ValkyrieManager (r79)
A STEP-BY-STEP GUIDE
Add Chassis
Add/Configure Port/s
Configure Streams
Filters
Capture
Histograms
Global / Port Statistics
Logging and Reporting
Statistics Charting
Event Log / Communication Trace
Click “Add Chassis” button.

Please select a resource in the treeview to view its properties.
ADD CHASSIS

Enter the IP of the Management port under “Chassis Address:”
Use “xena” as default “Chassis Password”.

![Add Chassis Window](image-url)
Use **Options > Set Username** to indicate who owns the port reservation:
ADD PORT(S)

1. Select the Port/s you want to use:

- Click “Reserve Used Ports”
- Check “Show Only Used Ports”

TIP: Right-clicking on ports, modules or chassis will provide additional options e.g.:
CONFIGURE PORT(S)

Select the port/s to configure and click “Resource Properties” tab:
Configure the following port parameters to accommodate your test.
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

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
**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 Stopper start
- Gap Monitor stop – After how many packets would Stopper 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)

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-TX**: Packet goes directly to RX (No link sync needed)
- **Port-to-port**: Any received packet goes out through the neighbor port
Latency offset
- Used to automatically eliminate transceiver + cable latency
- Set either manually or via Port Statistics “calibrate” button
Test port IPv4
- Address/Subnet/Gateway used for PING and ARP functionality

Reply to incoming ARP/PING-request
- Enable port’s ability to reply to incoming requests

ARP and PING address wildcard:
- Used to enable multi unique 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 STREAM(S)

To add stream click “Add Stream” under Edit Menu
Or right-click port and choose “Add Stream”
CONFIGURE STREAM(S)

The grid layout allows scaling configuration.

Select either to view streams under:

- All Port(s)
- Selected Port(s)
- Selected Stream(s)
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**
   - **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 amount of packets and stop traffic. Also used in sequential mode as stream packet quantity.
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.

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.

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

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

*MIX Weights sets can be loaded/saved via the port resource properties
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:

Select packet header

Select the packet header you want to import:

1) Ethernet / IPv4 / TCP / Raw (112 bytes)

Segment/Field Name | M | Field Value
--- | --- | ---
Ethernet - Ethernet II (14 bytes) | | ...
IPv4 - Internet Protocol v4 (20 bytes) | | ...
TCP - Transmission Control Protocol (2) | | ...
Raw - Data Segment (58 bytes) | | ...

0000 00 15 17 EF 2A 90 90 2B 34 D6 70 BD 08 00 45 00 | | ...
0010 00 62 2F 0A 40 00 40 06 D0 88 C0 A8 5C 75 C0 A8 | | ...
0020 5D 3D 01 BD 07 D1 6B 70 42 6A 57 8A 47 3C 50 18 | | ...
0030 00 3F 6B BC 00 00 00 00 00 36 FF 53 4D 42 75 00 | | ...
0040 00 00 00 88 01 C0 00 00 00 00 00 00 00 00 00 00 | | ...
0050 00 00 01 00 07 00 64 00 09 00 03 FF 00 00 00 01 | | ...
0060 00 0D 00 41 3A 00 4E 00 54 00 46 00 53 00 00 00 | | ...

...?*??+4?p?..E. b/\.@.????\u?? ]=.?.?kpBjW?G<P. ...
...??.?6?SMBu...
...d.......
...?.......
...-........
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”
5. Configure as follows:

![Configure Stream(S) Diagram]
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 ...
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 Diagram](image.png)

**Match Terms**

<table>
<thead>
<tr>
<th>Match ID</th>
<th>Segment/Field Type</th>
<th>Segment/Field Selector</th>
<th>Position</th>
<th>Filter Mask</th>
<th>Filter Value</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>M0</td>
<td>Ethernet - SMAC Address</td>
<td>Select Field</td>
<td>6</td>
<td>FF 00 00 00 00 00</td>
<td>00 00 00 00 00 00</td>
<td></td>
</tr>
<tr>
<td>M1</td>
<td>Ethernet - DMAC Address</td>
<td>Select Field</td>
<td>0</td>
<td>00 00 00 00 00 00</td>
<td>00 00 00 00 00 00</td>
<td></td>
</tr>
<tr>
<td>M2</td>
<td>VLAN - VLAN Tag</td>
<td>Select Field</td>
<td>14</td>
<td>FF 00 00 00 00 00</td>
<td>00 00 00 00 00 00</td>
<td></td>
</tr>
<tr>
<td>M3</td>
<td>IPv4 - Src IP Addr</td>
<td>Select Field</td>
<td>26</td>
<td>FF 00 00 00 00 00</td>
<td>00 00 00 00 00 00</td>
<td></td>
</tr>
<tr>
<td>M4</td>
<td>IPv4 - Dest IP Addr</td>
<td>Select Field</td>
<td>30</td>
<td>FF 00 00 00 00 00</td>
<td>00 00 00 00 00 00</td>
<td></td>
</tr>
<tr>
<td>M5</td>
<td>TCP Checksum - Src Port</td>
<td>Select Field</td>
<td>34</td>
<td>FF 00 00 00 00 00</td>
<td>00 00 00 00 00 00</td>
<td></td>
</tr>
</tbody>
</table>

**Length Terms**

<table>
<thead>
<tr>
<th>Length ID</th>
<th>Length Type</th>
<th>Length</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0</td>
<td>At Most</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>L1</td>
<td>At Least</td>
<td>1500</td>
<td></td>
</tr>
<tr>
<td>L2</td>
<td>At Most</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>L3</td>
<td>At Least</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>L4</td>
<td>At Most</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>L5</td>
<td>At Most</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

**Filters**

<table>
<thead>
<tr>
<th>Index</th>
<th>Enabled</th>
<th>Description</th>
<th>Filter Condition</th>
<th>Filter Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>ILLEGAL PACKET SIZE</td>
<td>L0</td>
<td>L1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>VLAN 100</td>
<td>M2</td>
<td>Remove</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>VLAN 100</td>
<td>-M2</td>
<td>Remove</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>SPECIAL TCP PACKET</td>
<td>M0</td>
<td>M1</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>AT MOST 512B</td>
<td>L2</td>
<td>Remove</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>LEGAL PACKETS</td>
<td>-L0</td>
<td>-L1</td>
</tr>
</tbody>
</table>
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:
# FILTERS

## Configuration Examples

### Match Terms

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

### Length Terms

<table>
<thead>
<tr>
<th>Length ID</th>
<th>Length Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>L0</td>
<td>At Most</td>
<td>64</td>
</tr>
<tr>
<td>L1</td>
<td>At Least</td>
<td>1500</td>
</tr>
</tbody>
</table>

### Filters

<table>
<thead>
<tr>
<th>Index</th>
<th>Enabled</th>
<th>Description</th>
<th>Filter Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>✔️</td>
<td>SRC IP = 1.1.1.10</td>
<td>M3 &amp; M4</td>
</tr>
<tr>
<td>1</td>
<td>✔️</td>
<td>VLAN ID= 100</td>
<td>M2</td>
</tr>
<tr>
<td>2</td>
<td>✔️</td>
<td>Runts</td>
<td>L0</td>
</tr>
<tr>
<td>3</td>
<td>✔️</td>
<td>Jumbo</td>
<td>L1</td>
</tr>
<tr>
<td>4</td>
<td>✔️</td>
<td>Legal Packet Size</td>
<td>~L0 &amp; ~L1</td>
</tr>
<tr>
<td>5</td>
<td>✔️</td>
<td>Illegal Packet Size</td>
<td>L0</td>
</tr>
</tbody>
</table>
FILTERS

Results Examples

Filter Results Under

Global Statistics > Port Statistics:

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

Capture Handling window:
- Start Trigger: From ON
- Stop Trigger: Until Full
- Packets To Keep: All Packets
- How Much To Keep: 0 bytes of each packet
- Test Payload ID (TID): 0

Capture Results: Captured Packets: 166

Segment/Field Name  | Field Value  | Named Values
-------------------|--------------|--------------
| Ethernet - Ethernet II (14 bytes) | | |
| Raw - Data Segment (50 bytes) | | |
CAPTURE

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

2 Start Triggers:

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

3 Stop Triggers:

- Until full – Means Automatically stop when buffer full
- Until FCS error – First(/2nd) FCS error seen triggers Stop
- Until payload error - First(/2nd)Payload error seen triggers Stop
- Filter x – First (/2nd) packet answering Filter condition triggers Stop
- Until User Stop – Capture will keep capturing FILO till manually stopped.
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
7. Save capture buffer as PCAP file (tcpdump, wireshark, ethereal...)

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

TIP:
Try downloading the Wireshark plugin to see the TID.
Choose the capture buffer visualization method:

- Display Type:
  - Packet Length (bytes)
  - Inter-Frame Gap (bytes)
  - Latency (ns)
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 resets the results.
HISTOGRAMS

1. **Add histogram** – Multiple histograms can be ran 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:

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

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

Ports

1. **Mark** – freeze constant results and show only changing results
2. **Save** – Save a CSV with all ports results
3. **Total traffic** - included results of TID traffic and non TID traffic:
GLOBAL STATISTICS

Ports

4  **Without test payload** – non TID traffic
5  **Filters** – Filter results but only 2 for port (the rest are under Statistics)
6  **ARP/PING** control plane results
7  **Injected errors** results (as shown in stream section)
8  **Miscellaneous** results:
   -# sent MAC training packets
   -# sent IGMP joins
   -# FCS errors caught
   -# RX Pause frames
   -Flow Control pause frames
Streams

9. **Mark** – freeze constant results and show only changing results

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

11. 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

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 and receiving x-y

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

<table>
<thead>
<tr>
<th>Stream Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src.Port</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>Port 0/11/0</td>
</tr>
</tbody>
</table>
Streams

Latency/Jitter:
- Minimum, Average, Maximum – based on overall traffic.
- 1-second – based on moving average per second
- Range = Maximum – Minimum

![Global Statistics Image]
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
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 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
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.
GLOBAL STATISTICS
Statistics Charting

Stream Statistics Charts

Add Chart

Transmit Rate (fps) / Rx Sequence Errors (Delta)

Left Axis Legend:
- Stream number 0 (P-0-11-4/S:0)
- Stream number 0 (P-0-11-5/S:0)
- Stream number 1 (P-0-11-4/S:1)
- Stream number 2 (P-0-11-4/S:2)

Right Axis Legend:
- Stream number 0 (P-0-11-4/T:16)
- Stream number 0 (P-0-11-5/T:13)
- Stream number 1 (P-0-11-5/T:14)
- Stream number 2 (P-0-11-5/T:15)
Event Log

The event log may be used to observe:
- Port link issues (Log Port Errors).
- Packet Loss (Log Packet Errors).
- Service disruptions (Log Disruptions).

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Source Type</th>
<th>Source ID</th>
<th>State</th>
<th>Event Type</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014.09.29 14:44:33</td>
<td>Port</td>
<td>P-0-11-0</td>
<td>Raised</td>
<td>Port Error</td>
<td>Port State: NO SYNC</td>
</tr>
<tr>
<td>2014.09.29 14:44:33</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Port Error</td>
<td>Port State: NO SYNC</td>
</tr>
<tr>
<td>2014.09.29 14:44:36</td>
<td>Port</td>
<td>P-0-11-0</td>
<td>Cleared</td>
<td>Port Error</td>
<td>Port State: IN SYNC</td>
</tr>
<tr>
<td>2014.09.29 14:44:37</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Cleared</td>
<td>Port Error</td>
<td>Port State: IN SYNC</td>
</tr>
<tr>
<td>2014.09.29 15:22:57</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Packet Error</td>
<td>Lost Packets: 1547613</td>
</tr>
<tr>
<td>2014.09.29 15:22:58</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Packet Error</td>
<td>Lost Packets: 1549024</td>
</tr>
<tr>
<td>2014.09.29 15:22:58</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Disruption</td>
<td>Disruption: 262143 gaps, 00:01:56.145 secs</td>
</tr>
<tr>
<td>2014.09.29 15:22:58</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Packet Error</td>
<td>Lost Packets: 1549717</td>
</tr>
<tr>
<td>2014.09.29 15:22:59</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Packet Error</td>
<td>Lost Packets: 1551117</td>
</tr>
<tr>
<td>2014.09.29 15:23:00</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Packet Error</td>
<td>Lost Packets: 1553206</td>
</tr>
<tr>
<td>2014.09.29 15:23:06</td>
<td>Port</td>
<td>P-0-11-1</td>
<td>Raised</td>
<td>Packet Error</td>
<td>Lost Packets: 1554609</td>
</tr>
</tbody>
</table>
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.
Want more?

CHECK TECHNICAL DOCUMENTATION

TRY OUR LIVE DEMO SYSTEM

BOOK A GUIDED SW TOUR

CONTACT US:
support@xenanetworks.com