
- Enable Variable Jitter by clicking on the **Variable Jitter Checkbox** as shown encircled below.
- Set the **Mode** and **Time Window** settings. These are explained in sub-section entitled **Adding Variable Jitter Impairment** on page 56.

- Click on the **User Defined** radio button as shown encircled below.



- Click on the **Import** button and choose the previously saved .cpd (or .csv) file that contains the PDV profile to be replayed.

When the file has been imported the packet data display will appear showing the PDV profile. The graph is enabled by clicking on **Graph -> Show Graph** in the Menu Bar.



Port	Packet #	Arrival Time	Inter-Packet Time	B:0	B:0	B:0	B:0	B:0	B:0	B:0	B:0
←	0	0.000000000	0.000000000								
←	1	0.000259920	0.000259920								
←	2	0.001864720	0.001604800								
←	3	0.002201685	0.000336965								
←	4	0.002411205	0.000209520								
←	5	0.002703365	0.000292160								
←	6	0.002868005	0.000164640								
←	7	0.003029045	0.000161040								
←	8	0.003188325	0.000159280								
←	9	0.003349285	0.000160960								
←	10	0.091941050	0.088591765								
←	11	0.092207850	0.000266800								
←	12	0.094721530	0.002513680								

Screen Min/Max:		Overall Min/Max:		Cursor Coords:	
Min=	0.000 054 320sec	Min=	0.000 054 320sec	x=	8425pkt
Max=	0.233 739 585sec	Max=	0.233 739 585sec	y=	0.245 423 850sec
					-m- -u- -n-

- Click on the **Impairments** button in the workflow area.
- Click on **<<Control** to return to the Impairments Summary View.
- When all required impairments have been added to the profiles click on ▶ Impairments to apply the Impairment Profiles to the traffic flowing through the instrument.

The button will change from ▶ Impairments to ■ Impairments.

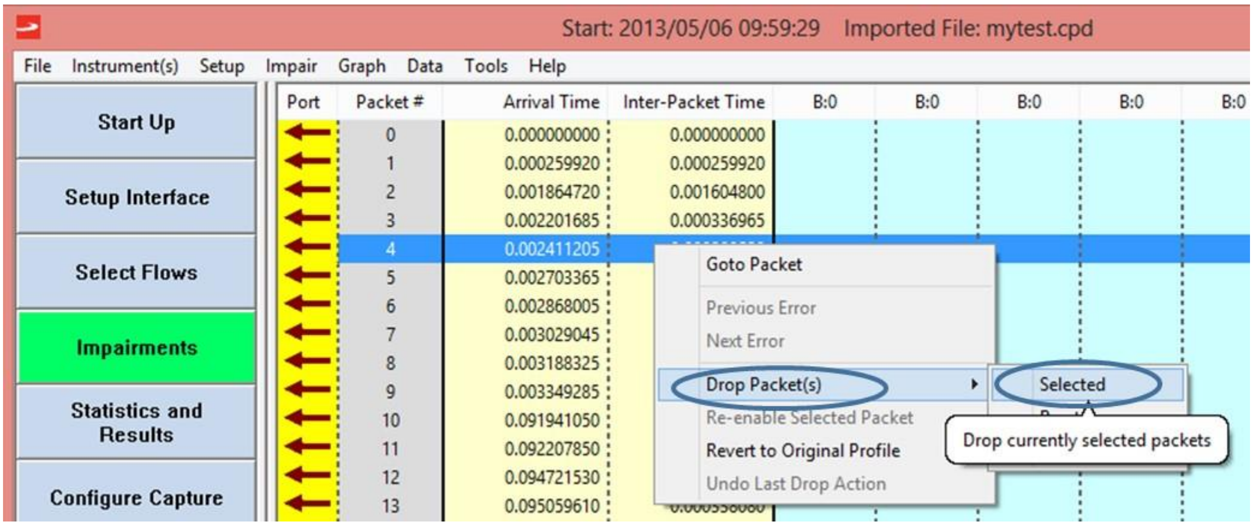
Note: Impairments cannot be edited while they are running. Click on ■ Impairments to stop, then edit the Impairments as required.

Dropping Packets during Profile Replay

This feature allows a captured PDV profile to be altered so that packets are dropped on a replay of the manipulated profile. A series of profiles can be generated from a single profile to allow the investigation of the impact of progressively longer intervals of packet drop out. The user should remember to save profiles created into suitably named files should they be required for future replay. There are undo features to re-enable packets allowing ease of experimentation or margin testing.

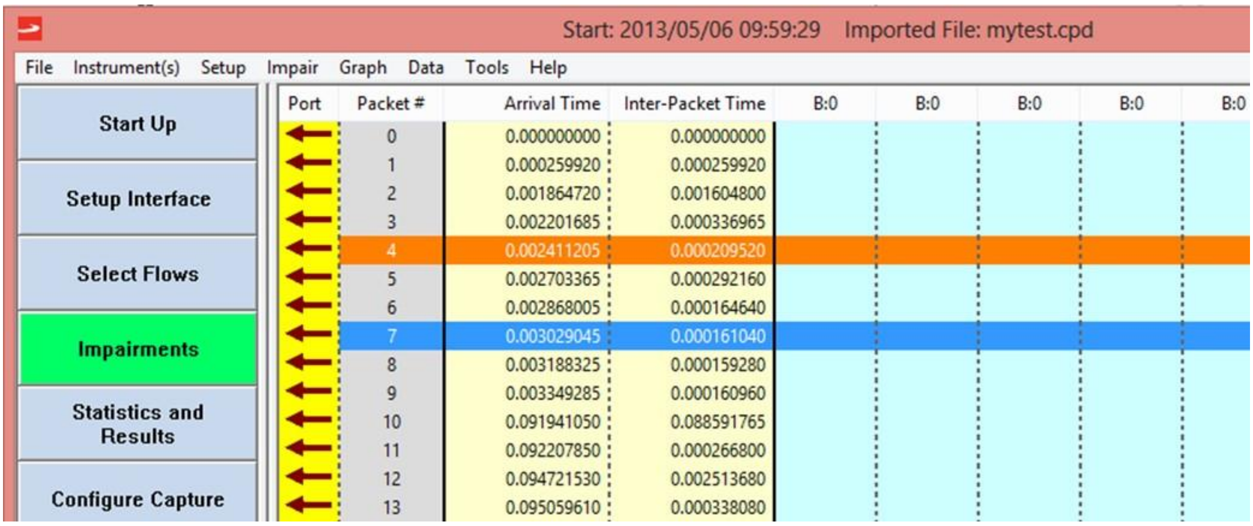
The packets to be dropped can be selected individually, as a burst, or as a periodic series as described below.

- To drop an individual packet right-click on the specific packet row location in the Data table display area. The entry will highlight in blue and a selection menu will pop-up. Select **Dropped Packet(s)**, then **Selected** as shown below.
  Note: If the graph is displayed it can be hidden by clicking **Graph** -> **Hide Graph**.



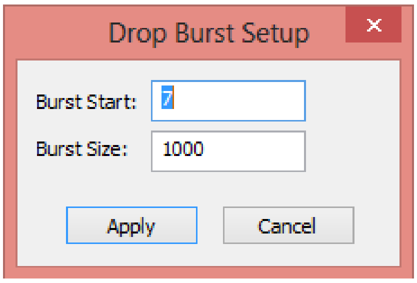
Port	Packet #	Arrival Time	Inter-Packet Time	B:0	B:0	B:0	B:0	B:0
←	0	0.000000000	0.000000000					
←	1	0.000259920	0.000259920					
←	2	0.001864720	0.001604800					
←	3	0.002201685	0.000336965					
←	4	0.002411205						
←	5	0.002703365						
←	6	0.002868005						
←	7	0.003029045						
←	8	0.003188325						
←	9	0.003349285						
←	10	0.091941050						
←	11	0.092207850						
←	12	0.094721530						
←	13	0.095059610						

This will mark the packet to be dropped. This is confirmed by the background colour for the line turning orange as shown below.



Port	Packet #	Arrival Time	Inter-Packet Time	B:0	B:0	B:0	B:0	B:0
←	0	0.000000000	0.000000000					
←	1	0.000259920	0.000259920					
←	2	0.001864720	0.001604800					
←	3	0.002201685	0.000336965					
←	4	0.002411205	0.000209520					
←	5	0.002703365	0.000292160					
←	6	0.002868005	0.000164640					
←	7	0.003029045	0.000161040					
←	8	0.003188325	0.000159280					
←	9	0.003349285	0.000160960					
←	10	0.091941050	0.088591765					
←	11	0.092207850	0.000266800					
←	12	0.094721530	0.002513680					
←	13	0.095059610	0.000338080					

- To drop a burst of packets right-click on the specific packet row location of the first packet in the burst. The entry will highlight in blue and a dialog box will pop-up. Select **Dropped Packet(s)**, then **Burst.** This brings up the dialog box shown below.



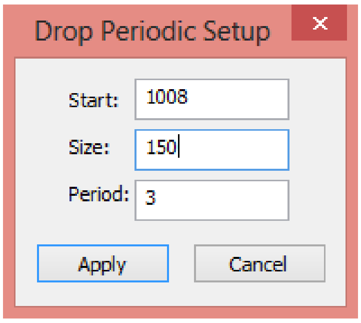
Burst Start: 7

Burst Size: 1000

- Set the **Burst Start** position **Burst Size** required, then click on **Apply.**

Again the table will be updated indicating the packets to be dropped with an orange background.

- To select a periodic drop of packets repeat the above but select **Drop Packet(s)**, then **Periodic**. This brings up the dialog box shown below.

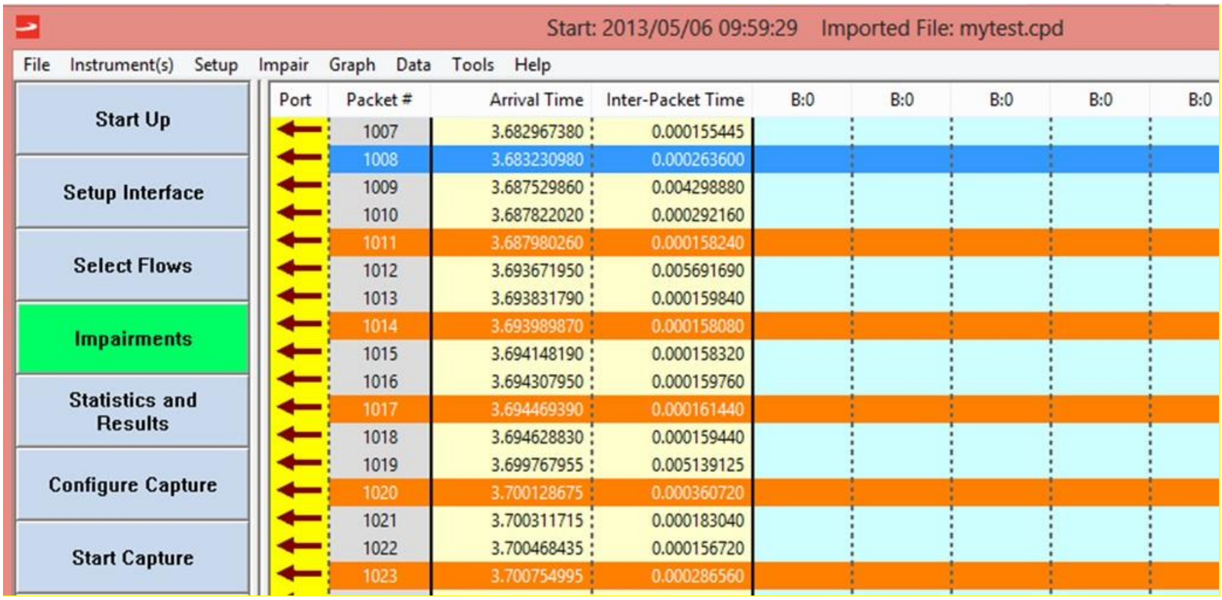


Start: 1008

Size: 150

Period: 3

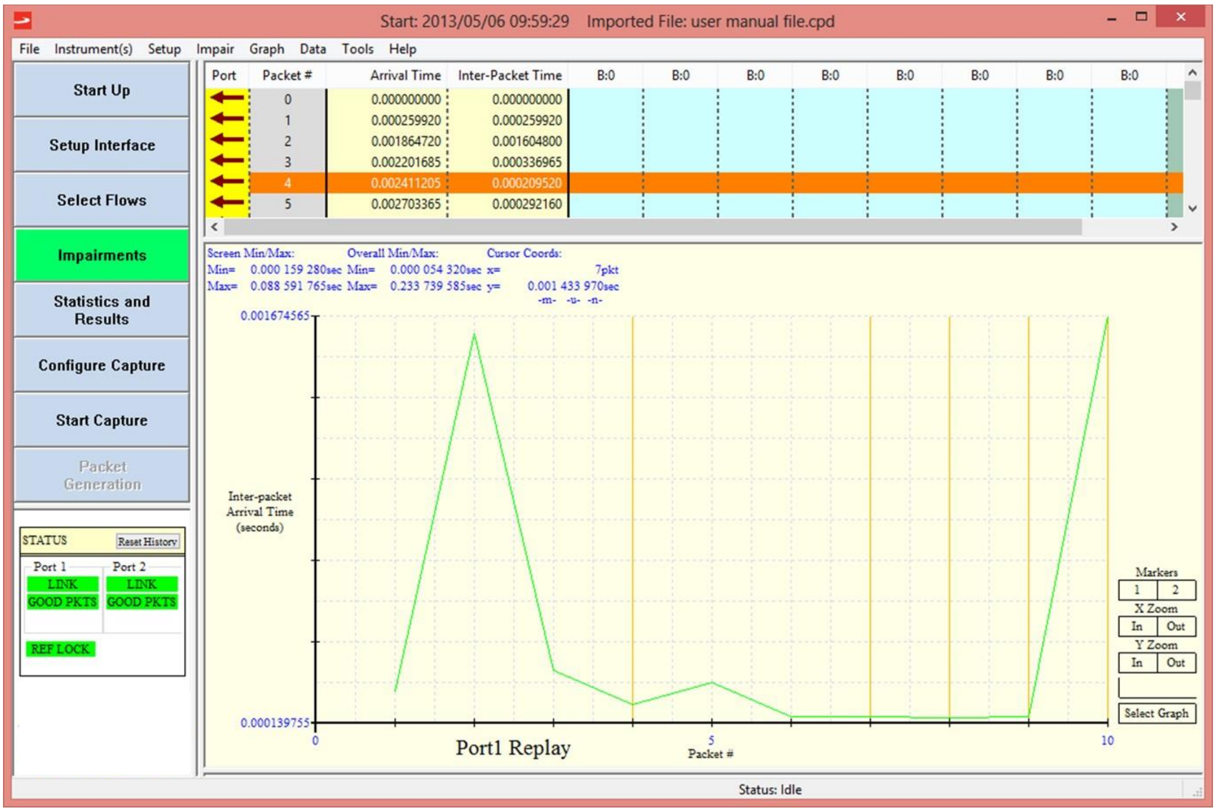
This allows the repeat interval to be set by entering a value in the **Period** field. The **Size** field is used to set the range of packets over which the repeat applies. So with Period set to 3 the following table display will result.



Start: 2013/05/06 09:59:29 Imported File: mytest.cpd

Port	Packet #	Arrival Time	Inter-Packet Time	B:0	B:0	B:0	B:0	B:0
←	1007	3.682967380	0.000155445					
←	1008	3.683230980	0.000263600					
←	1009	3.687529860	0.004298880					
←	1010	3.687822020	0.000292160					
←	1011	3.687980260	0.000158240					
←	1012	3.693671950	0.005691690					
←	1013	3.693831790	0.000159840					
←	1014	3.693989870	0.000158080					
←	1015	3.694148190	0.000158320					
←	1016	3.694307950	0.000159760					
←	1017	3.694469390	0.000161440					
←	1018	3.694628830	0.000159440					
←	1019	3.699767955	0.005139125					
←	1020	3.700128675	0.000360720					
←	1021	3.700311715	0.000183040					
←	1022	3.700468435	0.000156720					
←	1023	3.700754995	0.000286560					

The various modes of selection packets can be repeated to allow the desired pattern to be built up. Additionally the graph will be marked to show the position of packets to be dropped during the replay. Vertical orange bars appear at the appropriate time locations on the graph as shown below.



Port	Packet #	Arrival Time	Inter-Packet Time	B:0	B:0	B:0	B:0	B:0	B:0	B:0	B:0
←	0	0.000000000	0.000000000								
←	1	0.000259920	0.000259920								
←	2	0.001864720	0.001604800								
←	3	0.002201685	0.000336965								
←	4	0.002411205	0.000209520								
←	5	0.002703365	0.000292160								

Screen Min/Max: Overall Min/Max: Cursor Coords:
Min= 0.000 159 280sec Min= 0.000 054 320sec x= 7pkt
Max= 0.088 591 765sec Max= 0.233 739 585sec y= 0.001 433 970sec
-m- -u- -n-

There are “undo” controls to de-select packets for drop. These are accessed by right clicking the mouse in the Data table display area.

- **Undo Last Drop Action**. This allows for a single level of resetting.
- **Re-enable Selected Packet** will allow one packet to be unselected and replayed correctly. This applies regardless of the method of causing the drop, individual, burst or periodic.
- **Revert to Original Profile** will reset all the packets selected to be dropped since the file was loaded or captured.

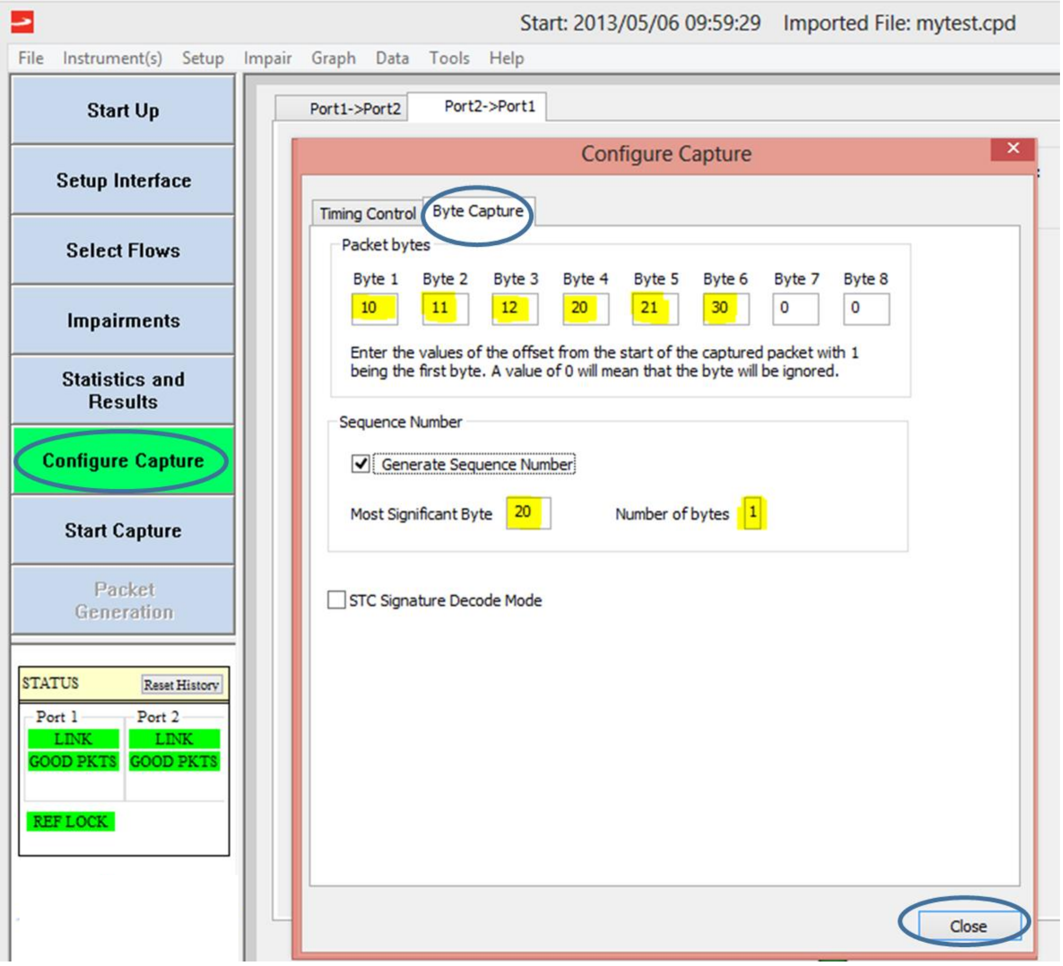
Once a profile of dropped packets has been created it can be saved for subsequent re-use by clicking on **File**, then **Export** in the Menu Bar. These files are saved as type **.cpd**

Note: The Random Packet Loss **Checkbox** must be ticked in order to drop packets from a PDV profile replay. No other Random Packet Loss settings are valid in this situation. Do not generate a Random Packet Loss Profile at this time or the dropped packets profile will be overwritten.

Chapter 8 - Capturing Selected Packet Byte Information

In addition to capturing network delay or Packet Delay Variation profile, described in Chapter 7, the Paragon-X Network Emulation application can simultaneously capture selected bytes from the incoming traffic.

- **Note:** Capture of Inter-Packet Gap / Packet Delay Variation is for one selected traffic flow only. It is MANDATORY to follow the steps in Chapter 4 – and use Flow Wizard to select a maximum of one flow for capture.
- Click the Configure Capture button, then click on the Byte Capture Tab (shown encircled below) to select the Packet bytes to be captured and displayed.



Packet bytes

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8
10	11	12	20	21	30	0	0

Enter the values of the offset from the start of the captured packet with 1 being the first byte. A value of 0 will mean that the byte will be ignored.

Sequence Number

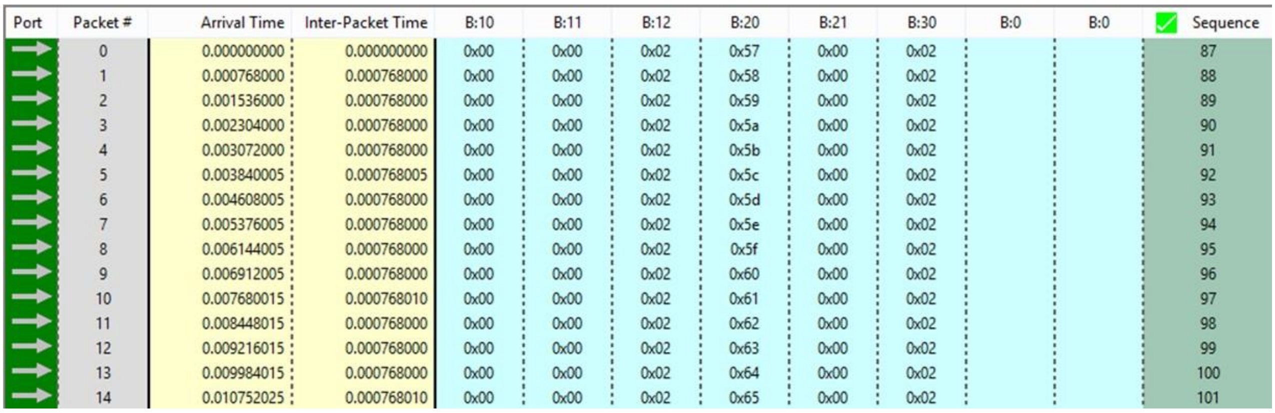
☑ Generate Sequence Number

Most Significant Byte 20 Number of bytes 1

☐ STC Signature Decode Mode

In the above example Packet bytes 10, 11, 12, 20, 21 and 30 are set to be captured for each packet received and byte 20 is used to generate a Sequence Number.

- Click on the Close button once the Byte Capture settings are complete.
- Click on Start Capture to start capturing Packet delay information and the selected Packet bytes. The resulting network delay capture display is shown on the next page.

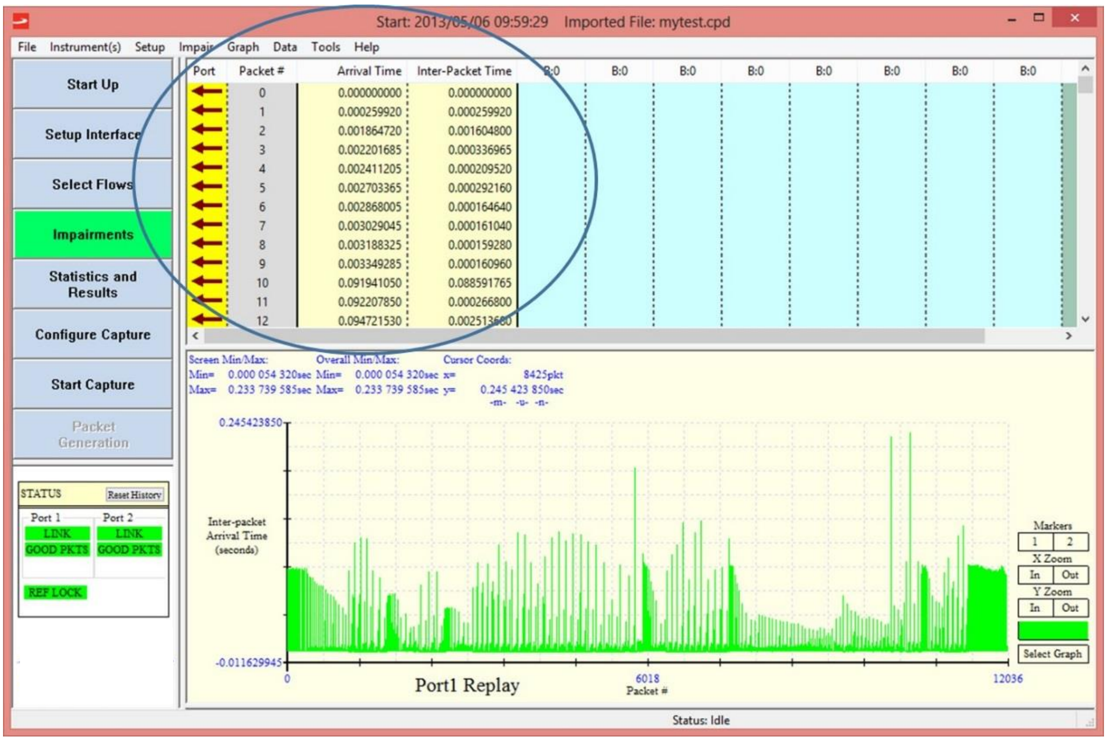


Port	Packet #	Arrival Time	Inter-Packet Time	B:10	B:11	B:12	B:20	B:21	B:30	B:0	B:0	☑ Sequence
→	0	0.000000000	0.000000000	0x00	0x00	0x02	0x57	0x00	0x02			87
→	1	0.000768000	0.000768000	0x00	0x00	0x02	0x58	0x00	0x02			88
→	2	0.001536000	0.000768000	0x00	0x00	0x02	0x59	0x00	0x02			89
→	3	0.002304000	0.000768000	0x00	0x00	0x02	0x5a	0x00	0x02			90
→	4	0.003072000	0.000768000	0x00	0x00	0x02	0x5b	0x00	0x02			91
→	5	0.003840005	0.000768005	0x00	0x00	0x02	0x5c	0x00	0x02			92
→	6	0.004608005	0.000768000	0x00	0x00	0x02	0x5d	0x00	0x02			93
→	7	0.005376005	0.000768000	0x00	0x00	0x02	0x5e	0x00	0x02			94
→	8	0.006144005	0.000768000	0x00	0x00	0x02	0x5f	0x00	0x02			95
→	9	0.006912005	0.000768000	0x00	0x00	0x02	0x60	0x00	0x02			96
→	10	0.007680015	0.000768010	0x00	0x00	0x02	0x61	0x00	0x02			97
→	11	0.008448015	0.000768000	0x00	0x00	0x02	0x62	0x00	0x02			98
→	12	0.009216015	0.000768000	0x00	0x00	0x02	0x63	0x00	0x02			99
→	13	0.009984015	0.000768000	0x00	0x00	0x02	0x64	0x00	0x02			100
→	14	0.010752025	0.000768010	0x00	0x00	0x02	0x65	0x00	0x02			101

Any packets that are out-of-sequence (mis-ordered) are highlighted.

Chapter 9 – Packet Delay Display and Graphs

The main features and functions of the Packet Delay Display and graphs are described in this chapter.

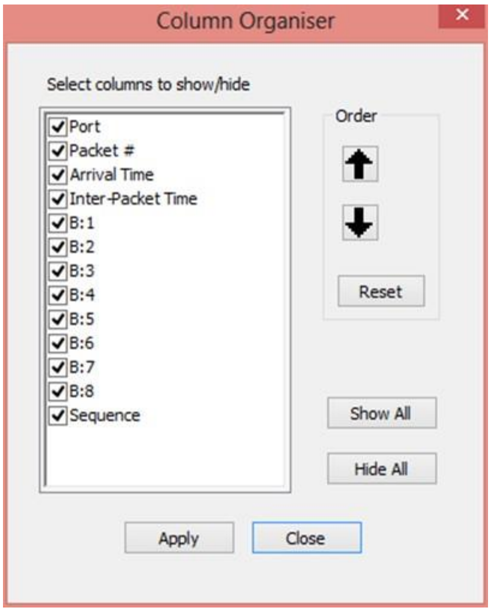


Port	Packet #	Arrival Time	Inter-Packet Time	B:0	B:0	B:0	B:0	B:0	B:0	B:0	B:0
←	0	0.000000000	0.000000000								
←	1	0.000259920	0.000259920								
←	2	0.001864720	0.001604800								
←	3	0.002201685	0.000336965								
←	4	0.002411205	0.000209520								
←	5	0.002703365	0.000292160								
←	6	0.002868005	0.000164640								
←	7	0.003029045	0.000161040								
←	8	0.003188325	0.000159280								
←	9	0.003349285	0.000160960								
←	10	0.091941050	0.088591765								
←	11	0.092207850	0.000266800								
←	12	0.094721530	0.002513680								

Screen Min/Max:		Overall Min/Max:		Cursor Coords:	
Min=	0.000 054 320sec	Min=	0.000 054 320sec	x=	8425pkt
Max=	0.233 739 585sec	Max=	0.233 739 585sec	y=	0.245 423 850sec
					-m- -u- -n-

Delay Display Column Organiser

This feature allows the user to select which sets of data are displayed on the Delay Display table, and in which order. The results tables are shown encircled above. To access this feature use the drop down menu **Data -> Column Organiser**. This will bring up the control dialog as shown below.



Select columns to show/hide

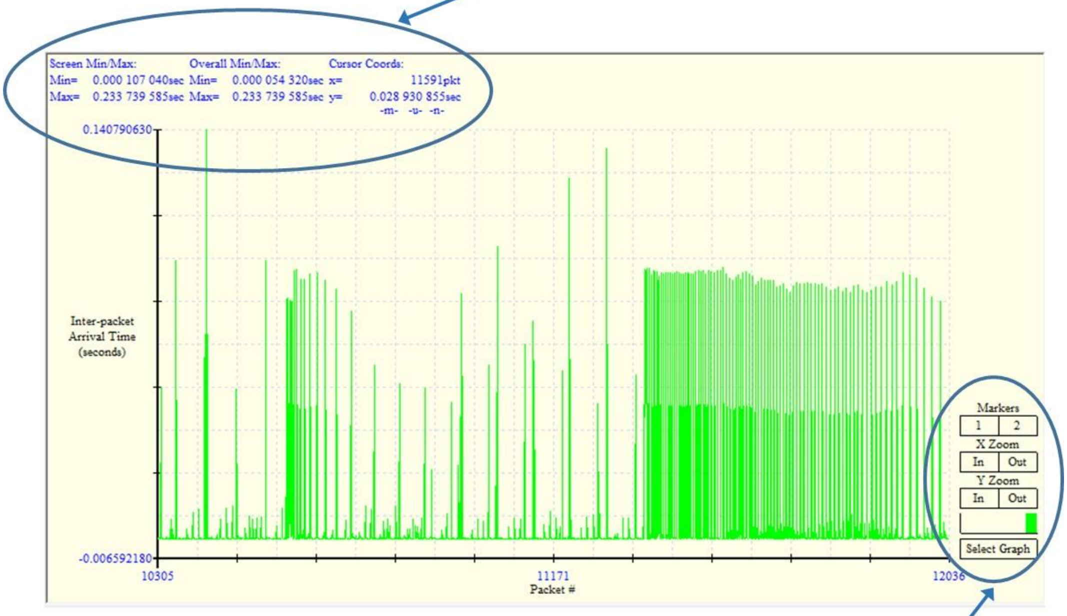
- ☑ Port
- ☑ Packet #
- ☑ Arrival Time
- ☑ Inter-Packet Time
- ☑ B:1
- ☑ B:2
- ☑ B:3
- ☑ B:4
- ☑ B:5
- ☑ B:6
- ☑ B:7
- ☑ B:8
- ☑ Sequence

The Checkboxes with ticks indicate the columns set for display, to suppress the display of a column un-tick the Checkbox. To change the order of display highlight a particular field and move it using the up/down arrows to place it in the correct order.

Graph Overview

A graph of inter-packet arrival time can be plotted by clicking on **Graph -> Show Graph.** The graph data is derived from the current capture buffer or imported capture file. An example graph display is shown below.

Measurement Data



```
Screen Min/Max:            Overall Min/Max:           Cursor Coords:
Min=   0.000 107 040sec   Min=   0.000 054 320sec   x=           11591pkt
Max=   0.233 739 585sec   Max=   0.233 739 585sec   y=    0.028 930 855sec
                                                            -m-  -u-  -n-
```

Graph Menu and Control Buttons

The display provides "Measurement Data" relating to the plotted graph and also convenient "Graph Menu and Control Buttons" to set Markers and adjust the Zoom factor of the graph. The locations of these features are shown encircled above. These features are described in the following sections.

The graph has 2 modes;

- Inter-packet Arrival Time versus Time
- Inter-packet Arrival Time versus Packet Number

The mode is selected by clicking on **Graph -> Graph Display Mode** from the Menu Bar (or **Select Graph -> Graph Display Mode** using the "Graph Menu and Control Buttons" shown above).

When the "Inter-packet Arrival Time versus Time" mode is selected the Time Format can be chosen between;

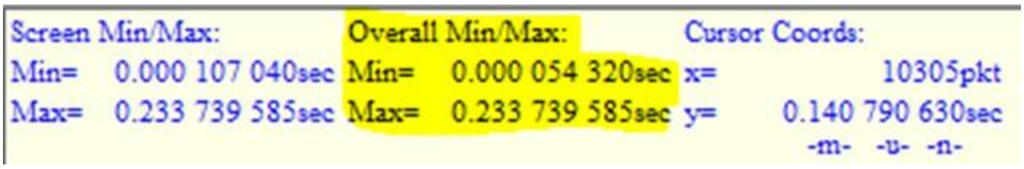
- **Time** – the x-axis is the instrument elapsed time (starts at zero)
- **Measured** – the x-axis includes the windows date/time at the start of the capture

This is selected by clicking **Graph -> Time Format**.

Graph Measurement Data

The graph displays the overall minimum and maximum values of the complete data set – this is shown highlighted in yellow below. It also displays the minimum and maximum values of the currently displayed data set.

The display provides a readout of the x, y co-ordinates when the cursor is placed on the graph.



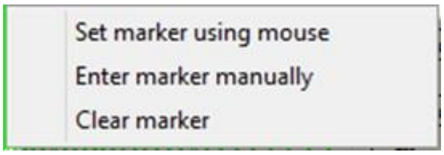
```
Screen Min/Max:             Overall Min/Max:            Cursor Coords:
Min=   0.000 107 040sec     Min=   0.000 054 320sec     x=              10305pkt
Max=   0.233 739 585sec     Max=   0.233 739 585sec     y=      0.140 790 630sec
                                                              -m-   -u-   -n-
```

Adding a Marker

Markers can be added to the graph to pin-point areas of interest. The graph will automatically display the x, y co-ordinates of the markers and also the delta value between the markers.

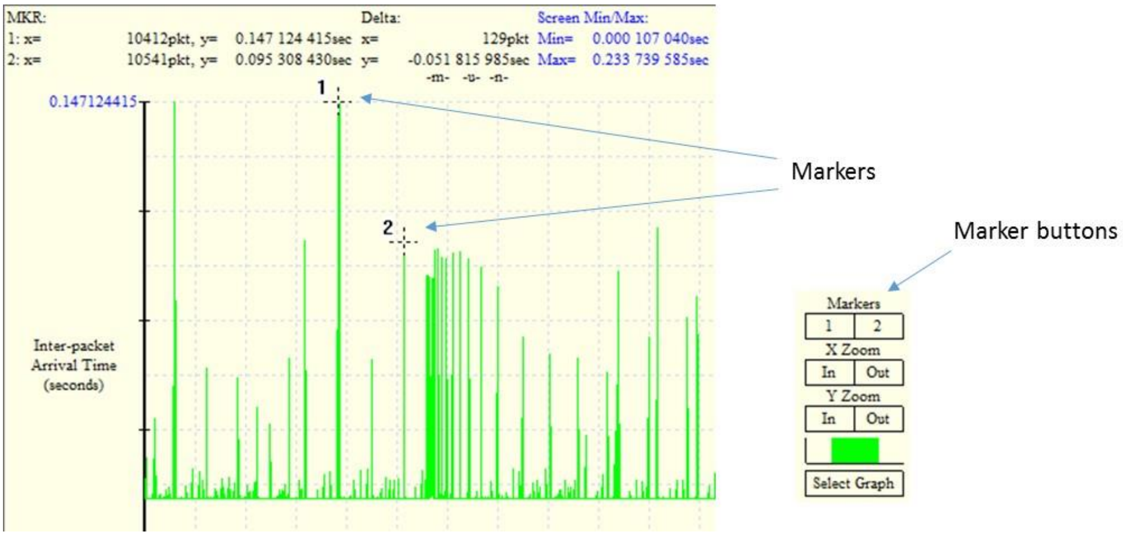
To add a marker;

- Click on the Marker Button (shown below). The pop-up below will be displayed.



- Choose "Set marker using mouse".
- Now click on the point of interest on the graph to set the marker.

An example display showing 2 Markers is shown below.



```
MKR:                                          Delta:                       Screen Min/Max:
1: x=       10412pkt, y=   0.147 124 415sec   x=              129pkt       Min=   0.000 107 040sec
2: x=       10541pkt, y=   0.095 308 430sec   y=   -0.051 815 985sec       Max=   0.233 739 585sec
                                                    -m-   -u-   -n-
```

Note that the marker values can also be entered manually.

The packets "marked" by the markers can be viewed on the Packet Delay Display table by clicking on **Data -> Go to … -> Marker #1**.

Graph Zoom features

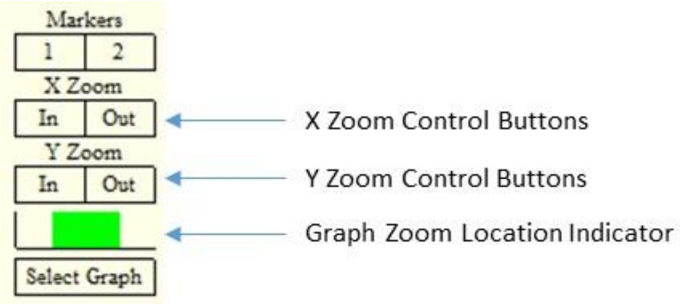
Both the x and y axis can be adjusted using the zoom controls.

X axis;

- Left-click the mouse on a specific point on the graph to zoom in to the area around that point.
  OR
- Left-click and drag the mouse over a specific area of interest.
- Further adjustments can be made using the X Zoom control buttons shown below.
- To provide an indication of the location of the current results being displayed with respect to the overall results set, a Graph Zoom Location Indicator is provided as shown below.
- To return to the original un-zoomed plot right-click the mouse on the graph.

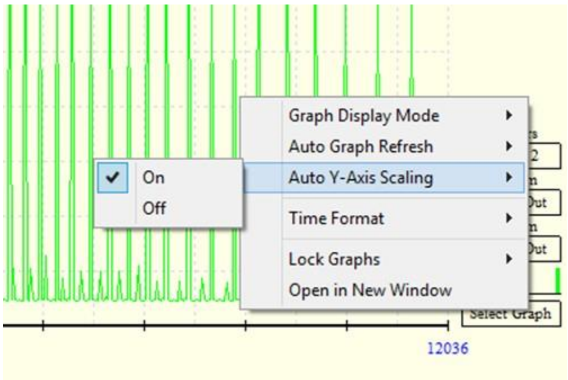
Y axis;

- Use the Y Zoom control buttons shown below.



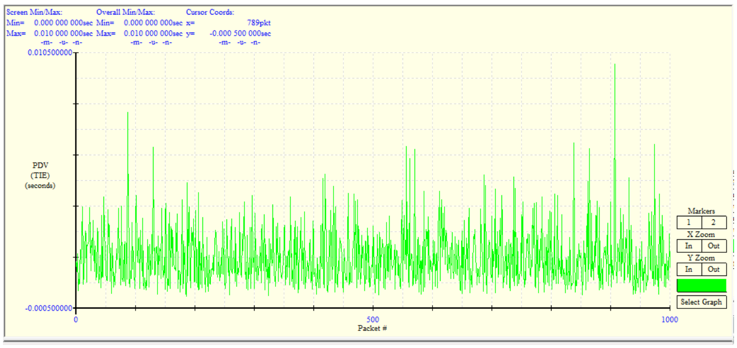
Graph Auto Y-Axis Scaling

This feature is enabled or disabled from the Select Graph control on the graph area. The default condition is Auto Y-Axis Scaling on.



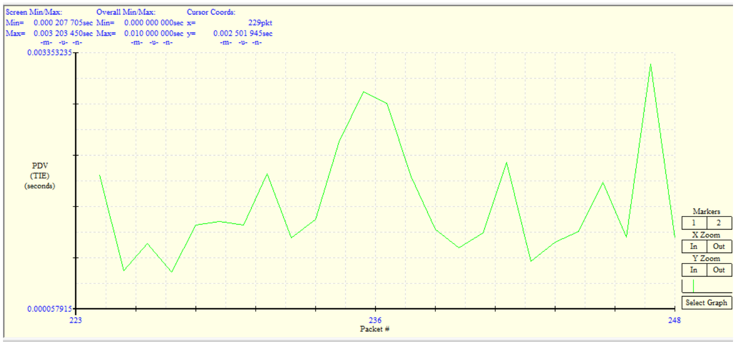
When the function is enabled, as the X-axis of a displayed graph is zoomed, the Y-axis automatically centres and scales to fill the screen.

Example data un-zoomed:



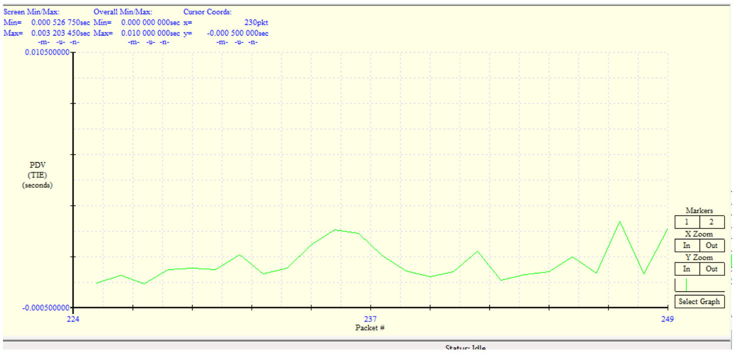
```
Screen Min/Max:            Overall Min/Max:           Cursor Coords:
Min=   0.000 000 000sec Min=   0.000 000 000sec x=              789pkt
Max=   0.010 000 000sec Max=   0.010 000 000sec y=    -0.000 500 000sec
         -m-  -u-  -n-           -m-  -u-  -n-             -m-  -u-  -n-
```

Same data, X-axis zoomed with auto Y-axis scaling turned on



```
Screen Min/Max:            Overall Min/Max:           Cursor Coords:
Min=   0.000 207 705sec Min=   0.000 000 000sec x=              229pkt
Max=   0.003 203 450sec Max=   0.010 000 000sec y=     0.002 501 945sec
         -m-  -u-  -n-           -m-  -u-  -n-             -m-  -u-  -n-
```

Same data, X-axis zoomed with auto Y-axis scaling turned off

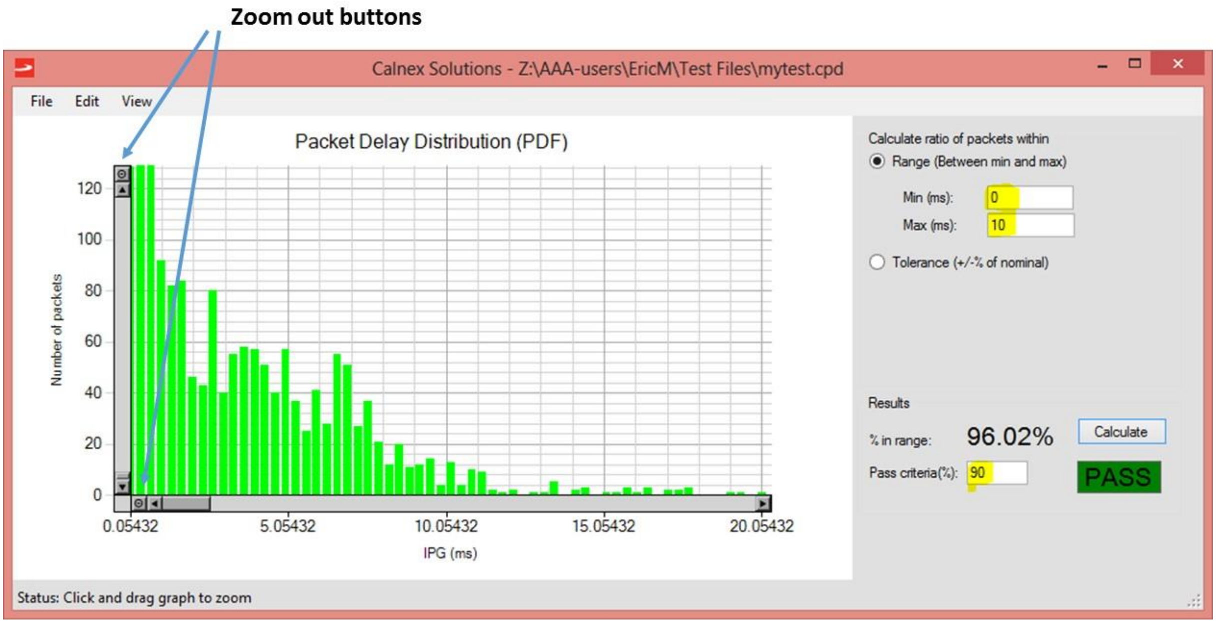


```
Screen Min/Max:            Overall Min/Max:           Cursor Coords:
Min=   0.000 526 750sec Min=   0.000 000 000sec x=              230pkt
Max=   0.003 203 450sec Max=   0.010 000 000sec y=    -0.000 500 000sec
         -m-  -u-  -n-           -m-  -u-  -n-             -m-  -u-  -n-
```

Packet Delay Distribution

This feature allows the analysis of a delay data set from a capture to be analysed and presented graphically as a Probability Density Function (PDF). The data to be analysed must be present in the Paragon-X Network Emulation Application either from a capture or from loading in a previous capture or profile. The data set is sorted into 1000 buckets covering the range of delay values of the data.

This feature is accessed by clicking on **Tools -> Plot PDF/CDF/Histogram** on the menu bar. An example display is shown below.



Zoom out buttons

Calnex Solutions - Z:\AAA-users\EricM\Test Files\mytest.cpd

Calculate ratio of packets within

● Range (Between min and max)

Min (ms): 0

Max (ms): 10

○ Tolerance (+/-% of nominal)

Results

% in range: 96.02%

Pass criteria(%): 90

Status: Click and drag graph to zoom

The graph may be left on the screen and other captures analysed by repeating process. This may be done with the same data or different data following a separate capture or profile load.

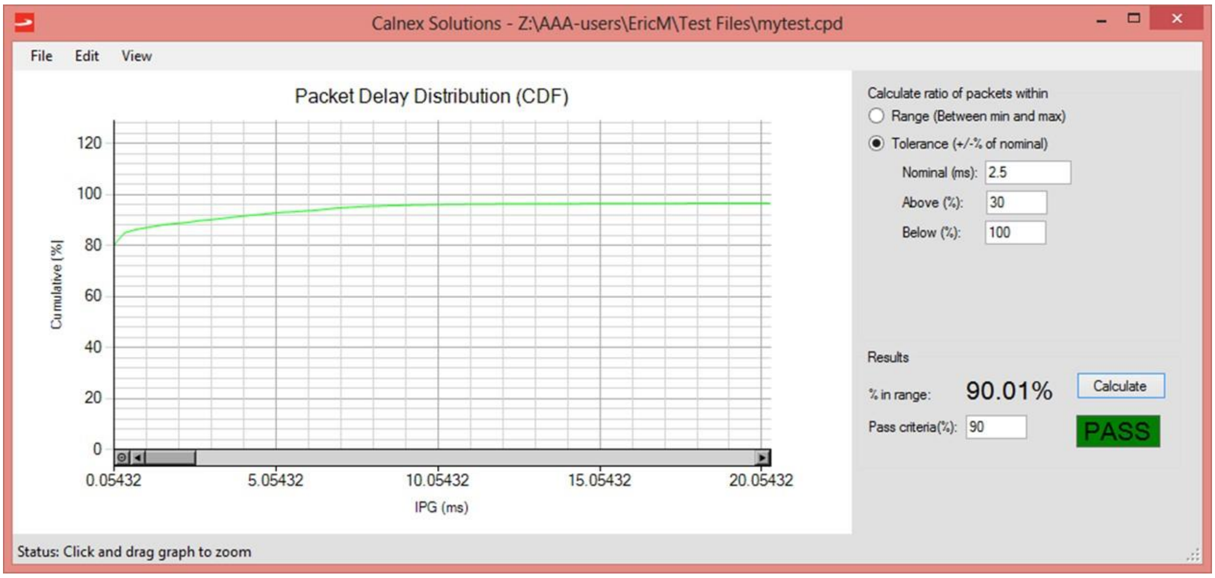
Once a Delay Distribution window is open it may be reused to analyse other data sets directly without having to load the data into the instrument first. On the Delay Distribution window click **File -> Open** then navigate to the results file using the standard Windows Explorer interface.

The graph may be printed using the **File -> Print** selection and the format of the printing may be seen using **File -> Print Preview**. These controls are located in the tool bar of the Delay Distribution window.

Any area of the Delay Distribution window can be zoomed by clicking and dragging the mouse over the specific area of interest. Use the “Zoom Out buttons” shown above to reverse the zoom operation.

By entering range or tolerance values in the fields highlighted in yellow above it is possible to perform a calculation on the data set to determine if the data set values fall within an acceptable range or tolerance. To use this feature enter the required values in the fields highlighted above and click on the Calculate button.

To view the same data in cumulative form (CDF) click on **View -> Cumulative (CDF)**. An example of the resulting display is shown on the next page.


Calnex Solutions - Z:\AAA-users\EricM\Test Files\mytest.cpd
File
Edit
View
Packet Delay Distribution (CDF)
Cumulative [%]
120
100
80
60
40
20
0
0.05432
5.05432
10.05432
15.05432
20.05432
IPG (ms)

Calculate ratio of packets within

○ Range (Between min and max)

● Tolerance (+/-% of nominal)

Nominal (ms): 2.5

Above (%): 30

Below (%): 100

Results

% in range: 90.01%

Calculate

Pass criteria(%): 90

PASS

Status: Click and drag graph to zoom

Appendix 1 - PC Specification and Performance Management

The Calnex Paragon-X product family is configured and monitored using Paragon-X Application software which runs on a user-supplied PC connected to the Paragon-X hardware. The Paragon-X Application software must intensively transfer data during operation, in particular between the Paragon-X hardware and the PC's file structure. Significant processing of data is also required. For the entire Paragon-X system to run with acceptable performance, the PC used must meet or exceed the following specifications.

Minimum - for light use only

Microsoft Windows OS	Win 7, Win 8 and 8.1 (32 and 64 bit)
Microprocessor	1.9 GHz Intel® Core™ Duo processor or equivalent
Microprocessor Cache	Level 2 cache 1MB or equivalent
Memory	1024 MB
Hard Drive	120GB (5400rpm)
Display Resolution	1280 x 800
Network Card	Ethernet 100BaseT

Recommended

Microsoft Windows OS	Win 7, Win 8 and 8.1 (32 and 64 bit)
Microprocessor	2.3 GHz Intel® Core™ 2 Duo processor or equivalent
Microprocessor Cache	Level 2 cache 1MB or equivalent
Memory	2048 MB
Hard Drive	120GB (7200rpm)
Display Resolution	1280 x 1024
Network Card	Ethernet 100BaseT

PC Management – Troubleshooting

The Paragon-X Application software is comparable to video processing software. Many hours of capture at maximum packet rates can result in data volumes of many Gigabytes.

Unlike video processing software, the Paragon-X Application software processes this data in **Real Time**. Consequently, the specification and software maintenance level of your PC will play a large part in the ability of the Paragon-X system to perform to its maximum ability.

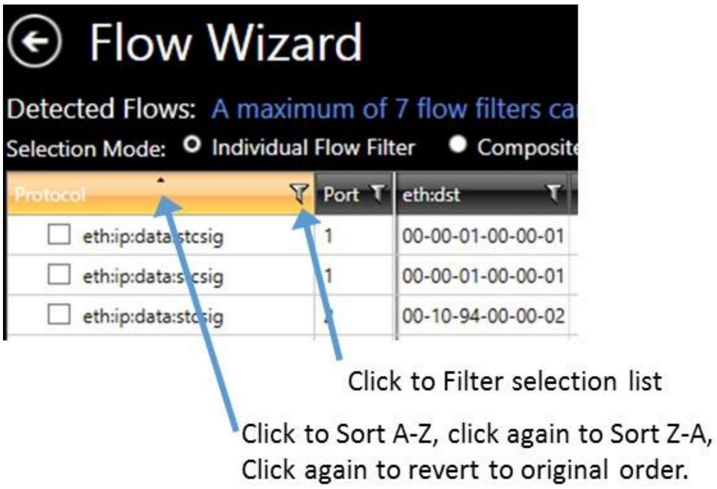
Specifically for **Minimum Specification** PCs, but applying equally to all PCs, if you experience a degradation in performance of your Paragon-X system or are trying to increase your maximum packet capture rate then please refer to the following recommendations.

PC to Paragon-X Ethernet Connection	**Do** directly connect your instrument to your PC using a single Ethernet cable. Additional network elements in the path, such as an office LAN, can degrade data transfer performance. The recommended approach to control over a network is to deploy a local controller directly connected to the Paragon-X hardware, and running the Paragon-X Application. Use a remote desktop arrangement to access the Paragon-X Application over the network.
PC Setup – Multitasking	**Do not** run additional programs on your PC while you are actively using the Paragon-X Application. On Minimum Specification PCs, this will result in increased use of virtual memory eventually leading to all applications apparently stalling or freezing.
PC Setup – Scheduled Tasks	**Do** disable any maintenance tasks your PC may perform during a capture. Performance can quickly degrade and capture data can be lost if your PC decides, for example, to defragment its hard drive, run a virus scan or perform Windows Updates.
PC Setup – Hard Drive	**Do** defragment your hard drive at least once a month. Overnight capture can result in file sizes of many Gigabytes. The PC's file system will perform better if these files are contiguous.
Software Setup – File Management	**Do** ensure that you have sufficient disc space for capturing data. Overnight capture can result in file sizes of many Gigabytes. Adjust the **Resource Management** control to delete unwanted capture files on a regular basis.
PC Setup – Virus Checker	**Do** disable any virus checker software. See *PC Setup – Multitasking*.
PC Setup – Power Management	**Do** disable any **Power Management** or **Power Options** settings. Parameters such as Hibernation, System Standby and Hard Disk timeouts have all been known to occur briefly during Capture. Monitor standby is permitted, although some screensaver programs can be CPU intensive.
PC Setup – Unwanted Services	**Do** disable or remove any third party tools which run in background on your PC such as *iTunes* or *Windows Media Server.* These and other applets can run frequently, monitoring your hard drive or downloading and installing updates.
PC Setup – Firewall	**Do** have your IT department open **TCP port 9990** if you are trying to connect to a Paragon-X local controller across a network firewall.

Appendix 2 – Optimizing Flow Wizard Window Viewing Features

The **Detected Flows** table in Flow Wizard has a "windows rich" feature set which allows the user to optimise the display of pertinent key packet information fields. These features are described below.

Sort and Filter capability.



Flow Wizard

Detected Flows: A maximum of 7 flow filters ca

Selection Mode: ○ Individual Flow Filter ● Composite

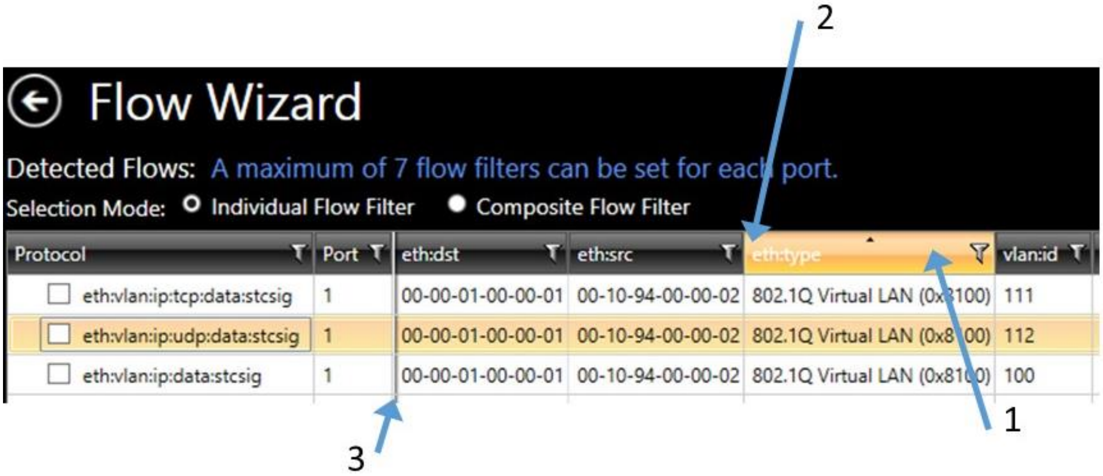
Protocol	Port	eth:dst
□ eth:ip:data:stcsig	1	00-00-01-00-00-01
□ eth:ip:data:stcsig	1	00-00-01-00-00-01
□ eth:ip:data:stcsig	2	00-10-94-00-00-02

Click to Filter selection list

Click to Sort A-Z, click again to Sort Z-A,
Click again to revert to original order.

Column Freeze and Adjustment

The **Detected Flows** table also has adjustable column order, column width and column freeze pane position as shown below.



Flow Wizard

Detected Flows: A maximum of 7 flow filters can be set for each port.

Selection Mode: ○ Individual Flow Filter ● Composite Flow Filter

Protocol	Port	eth:dst	eth:src	eth:type	vlan:id
□ eth:vlan:ip:tcp:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	111
□ eth:vlan:ip:udp:data:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	112
□ eth:vlan:ip:stcsig	1	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	100

1. To change the order of columns; click on the column header as shown highlighted orange and drag to the new position.
2. To change the width of a column; move the mouse over the edge of the column header (arrow 2 above) until the cursor changes to ⟷ then click-and-drag the column border to the correct size.
3. To adjust the Freeze column position; move the mouse over the border of the existing Freeze Column position (arrow 3 above) until the cursor changes to ◄┤├► .
Now click-and-drag the Freeze Column position as required.

Note: These settings are preserved until the Flow Wizard application is closed.

Appendix 3 - Other Features and Functions

This appendix details features and functions not described within the previous chapters of this User Manual.

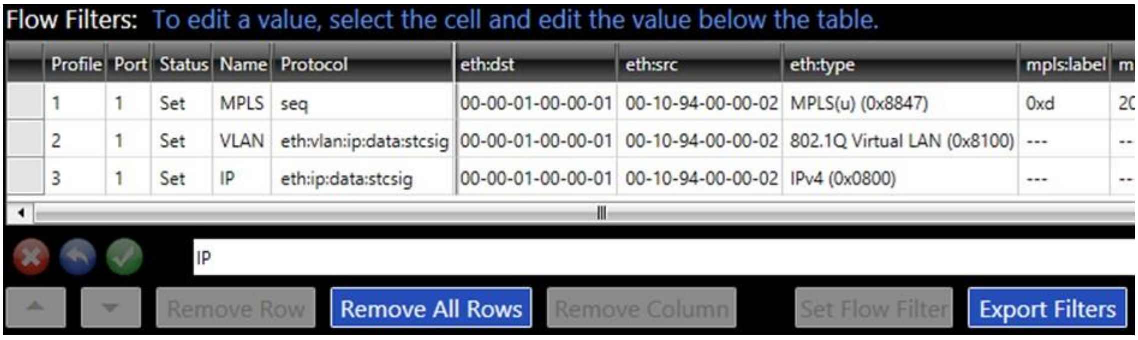
Menu Bar Functions

Menu Bar features and functions that have not been described within the previous chapters of this manual are described here;

- **Instrument -> Instrument Personality;** displays the Network Emulation Options fitted. Only one impairment option can be fitted.
- **Instrument -> Disconnect;** allows a graceful disconnection from the instrument hardware.
- **Instrument -> Details;** displays the revisions of code loaded on the instrument hardware**.**
- **Instrument -> Restart;** allows remote re-boot of the instrument hardware.
- **Setup -> Save/Recall;** allows Line Rate/Interface, Filters and Impairment Profile settings to be saved and recalled for subsequent re-use.
- **Help Menus**
  - **Help -> Contact Support;** provides support email address.
  - **Help -> Remote Control Manual;** launches the Remote Control Manual pdf file.

Importing and Exporting Filters

- To Export Filters use the Export Filters button within Flow Wizard as shown below. Filters are exported as .xml file type.

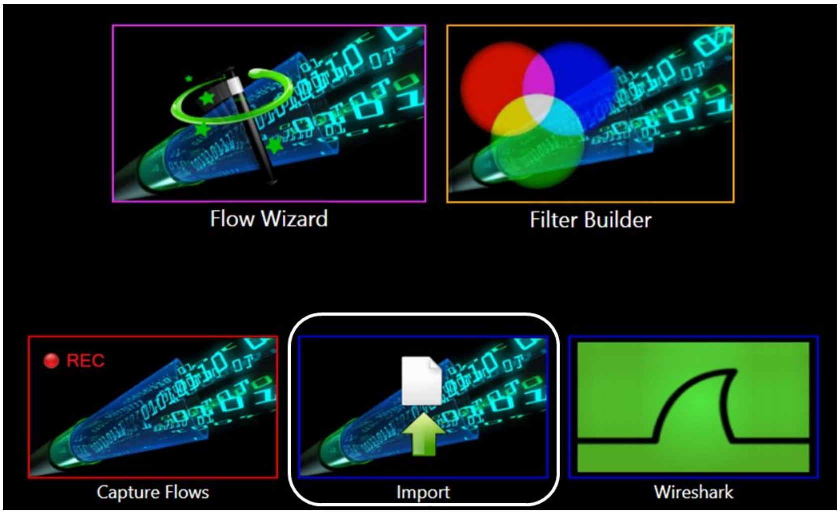


Flow Filters: To edit a value, select the cell and edit the value below the table.

	Profile	Port	Status	Name	Protocol	eth:dst	eth:src	eth:type	mpls:label	m
	1	1	Set	MPLS	seq	00-00-01-00-00-01	00-10-94-00-00-02	MPLS(u) (0x8847)	0xd	2C
	2	1	Set	VLAN	eth:vlan:ip:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	802.1Q Virtual LAN (0x8100)	---	--
	3	1	Set	IP	eth:ip:data:stcsig	00-00-01-00-00-01	00-10-94-00-00-02	IPv4 (0x0800)	---	--

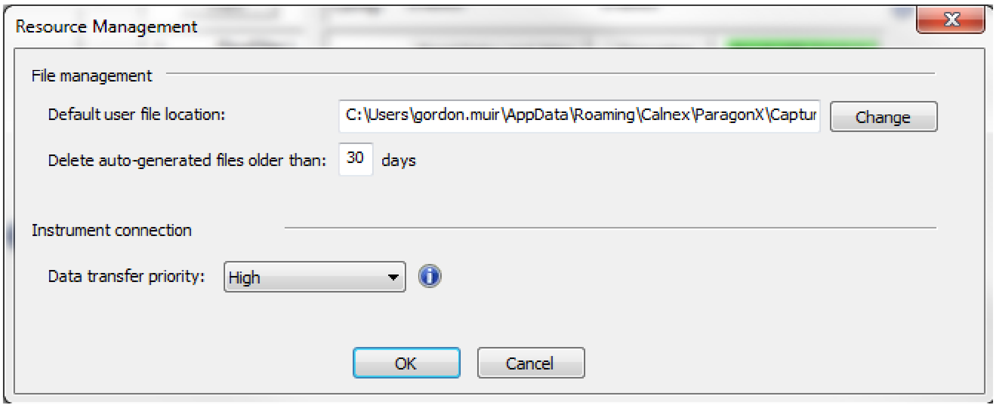
IP

- To Import Filters click on **Select Flows** in the Workflow area, then click on **Import** as shown below. Filters are imported as .xml file type. Filters can also be imported programmatically.



Data and Resource Management

The **default user file location** can be set by the user. This is done by selecting **File -> Resource Management** which brings up the following dialog box.



Resource Management

File management

Default user file location: C:\Users\gordon.muir\AppData\Roaming\Calnex\ParagonX\Captur

Delete auto-generated files older than: 30 days

Instrument connection

Data transfer priority: High

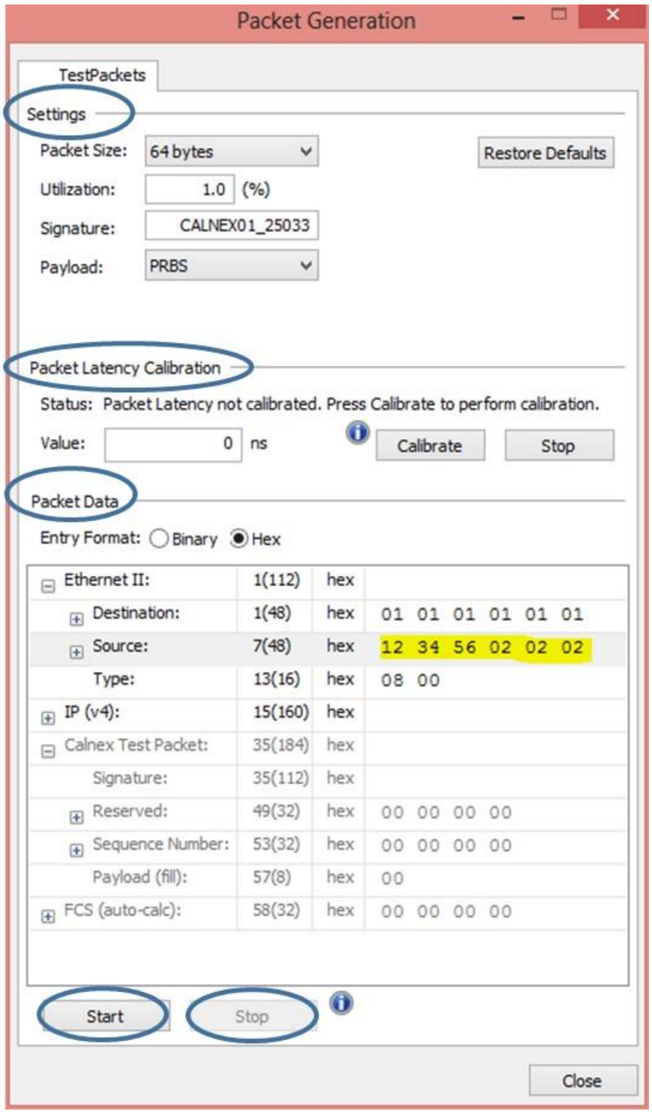
A folder named **Autosave** is held at the Paragon-X default user location. Data derived from any Captures is held here. To manage disk space these files are automatically deleted after a user set period of days.

Note: The normal method of saving Capture Files is using File -> Export from the Menu Bar. The **Autosave** files are held as a temporary back-up to avoid loss of data.

Test Packet Generation

Paragon-X Network Emulation can generate simple Test Packets when set in Tx+Rx Mode. The primary use of these Test Packets is for jitter tolerance testing, but they can also be used to generate simple traffic for device testing. The Test Packets are generated from Port 2 of the instrument on the set Interface. Port 1 can be used to receive the Test Packets.

- Click on the **Setup Interface** button in the Workflow area and set **Tx+Rx Mode**.
- Click **Close** to close the Setup Interface window.
- Now click on the **Packet Generation** button in the Workflow area. The Packet Generation window will be displayed as shown below.



Settings

Packet Size: 64 bytes

Utilization: 1.0 (%)

Signature: CALNEX01_25033

Payload: PRBS

Packet Latency Calibration

Status: Packet Latency not calibrated. Press Calibrate to perform calibration.

Value: 0 ns

Packet Data

Entry Format: ○ Binary ● Hex

⊟ Ethernet II:	1(112)	hex	
⊞ Destination:	1(48)	hex	01 01 01 01 01 01
⊞ Source:	7(48)	hex	12 34 56 02 02 02
Type:	13(16)	hex	08 00
⊞ IP (v4):	15(160)	hex	
⊟ Calnex Test Packet:	35(184)	hex	
Signature:	35(112)	hex	
⊞ Reserved:	49(32)	hex	00 00 00 00
⊞ Sequence Number:	53(32)	hex	00 00 00 00
Payload (fill):	57(8)	hex	00
⊞ FCS (auto-calc):	58(32)	hex	00 00 00 00

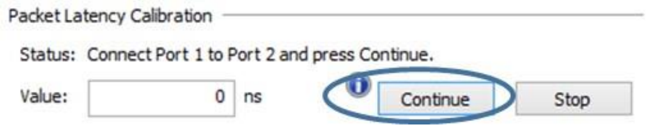
The Packet Generation window is split into 3 areas as shown encircled above; Settings, Packet Latency Calibration and Packet Data.

- In the **Settings** area; set the Packet Size, Utilization and the Payload type as required. A Calnex Signature identifying the source of the test packets is always included within the packet structure.

- In the **Packet Data** area; edit the packet byte values as required – example shown highlighted in yellow colour on the previous page.
  Note: Byte values shown in grey are not editable.
- The **Restore Defaults** button can be used to restore Settings and Packet Data to default values.

If packet latency tests are being made, perform a calibration to eliminate the Paragon-X and cabling latency from the latency results.

- In the **Packet Latency Calibration** area (encircled in the graphic on the previous page) click on the Calibrate button.
- Now connect Port 1 to Port 2 on the appropriate interface and click on the **Continue** button as shown encircled below.

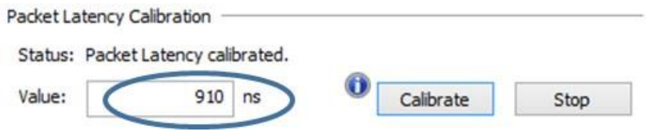


Packet Latency Calibration

Status: Connect Port 1 to Port 2 and press Continue.

Value: 0 ns

The calibration will now proceed. When complete the “intrinsic latency” value will be displayed – example shown encircled below.



Packet Latency Calibration

Status: Packet Latency calibrated.

Value: 910 ns

- Click on the **Start** button to start generating the test packets.
  The **Start** button is shown encircled in the graphic on the previous page.

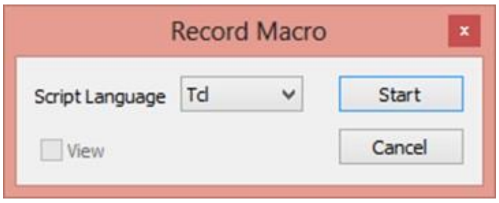
Test Packet counts and latency results can be viewed on the **TestPackets** tab of the Statistics and Results page. Access these results by clicking on the **Statistics and Results** button in the Workflow area. More details are provided in Chapter 6– Statistics and Results on page 60.

- Stop the Test Packet generation when required by clicking on the **Stop** button.
  The **Stop** button is shown encircled in the graphic on the previous page.

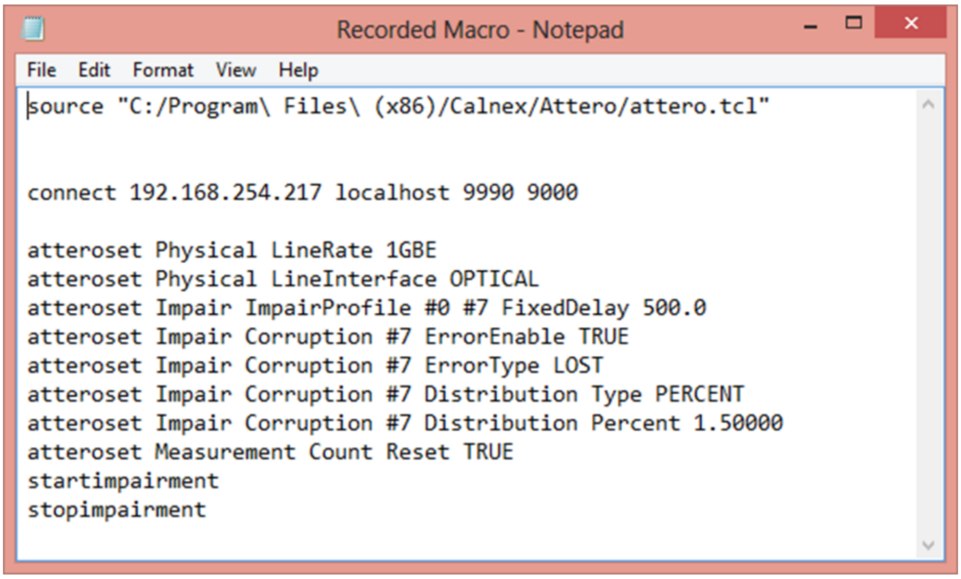
Script Recorder

Scripts can be generated automatically using the Script Recorder features available under the **Tools** Menu. There are two features; **Script Recorder** and **View Recorded Script**. Use Script Recorder to configure settings and start recording, then use View Recorded Script to see the resultant script.

- Click on **Tools->Script Recorder…**



- Select the **Script Language** from the Drop-List. Choose from **Tcl**, **Pearl** or **Python**.
- Press **Start** to start recording key presses from the Application.
- Use the Graphical User Interface of the Application to sequence through the steps in your impairment set up. The Script Recorder will append each step to the script.
- When complete click on **Tools->View Script** to see the resultant script. Example shown below.



```
source "C:/Program\ Files\ (x86)/Calnex/Attero/attero.tcl"


connect 192.168.254.217 localhost 9990 9000

atteroset Physical LineRate 1GBE
atteroset Physical LineInterface OPTICAL
atteroset Impair ImpairProfile #0 #7 FixedDelay 500.0
atteroset Impair Corruption #7 ErrorEnable TRUE
atteroset Impair Corruption #7 ErrorType LOST
atteroset Impair Corruption #7 Distribution Type PERCENT
atteroset Impair Corruption #7 Distribution Percent 1.50000
atteroset Measurement Count Reset TRUE
startimpairment
stopimpairment
```

- Adjust the script as necessary. Consult the **Remote Control Reference Manual** located under the **Help** Menu for more information on specific commands.

Editing a Jitter Distribution Profile

The Paragon-X Network Emulation’s Jitter and Variable Jitter functions can generate Jitter distribution profiles – for example a profile of 1024 points of Gaussian distribution. These profiles can be exported, edited to suit custom needs and re-imported. See section **Adding Jitter to an Impairment Profile** on page 40 for details on how to generate and export a Jitter profile as a .csv file.

The generated .csv file has the following format;

```
Paragon Capture,
File ID: 252184584,
File Version: V1,
Services Timestamp Data,
Inter-packet Timestamp (5ns clocks),
Start: 2014/01/18 13:36:17,
Instrument Name: Paragon-X       ,
Serial Number: 1000000,
Operating Mode: 2,
Capture Mode: 4,
Operating Mode Hdr Size: 28,
Data Record Size: 17,
Data Format: CAPTURE,
Services Settings,
Extra Byte Count: 8,
Extra Byte Offset Values: 0,0,0,0,0,0,0,0,
Relative Mode: 0,
Sequence Number Enabled: 0,
Sequence Number Byte 1 Offset: 0,
Sequence Number Byte Count: 1,
Sequence Number Start Offset: 0,
DATA START,
Timestamp, Byte1, Byte2, Byte3, Byte4, Byte5, Byte6, Byte7, Byte8, Flags,
0,0,0,0,0,0,0,0,0,0,
15450,0,0,0,0,0,0,0,0,0,
6452,0,0,0,0,0,0,0,0,0,
6776,0,0,0,0,0,0,0,0,0,
7044,0,0,0,0,0,0,0,0,0,
6195,0,0,0,0,0,0,0,0,0,
8496,0,0,0,0,0,0,0,0,0,
7036,0,0,0,0,0,0,0,0,0,
8392,0,0,0,0,0,0,0,0,0,
10329,0,0,0,0,0,0,0,0,0,
…..
DATA END,
```

The **Timestamp** values shown in **bold** above between **DATA START** and **DATA END** represent the delay at each jitter point. These values can be edited to create a custom profile. Each Timestamp value represents the number of 5ns clock cycles required to create the delay time. For example in the first jitter point above; 15450 * 5ns equals a delay of 77.