ProfiTap's ProfiShark Performance Results

The Technology Firm

Tony Fortunato
Sr. Network Performance Specialist
www.thetechfirm.com
THE TECHNOLOGY FIRM

TABLE OF CONTENTS

GOAL

Summary

The goal of this document is to introduce the reader to some of the possible limitations Wireshark, or software based packet capture tools may encounter. We will compare the traditional Wireshark capture methods and record how efficient each scenario is.
An important point to make is that we didn't want to run the tests at full line rate since the average protocol analyst will not be using their laptop and Wireshark in those scenarios.

Methodology

We used a NETSCOUT OptiView XG for traffic generation and service level testing. Since the OptiView supports up to 10 Gb, it can easily handle our 1 Gb testing.
Our test computer is an Alienware Intel(R) Core(T M) i7-4910MQ processor (Quad C ore, 8MB Cache) with a 1 Gb Killer e2200 Gigabit Ethernet Adapter running Windows 8.1.
We tested the ProfiShark 1G, USB 3.0 Ethernet adapter, Cisco span port and the laptop built in Ethernet adapter.

Microsoft Windows Notes

All protocol drivers were disabled except for IPv4 and all non-essential services were stopped. IPv4 checksum receive offloading was enabled. The Microsoft Firewall and antivirus server was disabled as well to ensure optimal performance.

Highlights

The ProfiShark 1G provided full line rate capture at various loads and frame sizes while WinPcap had issues keeping up.
Important to note that the dropped packet counter was far from accurate using tshark or the GUI.
Using a TAP or SPAN port in an effort to capture more packets seems to be a myth at best.
An USB Ethernet adapter is not recommended for reliable packet analysis.

"If you use Wireshark, ensure your shark isn't missing teeth."

TESTING SUMMARY

The majority of the tests were conducted back to back with an Ethernet cable and no switch to eliminate any delays, packet loss or other variables a switch may cause.

One of the goals to demonstrate that it doesn't take 1 Gbps of traffic to cause packet loss on WinPcap based systems. Practical frame sizes and loads were selected for the majority of the tests.

Here are the various test scenarios covered in this document:

- OptiView XG to OptiView XG
- OptiView XG to Laptop
- OptiView XG to OptiView XG through a TAP
- OptiView XG to OptiView XG through a TAP with a laptop capturing via Ethernet
- OptiView XG to OptiView XG through the ProfiShark with a laptop capturing via USB
- Two OptiView XG's with a span port to a laptop

The table below summarizes the results from the traffic generation test using Wireshark's GUI, tshark utility and the ProfiShark 1G.

Frame Size	Rate/Second	Utilization	Percent Lost GUI	Percent Lost tshark	Percent Lost ProfiShark 1G
64	553,097	37.2	42%	44%	0%
256	158,490	35	3%	0.24%	0%
512	82,224	35	0%	0.30%	0%
512	117,489	50	11%	0.10%	0%
512	164,058	69.8	11%	5.77%	0%

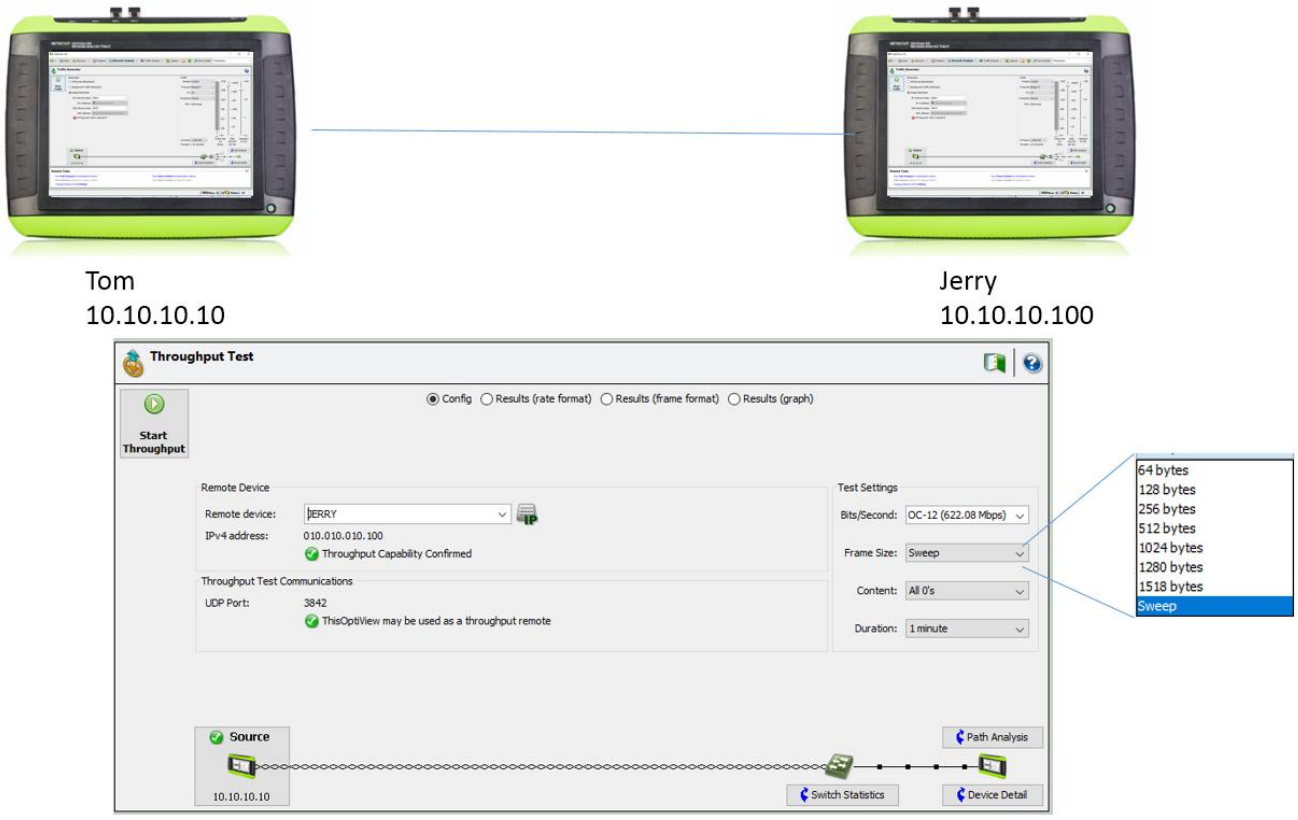
OPTIVIEW XG BACK TO BACK

Setting a Baseline

Two OptiView XG were connected back to back with CAT-6a cables to set a baseline of equipment performance and confirm patch cables meet performance specifications. The OptiView Throughput Test simply generates a traffic stream based on four variables; speed, frame size content and duration.

For our back-to-back test, I chose the following test parameters: Bits/Second 622Mbps, Frame Size Sweep (64, 128,256,512, 1024, 1280 and 1518 Bytes), Content All Zeros, Duration 1 minute per frame size.

The OptiView was tested successfully using the 1 Gb bandwidth setting five times. 622 Mbps was then selected as average of a typical 1 Gb link seen within corporate environments.



Results

There was no packet loss reported between the OptiView's across all frame sizes. The test was repeated five times to confirm our results.

The table below was created using our standard testing methodology:

- five tests were recorded
- the worst and best values were discarded
- the remaining three values were averaged

Frame Size	Frames Generated	Percent Received
64	55,556,209	100%
128	31,529,553	100%
256	16,906,358	100%
512	8,770,100	100%
1024	4,468,994	100%
1280	3,589,016	100%
1518	3,033,635	100%

OPTIVIEW XG TO LAPTOP - GUI

Wireshark - GUI

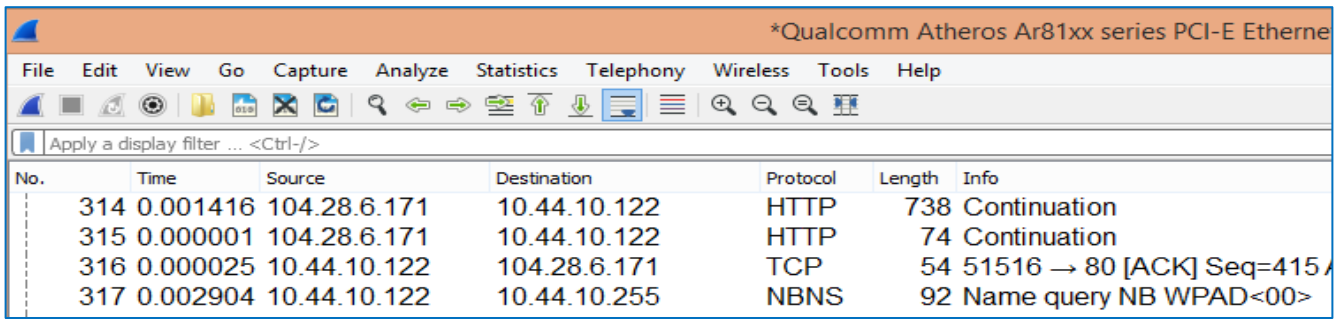
One OptiView XG was connected directly to the test laptop's Ethernet port using a CAT-6a cable.

The OptiView Throughput Test was used with various Frame Size and Utilization Settings.

For this test we wanted to document if there was any difference capturing from the Wireshark GUI versus the tshark command line utility.

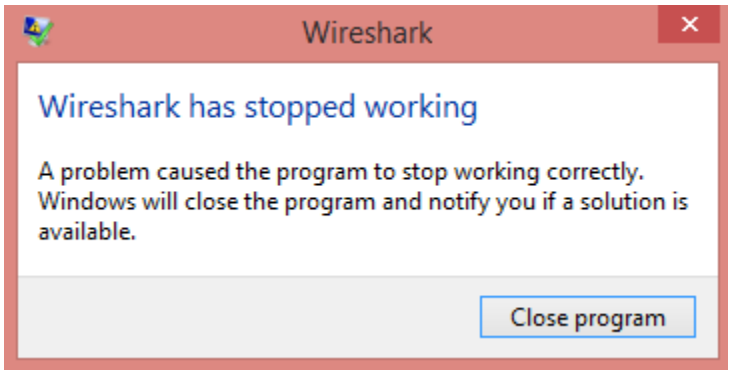
The parameters used for the one million packets generated are:

- 64 Byte frame size, 37.2% utilization
- 256 Byte frame size, 35% utilization
- 512 Byte frame size, 35% utilization
- 512 Byte frame size, 50% utilization
- 512 Byte frame size, 69.8% utilization



Notes

We noticed that Wireshark displayed the following error message when the incoming data rate overwhelmed the gUI.



Since the packet dropped counter was not accurate, we simply compared the OptiView transmitted value against what Wireshark reported captured.

Interface	Dropped packets	Capture filter
\Device\NPF_{A06AA122-9BDE-493C-ADF0-845BE0326E67}	524163 (2e+1 %)	none

Results

The table below is created using the following methodology;

- five tests were recorded
- the worst and best values were discarded
- the remaining three values were averaged

We noticed that using a 35% utilization and 512 Byte frame size was this laptops ‘sweet spot’. As soon as we increased the utilization, dropped packets were recorded but didn’t go past 11% loss.

Frame Size	Rate/Second	Utilization	Percent Lost
64	553,097	37.2	42%
256	158,490	35	3%
512	82,224	35	0%
512	117,489	50	11%
512	164,058	69.8	11%

OPTIVIEW XG TO LAPTOP - TSHARK

Wireshark - tshark

The OptiView XG was connected directly to the test laptop's Ethernet port using a CAT-6a cable. The OptiView Throughput Test was used with various Frame Size and Utilization Settings. The previous test was repeated using the tshark command line utility.

The parameters used for the one million packets generated are:

- 64 Byte frame size, 37.2% utilization
- 256 Byte frame size, 35% utilization
- 512 Byte frame size, 35% utilization
- 512 Byte frame size, 50% utilization
- 512 Byte frame size, 69.8% utilization

Notes

On our system, using the -w (write to file) option resulted in a higher number of packets captured compared to using the default where packets are displayed to the screen.

The *'packets dropped'* counter was not accurate, so we simply compared the OptiView transmitted value against what Wireshark reported.

In this example screenshot, the total of received and dropped packets is 988,647 which is 11,353 off the 1,000,000 packets generated.

```
C:\Users\tony fortunato\Desktop>tshark -i 8 -w test1.pcapng

C:\Users\tony fortunato\Desktop>tshark -i 8 -w test1.pcapng
Capturing on 'Qualcomm Atheros Ar81xx series PCI-E Ethernet Controller'
972711
15936 packets dropped
```

Results

The table below is created using the following methodology;

- five tests were recorded
- the worst and best values were discarded
- the remaining three values were averaged

Even though none of the tshark tests resulted in no packet loss, there overall less packet loss compared to the GUI.

Frame Size	Rate/Second	Utilization	Percent Lost
64	553,097	37.2	44%
256	158,490	35	0.24%
512	82,224	35	0.30%
512	117,489	50	0.10%
512	164,058	69.8	5.77%

OPTIVIEW XG TO LAPTOP – USB ETHERNET

PrimeCable USB 3.0 Adapter

The OptiView XG was connected directly to the test laptop's USB Ethernet adapter using a CAT-6a cable. The OptiView Throughput Test was used with various Frame Size and Utilization Settings. The previous test was repeated using the tshark command line utility. The parameters used for the one million packets generated are:

- 64 Byte frame size, 37.2% utilization
- 256 Byte frame size, 35% utilization
- 512 Byte frame size, 35% utilization
- 512 Byte frame size, 50% utilization
- 512 Byte frame size, 69.8% utilization

Results

The table below is created using the following methodology;

- five tests were recorded
- the worst and best values were discarded
- the remaining three values were averaged

These tests resulted in a consistently higher packet loss compared to the built in NIC.

Frame Size	Rate/Second	Utilization	Built In NIC Percent Lost	USB Ethernet Percent Lost
64	553,097	37.2	44%	53%
256	158,490	35	0.24%	0.5%
512	82,224	35	0.30%	1%
512	117,489	50	0.10%	1%
512	164,058	69.8	5.77%	9%

OPTIVIEW WITH PROFISHARK 1G

Throughput Test

Two OptiView XG were connected to the ProfiShark 1G with CAT-6a cables. The ProfiShark is connected to a laptop via USB 3.0. The same Throughput Test was conducted sending 1,000,000 frames at various sizes and speeds

Results

The ProfiShark 1G did not drop any packets regardless of load or packet sizes tested.

Frame Size	Rate/Second	Utilization	Percent Lost
64	553,097	37.2	0%
256	158,490	35	0%
512	82,224	35	0%
512	117,489	50	0%
512	164,058	69.8	0%

OPTIVIEW WITH PROFISHARK 1G

Service Test

The two OptiView XG that are connected to the ProfiShark 1G with CAT-6a cables were configured to perform a ‘service test’ to document if the ProfiShark adds any noticeable delay.

Tom
10.10.10.10

Jerry
10.10.10.100

Results

The test was configured to transmit 1 Gbps and with the following thresholds; 100 msec Latency, 20 ms Jitter and Frame Loss Ratio of 0.003

There was no packet loss, excessive latency, jitter or frame loss ratio reported between the OptiView’s. The test was repeated five times to confirm our results.

Test Suite
Service Performance Test | Results

Overall Status	Throughput (Mbps) Min	Avg	Max	Frame Loss Count	Ratio	Latency (ms) Min	Avg	Max	%	Jitter (ms) Min	Avg	Max	%	Avail %
Overall Results	971.62	971.62	971.63	0	0	<1	<1	<1	100	<0.01	<0.01	0.01	100	100
12/06 7:09 PM	971.62	971.62	971.62	0	0	<1	<1	<1	100	<0.01	<0.01	0.01	100	100
12/06 7:08 PM	971.62	971.62	971.62	0	0	<1	<1	<1	100	<0.01	<0.01	0.01	100	100
12/06 7:07 PM	971.62	971.62	971.63	0	0	<1	<1	<1	100	<0.01	<0.01	0.01	100	100
12/06 7:06 PM	971.62	971.62	971.63	0	0	<1	<1	<1	100	<0.01	<0.01	0.01	100	100
12/06 7:05 PM	971.62	971.62	971.63	0	0	<1	<1	<1	100	<0.01	<0.01	0.01	100	100

OPTIVIEW XG TAP BASELINE

OptiView XG TAP

Both OptiView XG's were connected to a tap using a CAT-6a cable.

The goal is to document if the tap affects the performance between the OptiView XG's and if the TAP can help the laptop capture more packets.

For this back-to-back test, I chose the following test parameters: Bits/Second 622Mbps, Frame Size Sweep (64, 128,256,512, 1024, 1280 and 1518 Bytes), Content All Zeros, Duration 1 minute per frame size.

The OptiView was tested successfully using the 1 Gb bandwidth setting five times. 622 Mbps was then selected as average of a typical 1 Gb link seen within corporate environments.

Results

There was no packet loss reported between the OptiView's across all frame sizes. The test was repeated five times to confirm our results.

Frame Size	Frames Generated	Percent Received
64	55,556,209	100%
128	31,529,553	100%
256	16,906,358	100%
512	8,770,100	100%
1024	4,468,994	100%
1280	3,589,016	100%
1518	3,033,635	100%

OPTIVIEW XG TAP TO LAPTOP - WIRESHARK

OptiView XG TAP and Laptop – GUI and tshark

Both OptiView XG's were connected to a tap as well as the test laptop's built in NIC using a CAT-6a cable.

The goal is to document if the tap affects the performance between the OptiView XG's and if the TAP can help the laptop capture more packets.

For this back-to-back test, I chose the following test parameters: Bits/Second 622Mbps, Frame Size Sweep (64, 128,256,512, 1024, 1280 and 1518 Bytes), Content All Zeros, Duration 1 minute per frame size.

Results

The table below is created using the following methodology;

- five tests were recorded
- the worst and best values were discarded
- the remaining three values were averaged

We concluded that a TAP does not reduce the number of dropped packets.

Frame Size	Rate/Second	Utilization	GUI Percent Lost	tshark Percent Lost
64	553,097	37.2	52%	43%
256	158,490	35	6%	0.14%
512	82,224	35	2%	0.20%
512	117,489	50	13%	0.20%
512	164,058	69.8	14%	5%

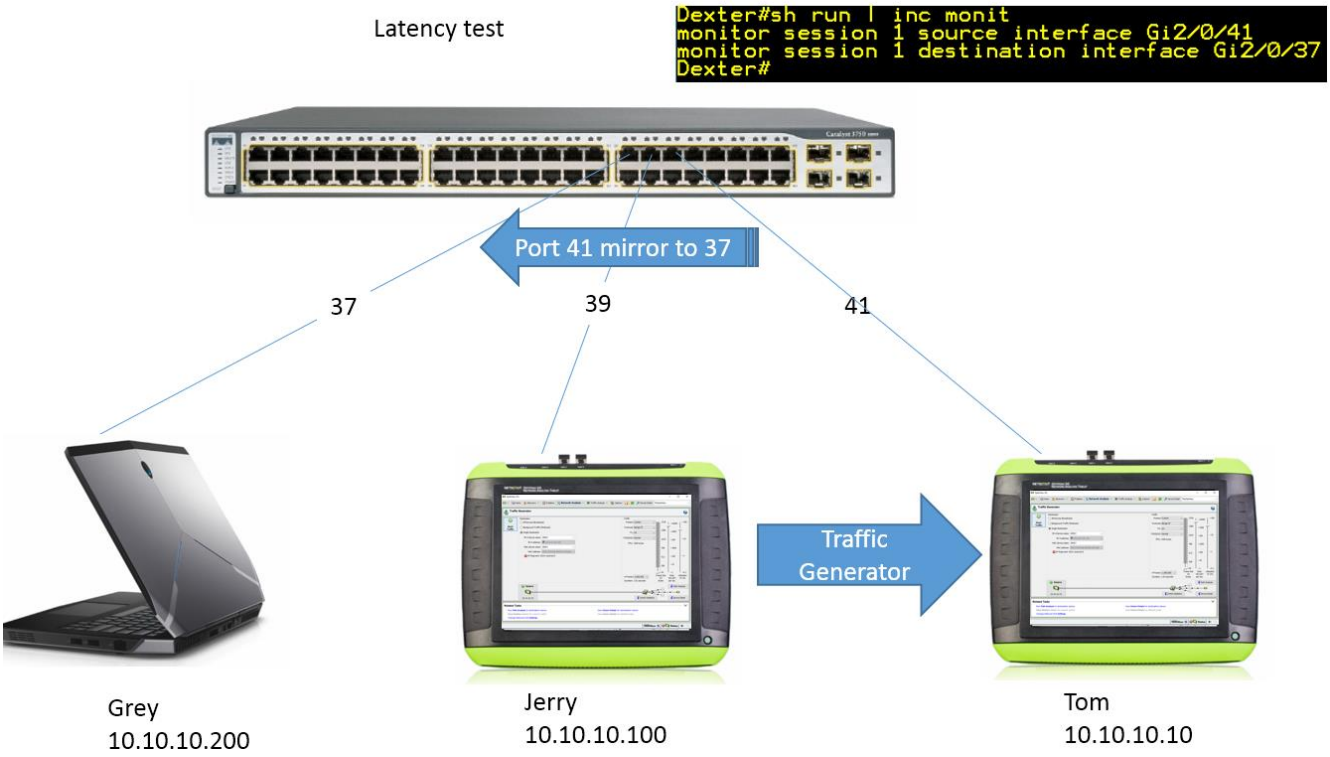
SPAN PORT

OptiView XG TAP And Laptop – GUI and tshark

Both OptiView XG's were connected to a Cisco 3750 as well as the test laptop using a CAT-6a cable.

The goal is to document if the switch's span port affects the laptop capturing packets. One theory out there is that switches can buffer and decrease the number of dropped packets.

The same throughput test was used and 1,000,000 packets were transmitted.



Results

The table below is created using the following methodology;

- five tests were recorded
- the worst and best values were discarded
- the remaining three values were averaged

We noticed that there wasn't that much of a difference in packet loss when using a TAP.

Frame Size	Rate/Second	Utilization	GUI Percent Lost	tshark Percent Lost
64	553,097	37.2	50%	35%
256	158,490	35	4%	0.14%
512	82,224	35	0%	0.80%
512	117,489	50	11%	0.80%
512	164,058	69.8	12%	3%