XENA™

Test. Improve. Repeat.

ValkyrieManager (val-94)

A STEP-BY-STEP GUIDE**

Content

VALKYRIE™

MANAGER

XENA™
NETWORKS

CONTENTS

Add Chassis

Click "Add Chassis" button.

Add Chassis

For the **Chassis Address** enter the IP address of the Management port:

The default port number is 22606
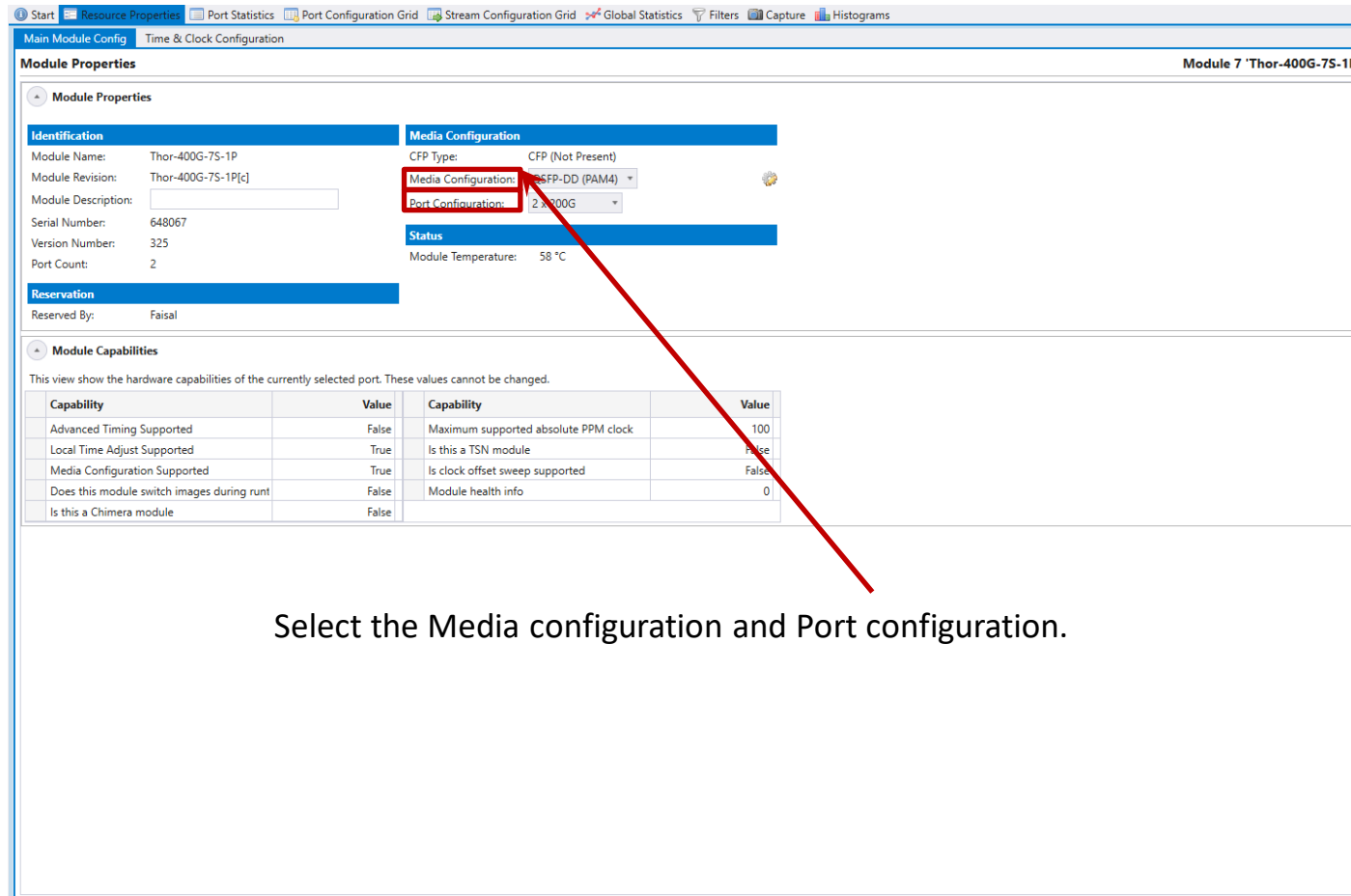The default **Chassis Password** is "xena"

Add Chassis

Use **Options > Set Username** to indicate who owns the port reservation:
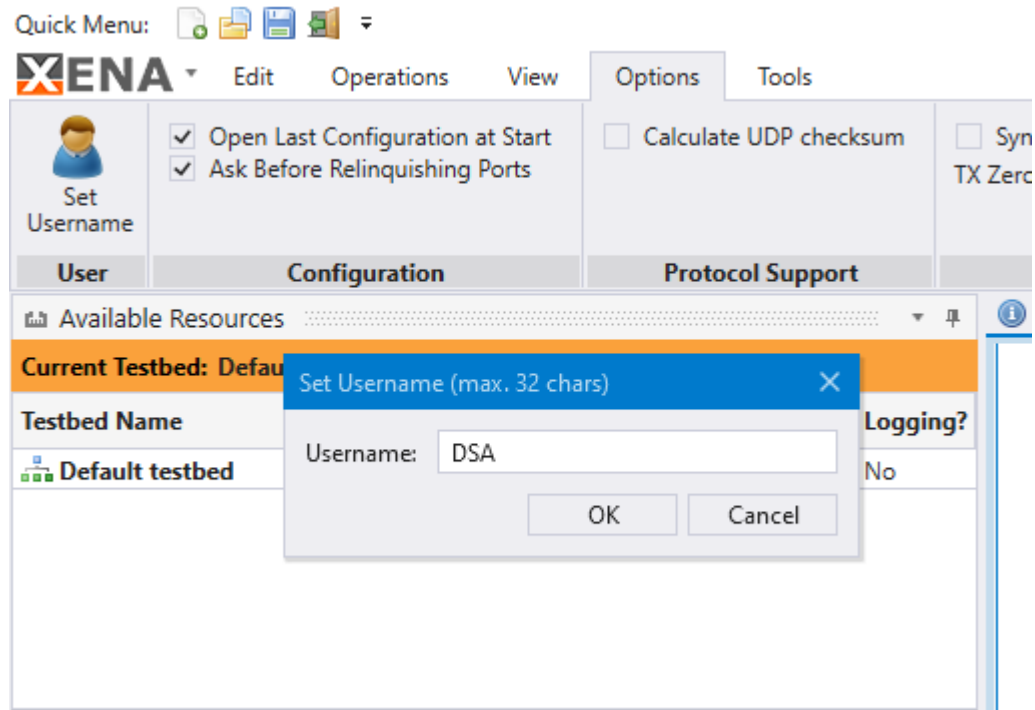
Configure Module

Select the Media configuration and Port configuration.

Time & Clock Configuration

Configure the required clock configuration from this screen.

This section is available only on selected modules

Add Port(s)

1 Select the Port/s you want to use:
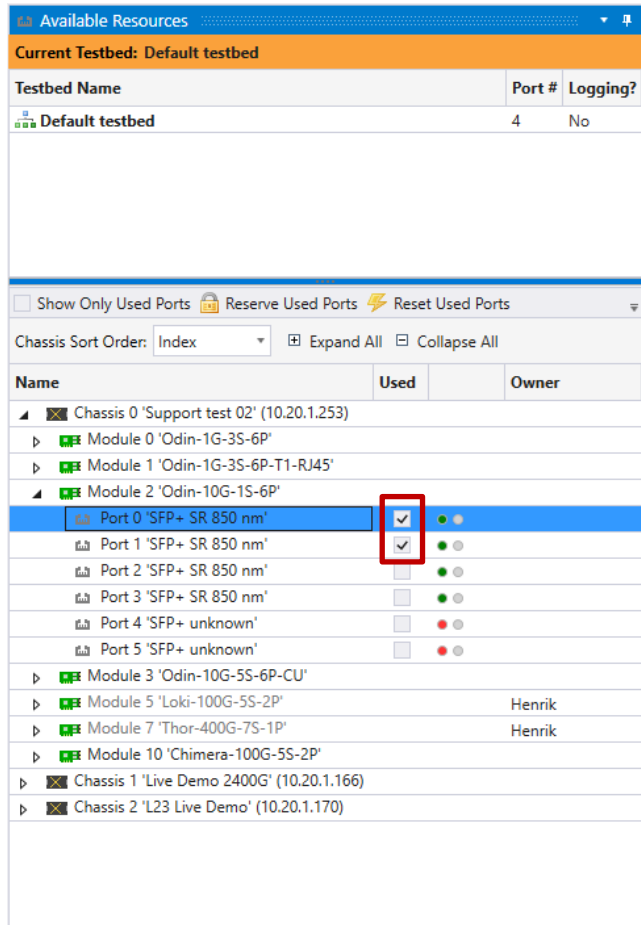
2 - Click "Reserve Used Ports"
- Check "Show Only Used Ports"
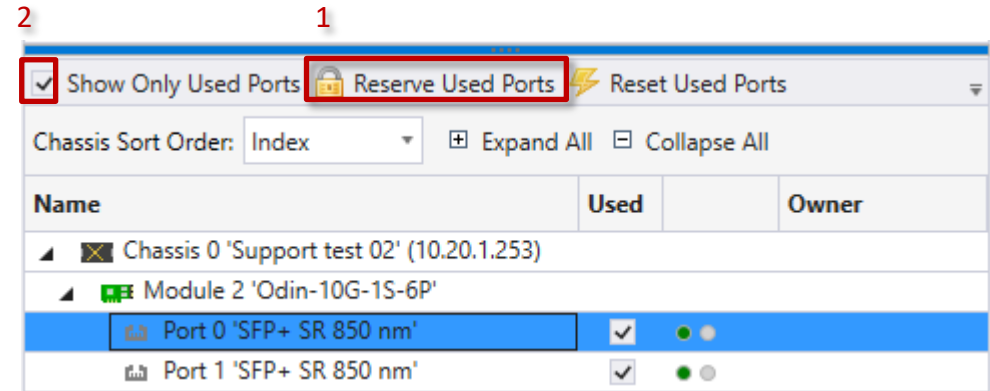
TIP: Right-clicking on ports, modules or chassis will provide additional options e.g.:

CONTENTS
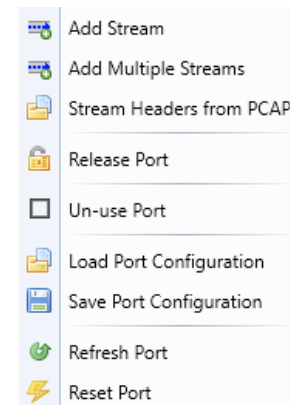
Configure Port(s)

Select the port(s) to configure and click "Resource Properties" tab:

CONTENTS

Configure Port(s)

Configure the following port parameters to accommodate your test.

Configure Port(s)

1 **Minimum IFG**
- Set to 20 -> 12B (Minimum allowed by Ethernet at 100% load) +8B Preamble
-   can be set to 16B to achieve >100% load for port pressure testing
* Values range between 16B-20B depending on module.

2 **Mac Address**
- Used as default SRC.MAC for each stream
- Used when sending Ping or replying to ARP

3 **Mac training**
- Used to train Devices with Xena MAC so stream won`t be flooded

4 **React to pause frames**
- This means enable **Flow Control** on this port

XENA™
N E T W O R K S

Configure Port(s)

5 **Gap Monitor**
- Used to monitor(time) the disruptions of service to traffic
- Gap Monitor start - After how many uSec would the Monitor start
- Gap Monitor stop – After how many packets would Monitor stop
- Results can be seen in port statistics (type of GAP can only be set)

6 **Payload checksum, start at:**
- Used to enter a Headers + Payload Data Integrity Checksum
- Should start from offset 14 for pure L2 packets
- Should start after IP offset for L3 and beyond packets
(because of TTL)

7 **Max. stream header length**
- When user wants to set headers larger than 128
- Number of streams will be downsized to 1/2

Configure Port(s)

Loopback Mode: Off ▼

Off
L1 RX-to-TX
L2 RX-to-TX
L3 RX-to-TX
TX(on)-to-RX
TX(off)-to-RX
Port-to-Port
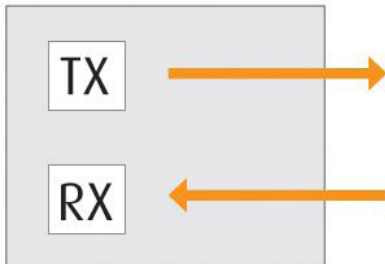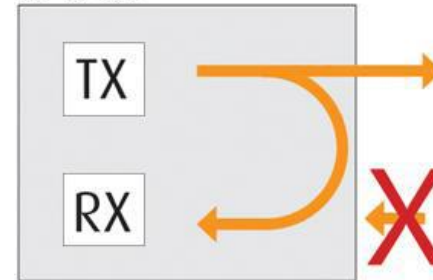
8 **Loopback mode**
- Off: Traffic flows naturally out of the port
- L1 RX-to-TX: Any received packet is bounced back through TX
- L2 RX-to-TX: Same as 8.2 yet it also swaps MAC SRC<>DST
- L3 RX-to-TX: Same as 8.3 yet it also swaps IP SRC<>DST
- TX(on)-to-RX: Packet goes out of TX but also internally direct to RX
- TX(off)-to-RX: Packet goes directly to RX (No link sync needed)
- Port-to-port: Any received packet goes out through the neighbor port
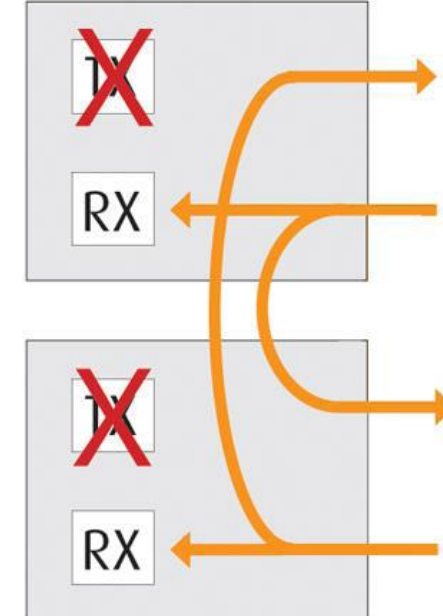
Configure Port(s)

9   **Latency offset**
- Used to automatically eliminate transceiver + cable latency
- Set either manually or via Port Statistics "calibrate" button

🔧 Calibrate Latency
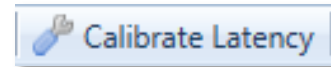
Configure Port(s)

1 **Test port IPv4**
- Address/Subnet/Gateway used for PING and ARP functionality

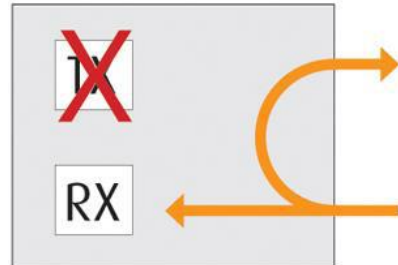**2** **Reply to incoming ARP/PING-request**
- Enable port`s ability to reply to incoming requests

3 **ARP and PING address wildcard:**
- Used to enable multi <u>unique</u> ARP/PING requests

This means 1.1.1.**x will be replied** as long as it is part of 1.1.1.1/28 subnet.

Configure Port(s)

Some modules support:

1 **Port Impairment**
- Link Flap: Set Duration, Repeat Period and Repetitions (0=continuous)
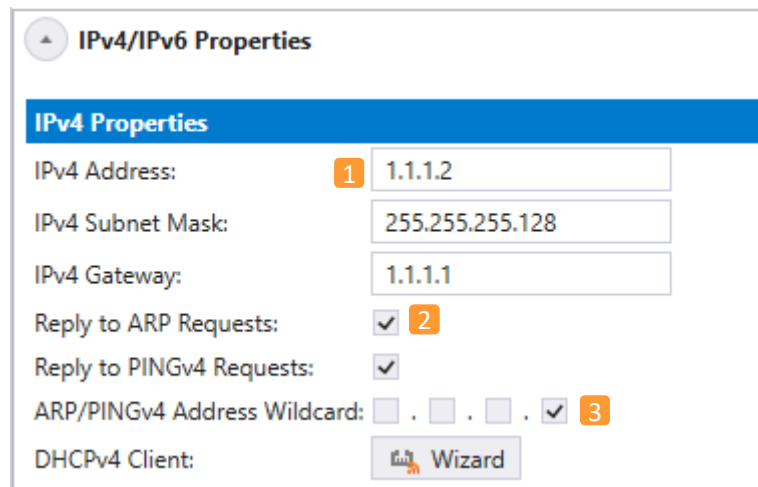- PMA Errors: Set BER coeff and BER exp for the error insertion

2 **Payload Mode**
- Extended Payload
- Custom Data Field
See application note
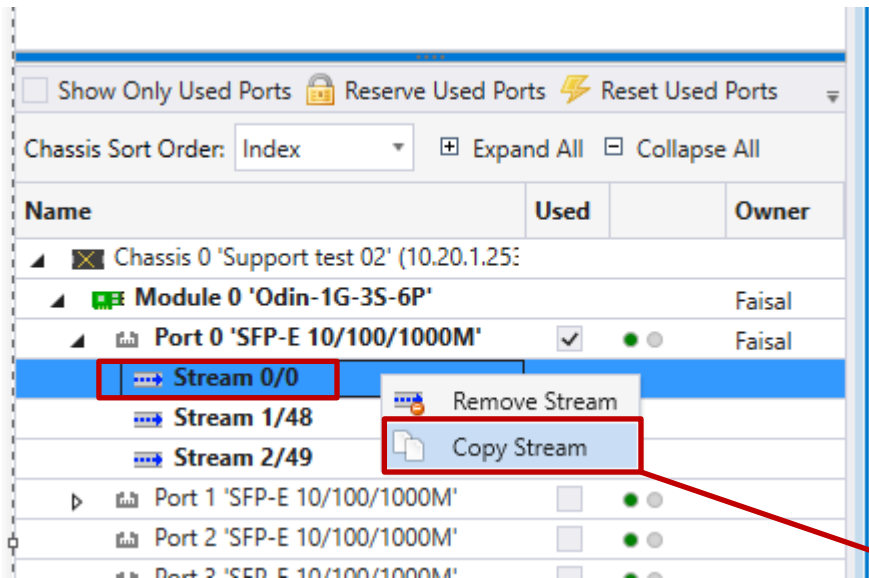*Freely Programmable Test Packets (Custom Data Fields)* for details

Configure Stream(s)

To add a stream, click "**Add Stream**" under Edit Menu
Or right-click port and choose "**Add Stream**" , to add multiple streams select the add multiple streams option

Copy Stream

Copy Stream feature can also be used when user right clicks on any stream and then select copy stream and paste it anywhere.

Configure Stream(s)

Configure Stream(s)

1 **Insert test payload, TID:** This is the stream ID used to identify Latency/Jitter/Packet Loss.

2 **Description**: Stream Description text
(e.g. "Upstream connected to DUT Port 11")

3 **Stream State**

State
Enabled ▾
Disabled
Enabled
Suppressed

Disabled: Stream is not started when traffic is ON nor is it included in port rate usage.

Suppressed: Stream is not started when traffic is ON, but it is included in port rate usage. ("Paused State") can be switched to enabled on the fly.

Enabled: Stream is started when traffic is ON.

4 **Stop After:** Send specific number of packets and stop traffic.
Also used in sequential mode as stream packet quantity.

XENA™
NETWORKS

Configure Multiple Stream(S)

Multiple streams can be configured from Stream configuration Grid

Configure Stream(s)

The grid layout allows scaling configuration.

Select either to view streams under:
      All Port(s)
      Selected Port(s)
      Selected Stream(s)

CONTENTS

Configure Stream(s)

1 Stream transmission profile:

Percent is L1 rate including IFG + Preamble.
Configuring on field actually changes all the others accordingly.
Grayed text can be edited. To have it set you need one more click.

2 Burst used to configure bursty traffic.

Density sets the inner IFG inside the burst
There is a trade-off between the stream
rate and the Burst rate.

3 Error injection: Can send specific errors on the fly – but only when traffic is ON.

4 Insert frame checksum, FCS: Un-checking this checkbox will cause error frames.

CONTENTS

Configure Stream(s)

5 **Packet length:**

Fixed – for min value =x all packets will be x

Incrementing – for min value =100 and max value=200
  100,101,102,103,…,197,198,199,200,100,101,102

Butterfly – for min=100 max=200
  100,200,**101,**199,**102,**198,**103,**197,**104,**196,**105,…**

Random – random values between min. and max.

Mix sends internet mixture of packet sizes:
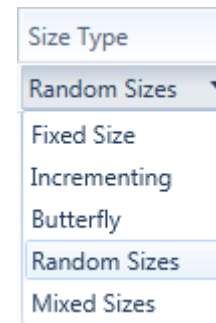
For some modules 4 packet sizes are programmable. If not supported the programming boxes are dimmed
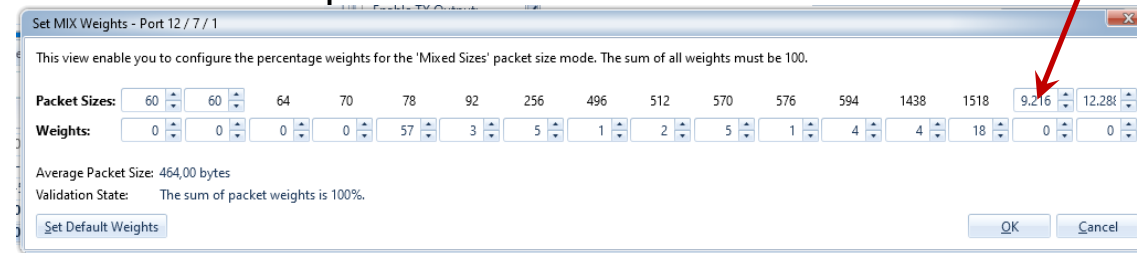
*MIX Weights sets can be loaded\saved via the port resource properties

Configure Stream(s)

6 **Payload Type:**

Incrementing means "000102030405…FF00010203…" provides built-in data integrity check for payload.

PRBS provides Pseudo Random Bit Sequence of 2^31-1 pattern
No data integrity with adding Payload checksum in port properties.

Random provides Random bit Sequence pattern
No data integrity with adding Payload checksum in port properties.

Pattern mean you can set your own custom pattern:

Configure Stream(s)

Create Stream based on PCAP

Pcap Import:

Configure Stream(s)

How To Create Flows

To create multiple flows per stream, place the modifier on important headers.
e.g. to create 1 Stream with 1000 VLAN flows with values between 1000-2000

1 "Add Segment"

2 Choose VLAN

3 Click "OK"
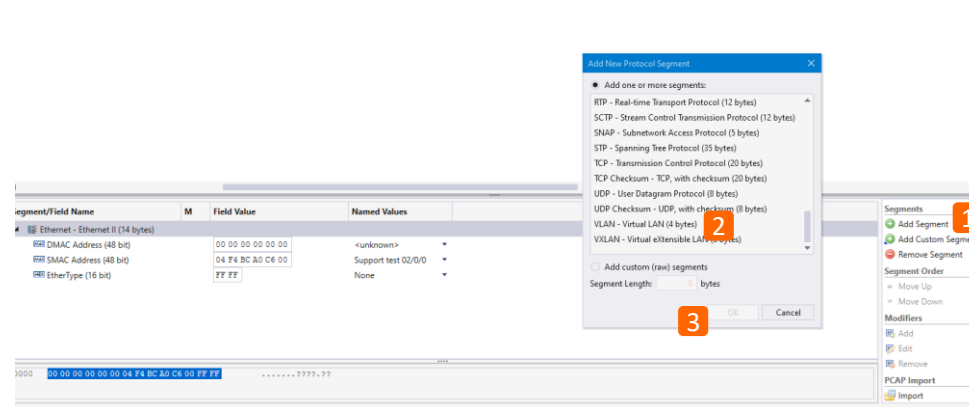
4 Right-click VLAN tag and "Add modifier"
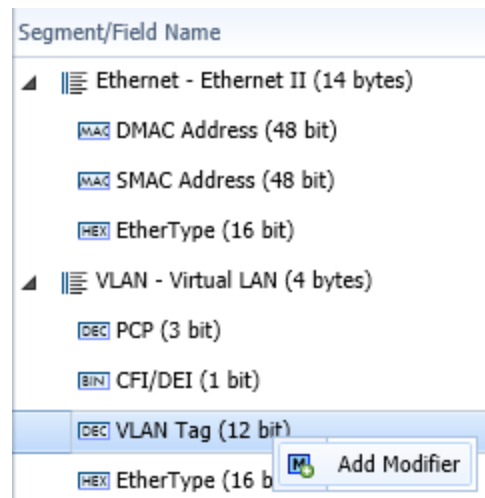
4 Configure as follows:
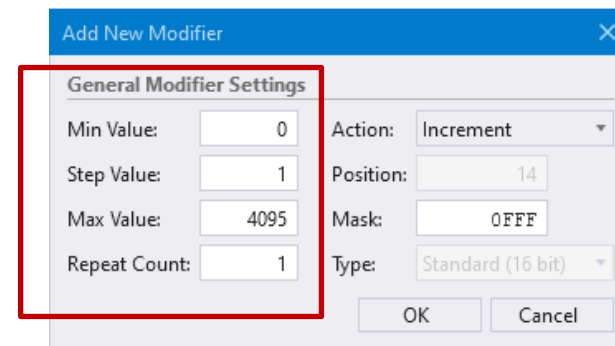
Configure Stream(s)

Setup simple bidirectional traffic.

1 Add 1 stream for each traffic port (right-click -> Add Stream)

2 Select both streams using the Available Resources panel and CTRL+

3 Clicking "Pair Streams" results in …

Configure Stream(s)

Stream Scheduler

The Stream Scheduler can be used to build a series of actions ("operations") based on existing streams in the current testbed.

Before starting the Stream Scheduler, you must reserve ports and configure ports and streams.

Example: 120 times the traffic is running for 5 seconds and then stopped for 5 seconds:

FILTERS

Filters

Filters are used in order to get statistics on specific types of packets either specific content or specific packet size.

These filters can also trigger the Capture mechanism or focus Histogram results.

1 **Add match term** –click to add new match term
(Added to provided Statistics for a matched packet (e.g. Packets of VLAN 100)

2 Click to access the field you want to match (headers must be added manually per match term).

3 **Position** is set to beginning of field e.g. if you want to match last octet of IP, the offset should be incremented manually
Mask – to focus on a specific Byte the other should be set to "00"

4 **Value** – The value you would like to match (the value is in Hex so 50Dec = 32Hex)

5 Length term –used to find specific packet sizes

Filters

6   **Add filter** – click to add/build a new filter based on match terms

7   **Enable** checkbox to enable a filter to be present in the results and capture trigger

8   **Describe** –Name of the filter

Filter Condition – Build a filter based on pre-built terms using the &, |, and ~ operators

* Load/Save Filters settings:

CONTENTS
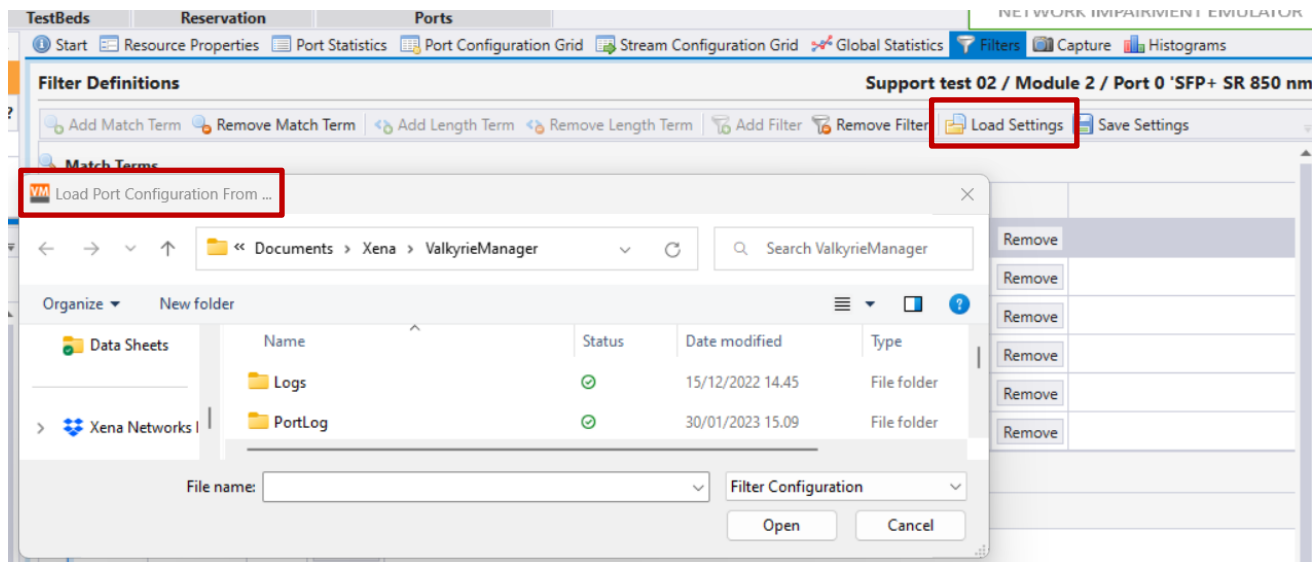
Filters

Configuration Examples

Match Terms

	Match ID	Segment/Field Type	Segment/Field Selector	Position	Filter Mask	Filter Value
	M0	Ethernet - SMAC Address	Select Field	6	FF FF 00 00 00 00	00 01 00 00 00 00
	M1	Ethernet - DMAC Address	Select Field	0	FF FF 00 00 00 00	00 02 00 00 00 00
	M2	VLAN - VLAN Tag	Select Field	14	0F FF 00 00 00 00	00 64 00 00 00 00
	M3	IPv4 - Src IP Addr	Select Field	26	FF FF 00 00 00 00	01 01 00 00 00 00
	M4	IPv4 - Src IP Addr	Select Field	28	FF FF 00 00 00 00	01 0A 00 00 00 00
	M5	TCP - Src Port	Select Field	34	FF FF 00 00 00 00	00 00 00 00 00 00

Length Terms

	Length ID	Length Type	Length	
	L0	At Most ▼	64	Remove
	L1	At Least ▼	1500	Remove

Filters

	Index	Enabled	Description	Filter Condition
	0	☑	SRC IP = 1.1.1.10	M3 & M4
	1	☑	VLAN ID= 100	M2
	2	☑	Runts	L0
	3	☑	Jumbo	L1
	4	☑	Legal Packet Size	~L0 & ~L1
	5	☑	Illegal Packet Size	L0 | L1

CONTENTS

Filters

Results Examples

Filter Results Under
Global Statistics > Port Statistics:

Name	Description	RX (%)	RX (bit/s)	RX (pps)	RX (bytes)	RX (packets)
◢ P-0-10-0	(Aggregated filter counters)	29.585	290,855,140	31,231	8,139,506,404	6,939,422
Filter 0	SRC IP = 1.1.1.10	1.005	9,857,620	1,192	116,137,606	113,177
Filter 1	VLAN ID= 100	0.008	79,160	10	1,078,644	1,041
Filter 2	Runts	0.005	35,730	72	900,469	14,533
Filter 3	Jumbo	8.673	85,749,370	6,115	2,444,688,239	1,397,063
Filter 4	Legal Packet Size	11.214	109,319,420	17,653	3,131,110,945	4,002,011
Filter 5	Illegal Packet Size	8.680	85,813,840	6,189	2,445,590,501	1,411,597

CONTENTS

Capture

1	Start Capture	3	Stop Trigger	5	Test Payload ID	7	Save Packets
2	Start Trigger	4	Packets to Keep	6	Byte to keep	8	Launch Wireshark

CONTENTS

Capture

1 Checkbox enabled means when click Start/Stop in global view, capture mechanism will Start/Stop on this port.

From ON	▼
From ON	
From FCS Error	
From Filter	
From Payload Error	

2 **Start Triggers:**

- From ON – Means Automatically <u>Start</u>
- From FCS error – First FCS error seen triggers Capture <u>Start</u>
- From payload error - First Payload error seen triggers Capture <u>Start</u>
- Filter x – First packet answering Filter condition triggers Capture <u>Start</u>

| Until Full	▼
Until Full	
Until FCS Error	
Until Filter	
Until Payload Error	
Until User Stop	
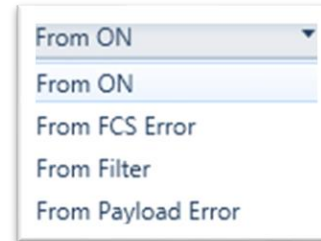
3 **Stop Triggers**:

- Until full – Means Automatically stop when buffer full
- Until FCS error – First(/2nd) FCS error seen triggers <u>Stop</u>
- Until payload error - First(/2nd)Payload error seen triggers <u>Stop</u>
- Filter x – First (/2nd) packet answering Filter condition triggers <u>Stop</u>
- Until User Stop – Capture will keep capturing FILO till manually stopped.

CONTENTS
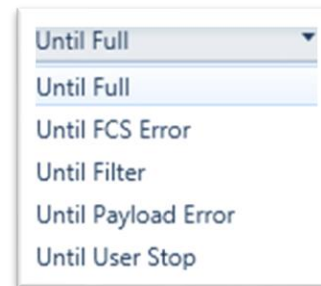
Capture

4   **Which packets to keep** (which will be left in capture buffer):
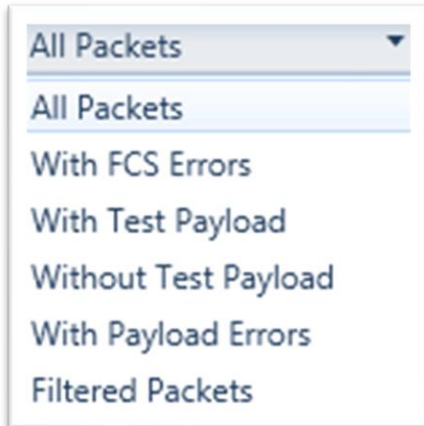
- **All** - All packets are captured

- **With FCS error** – Only FCS error frames

- **With payload error** – Only payload error frames

- **Without test payload** – Only non-stream packets remain

- **With test payload** – keeps only packets that are part of stream x(5) fill in the payload ID

- **Filter x** – keeps only packets answering Filter x conditions

Capture

7   Save capture buffer as PCAP file (tcpdump, wireshark, ethereal…)

8   Open Capture buffer with Wireshark* (or any PCAP associated software)

```
⊞ Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊞ Ethernet II, Src: XenaNetw_0b:16:c2 (04:f4:bc:0b:16:c2), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
⊟ XENA Protocol
    Payload
    Sequence Number: 2
    Time Stamp: 3470317309
    Test Payload ID: 1
    Payload Check Offset: 14
    First Packet Flag: 0
    Payload CRC Enabled: 0
    TPLD Signature: 0x91d9d1d857ff94ce
    Valid: True
```

Tip:

Try downloading the Wireshark plugin to see the TID.

XENA
N E T W O R K S

CONTENTS

Capture

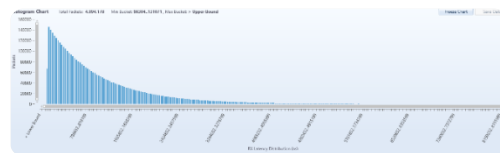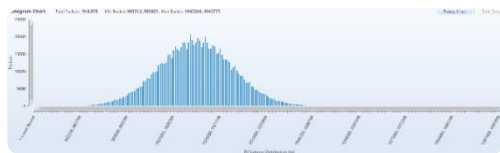**9** Choose the capture buffer visualization method:
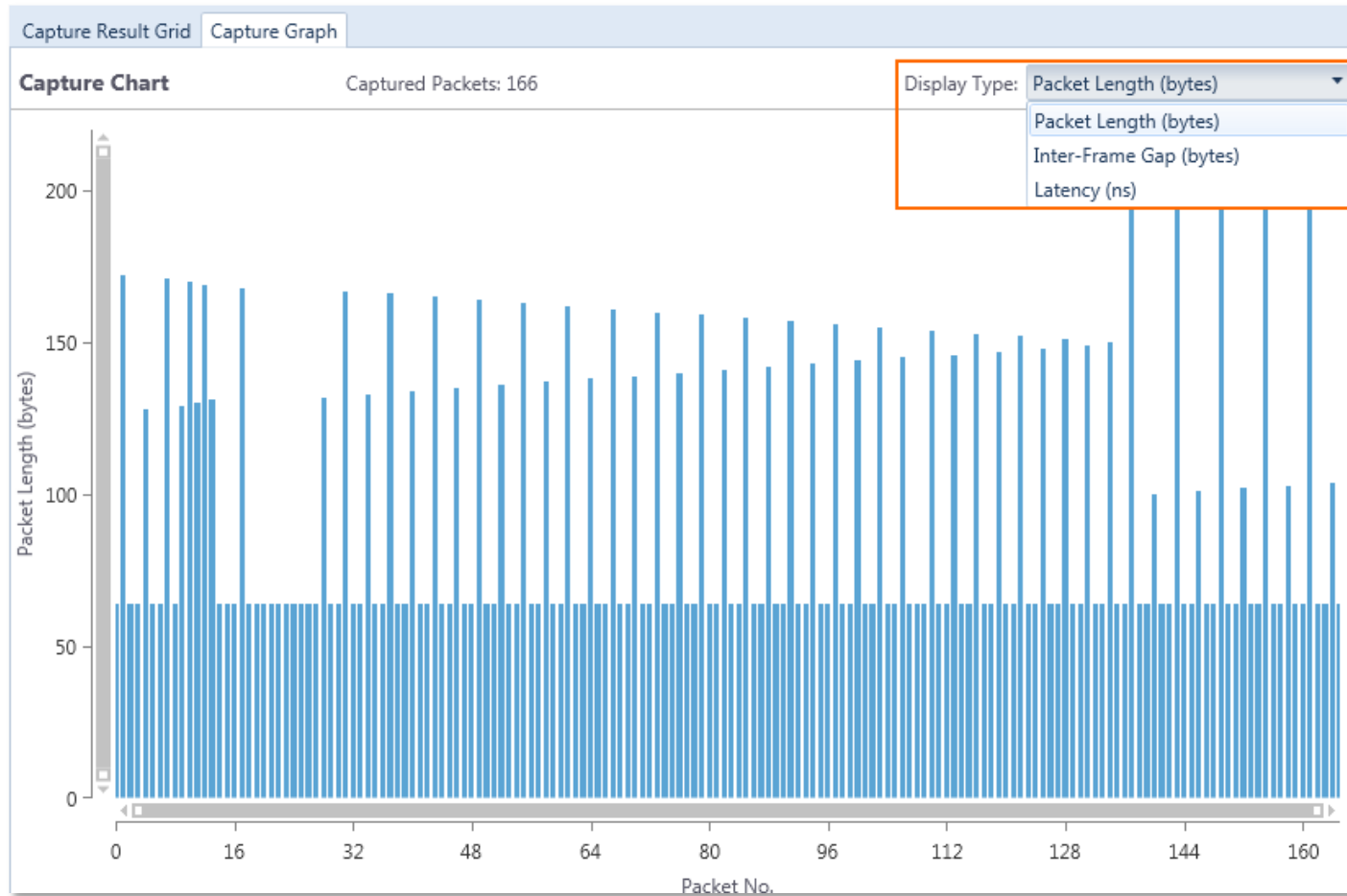
Histograms

Histograms are used to plot different distributions of values gathered over time e.g.
- Tx/Rx Length (Packet size distribution)
- Rx Latency (Latency and Jitter may drift over time)
- Rx Jitter
- Rx IFG (an additional way of observing Jitter behavior)

Each change of configuration will reset the results.

CONTENTS

Histograms

1   **Add histogram** – Multiple histograms can be run simultaneously

2   **Start Histogram** – Start Manually or use checkbox to start from Global

3   Select the type of measurement
you would like to track using the Histogram:

Source Type

TX IFG

- TX IFG
- TX Length
- RX IFG
- RX Length
- RX Latency
- RX Jitter

Which Packets

All

- All
- Test Payload
- Filter

4   Select which packets will be monitored by this Histogram:
… either Specific TID or packets answering a specific filter

Histogram Chart   Total Packets: 760,928   Freeze Chart   Save Data

RX IFG Distribution (bytes)
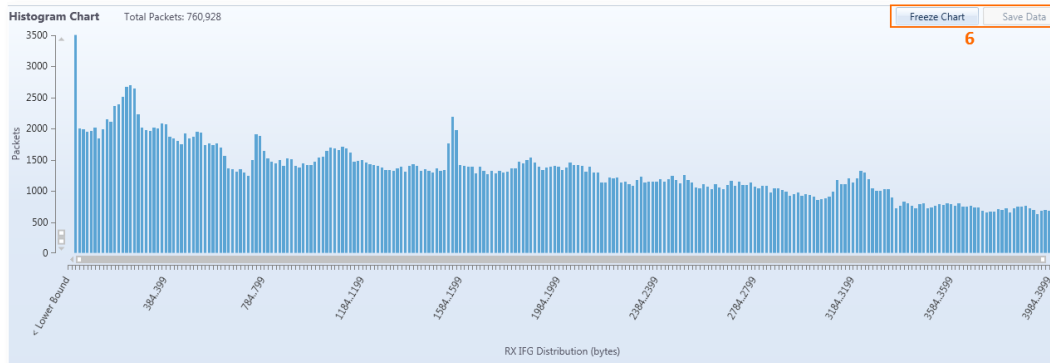
5   **X-axis range** – choose the minimum offset and the resolution (step)

6   Use the **Freeze button** to freeze the view and enable the Save option.

Global Statistics change icons

Ports Statistics

1   **Mark** – freeze constant results and show only changing results

2   **Save** – Save a CSV with all ports results

CONTENTS

Global Statistics

Ports

3   **Port Summary** – SYNC status and error summary

4   **Main Port Traffic Statistics –** included results of TID traffic and non TID traffic:

CONTENTS

Global Statistics

Ports

5 **Traffic without test payload** – non TID traffic

6 **Filters** – Filter results but only 2 for port (the rest are under Statistics)

7 **ARP/PING** control plane results

8 **Frame** Events

9 **Injected errors** statistics

10 **Alarm and Error** statistics
Contents depend on module
and port mode

11 **Miscellaneous** results:
- # sent MAC training packets
- # sent IGMP joins
- Gap count and duration
- # RX Pause frames received
- Flow Control pause frames received
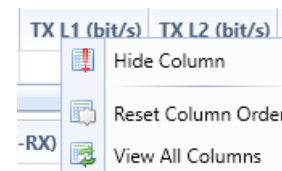
Global Statistics

Streams

12 For each stream instance a separate set of results would be presented.

13 The traffic results (move the right bar to the left to see results that have +eXX)

* Right click on results counter to set counter visibility:

Global Statistics

Streams

14 **Stream Errors:**

(TX –RX) packets gives packet loss results
- Based on simply Tx-Rx (not live results)
- Might fail in case of duplicates

Lost packets – Live results based on
- "Next Expected Sequence Number"
- Might fail for First or Last packet or in case of reordering

Misordered packets – for example expecting Sequence x, y and receiving y,x

Payload errors calculated per packet.
- examined based on Payload checksum or Incremental Payload.

Bit error rate calculated based on number of defected packets vs. correct packets bit count

Packet Loss Ratio calculated as "Lost Packets/(Lost Packets + Rx Packets)"

Stream Errors

Src.Port	SID	TID	Dest.Port	Description	(TX-RX)	Lost Packets	Misordered	Payload Errors	BER (aggr)	BER (curr)	Packet Loss Ratio
Port 12 / 7 / 0	0	1	Port 12 / 7 / 1	Stream number 0	(running)	0	0	0	0,000E+000	0,000E+000	0,000E+000
Port 12 / 7 / 1	0	2	Port 12 / 7 / 0	Stream number 0	(running)	0	0	0	0,000E+000	0,000E+000	0,000E+000

Global Statistics

Streams

15 **16** **Latency/Jitter:**

- Aggr.: Minimum, Average, Maximum – based on overall traffic.
- Curr.: 1-second– based on moving average per second
- Range = Maximum –Minimum

Latency and Jitter

ID				ID	RX Latency (ns)								RX Jitter (ns)						
Src.Port	SID	TID	Dest.Port	Description	AggrMin	AggrAvg	AggrMax	AggrRng	CurrMin	CurrAvg	CurrMax	CurrRng	AggrMin	AggrAvg	AggrMax	AggrRng	CurrMin	CurrAvg	CurrMax
Port 12 / 7 / 0	0	1	Port 12 / 7 / 1	Stream number 0	26	53	90	64	26	53	90	64	0	4	40	40	0	4	32
Port 12 / 7 / 1	0	2	Port 12 / 7 / 0	Stream number 0	26	54	90	64	26	54	90	64	0	4	40	40	0	4	32

CONTENTS

Global Statistics

Logging and Reporting

In order to save results over time and record all results for each second that passes
- Enable Counter Logging.

In order to generate a report of accumulated results
- Enable Generate Report

CONTENTS

Global Statistics

Logging and Reporting

Select the counters you want to record and/or include in the report:

- Please observe that rate counters (e.g., Receive Rate) and Latency and Jitter 1 sec. counters will not be shown in report tables – they may however be included in charts in reports
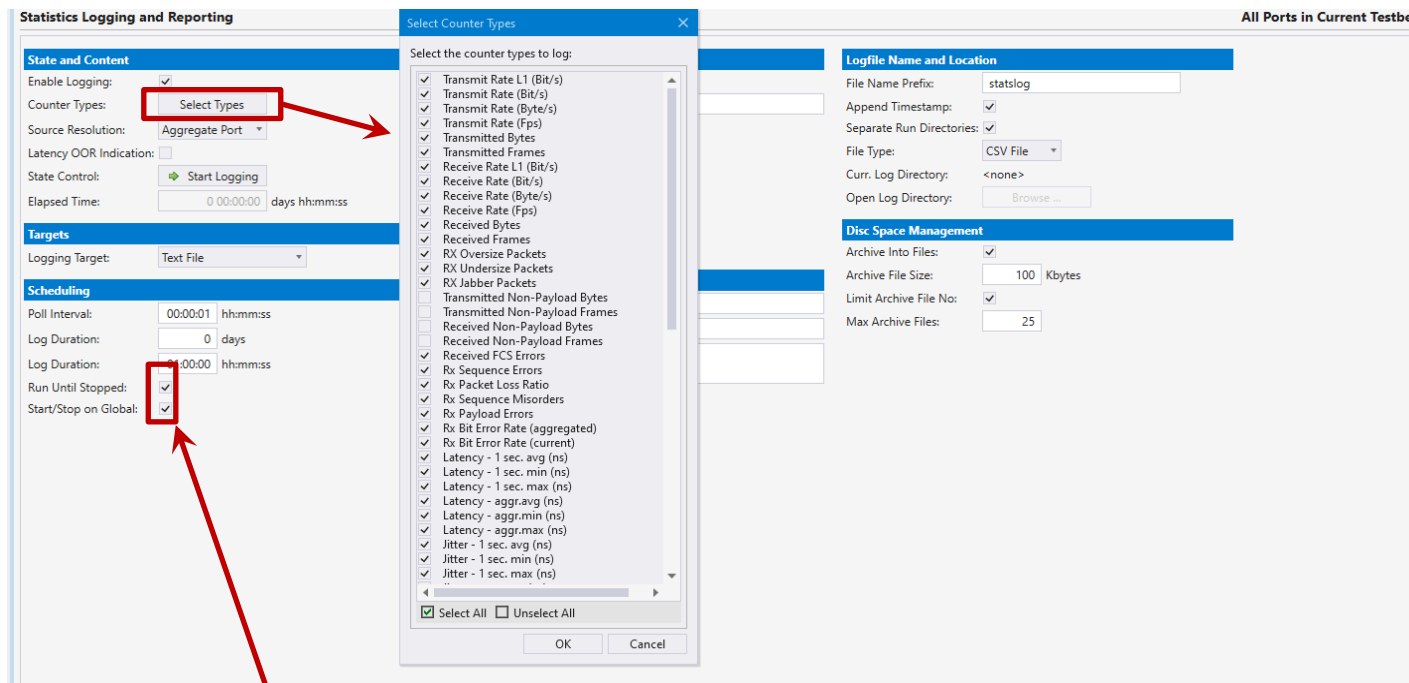
- Check these boxes to start and stop logging and reporting with traffic generation

Global Statistics

Logging and Reporting

1. A text that will be shown in the report
2. Select PDF and/or HTML as file type.
3. Configure PDF pages.
4. Select counters to chart in the report.
5. Click to open directory where the report is stored.

Additional information and a logo for the report

Global Statistics

Logging and Reporting

1. A prefix that will be used for the file name
2. Select file name with or without Timestamp.
3. Select to separate files by Directory.
4. Select CSV or XML as file type.
5. Click to open directory where the log file is stored.

CONTENTS

Global Statistics

Statistics Charting

Event Log

The event log may be used observe:

- Port link issues (Log port Errors).
- Packet Loss (Log Packet Errors).
- Service disruptions (Log Disruptions).

Communication Trace

You can use the Communication Trace to debug communication between the GUI and the Appliance.

Filters can be used to narrow the search for errors or loss of communication.

What's Next?

CHECK TECHNICAL DOCUMENTATION

TRY OUR LIVE DEMO SYSTEM

BOOK A TECH MEETING

SUPPORT