PROFI TAP

WHITE PAPER:

PROFISHARK PERFORMANCE RESULTS

WIRESHARK HEROES SERIES

VISIT WWW.PROFITAP.COM

TONY FORTUNATO

NETWORK PERFORMANCE SPECIALIST

Tony Fortunato is a Senior Network Performance Specialist with experience in design, implementation and troubleshooting networks since 1989.

Tony's background in networking started with design, support and implementation of financial trading floor networks and ISP's where Tony integrated and supported various vendors' equipment since1989. Tony works with a variety of products from Microsoft, Profitap, NetScout, Viavi and other Open Source products such as protocol analyzers (Wireshark) and MRTG.

Tony has taught and presented at numerous Colleges/Universities, public forums and private classes to thousands of analysts since 1999.

Tony has worked in various roles ranging from project management, network design, consulting, troubleshooting, designing customized courses and assisting with installing physical equipment, those daunting datacenter clean-ups and network migration projects.

WWW.THETECHFIRM.COM

TABLE OF CONTENT

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(TM) i7-4910MQ processor (Quad Core, 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.
- ⊙ Important to note that the dropped packet counter was far from accurate using tshark or the Wireshark GUI.
- × Wireshark/WinPcap experienced packet loss at moderate loads.
- × Using a TAP or SPAN port in an effort to buffer and capture more packets is a myth.
- × An Ethernet USB adapter is not recommended for reliable packet analysis.

TESTING SUMMARY

Initial equipment tests were conducted back to back with an Ethernet cable between equipment when possible. By eliminating the switch we wanted to remove any factors such as delays, packet loss or other variables that a switch may cause. This methodology was also used to establish a baseline before introducing other equipment.

One of the goals of this paper is to demonstrate that it does NOT take 1 Gbps of line rate traffic to cause packet loss on WinPcap based systems. Practical frame sizes and loads were selected for the majority of the tests. Full line rate tests were provided at the end to document ProfiShark 1G performance.

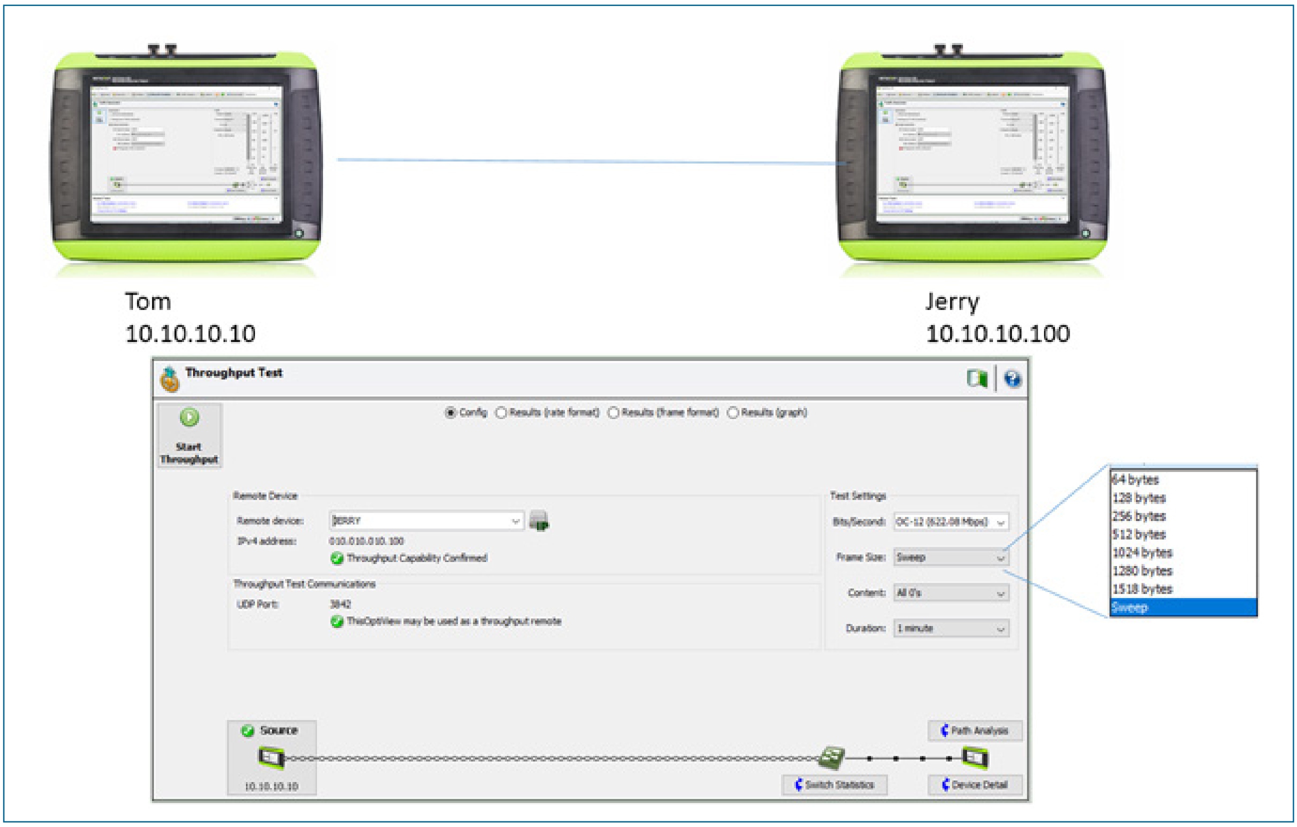
The various test scenarios covered in this document used traffic generators, a TAP, SPAN, laptop and of course the ProfiShark1G.

TRAFFIC GENERATOR BACK TO BACK

Setting a Baseline

Two traffic generators 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 XG 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



Remote Device
Remote device: JERRY
IPv4 address: 010.010.010.100
Throughput Capability Confirmed

Throughput Test Communications
UDP Port: 3842
ThisOptiView may be used as a throughput remote

Test Settings
Bits/Second: OC-12 (622.08 Mbps)
Frame Size: Sweep
Content: All 0's
Duration: 1 minute

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:

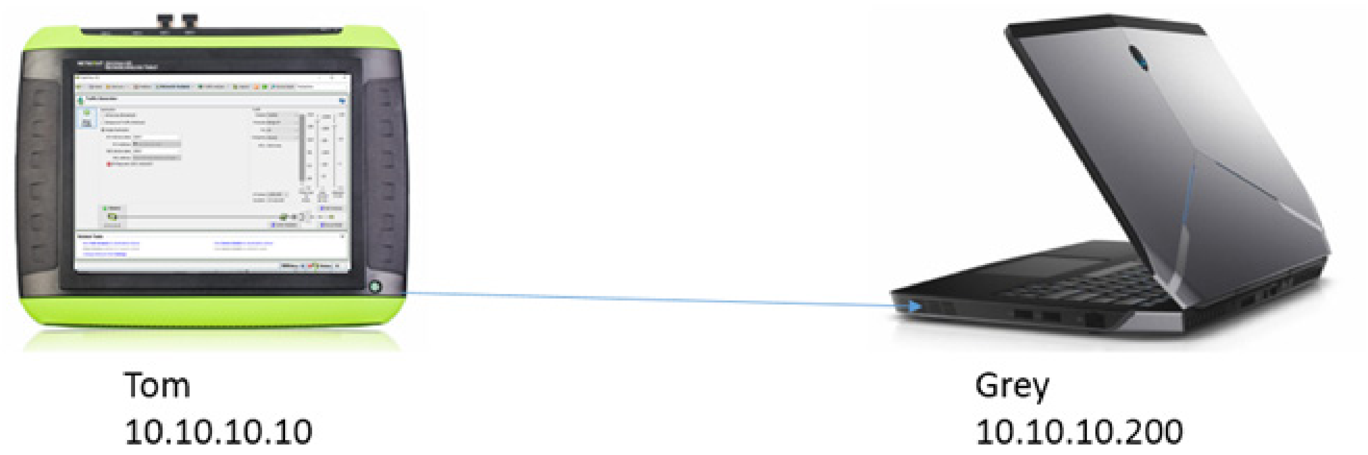
1. Five tests were recorded
2. The worst and best values were discarded
3. The remaining three values were averaged

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%

TRAFFIC GENERATOR TO LAPTOP - WIRESHARK GUI

Wireshark - GUI

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

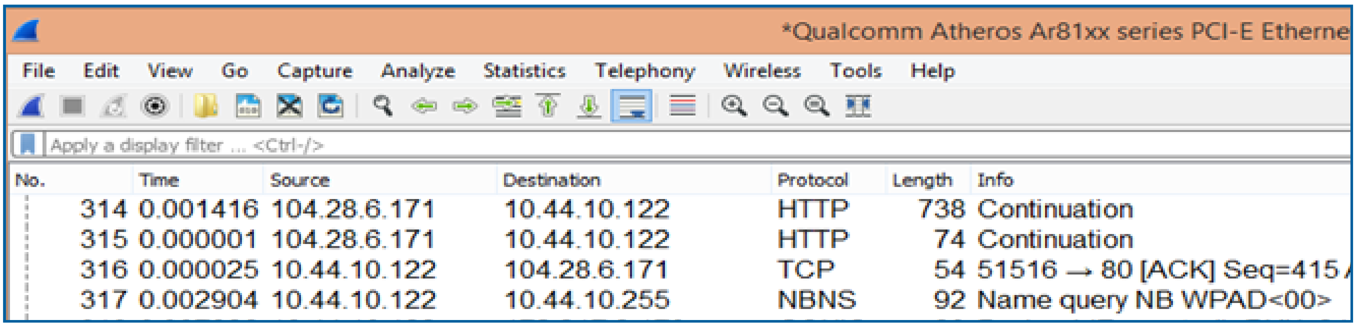


The Throughput Test was used with various Frame Size and Utilization Settings.

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

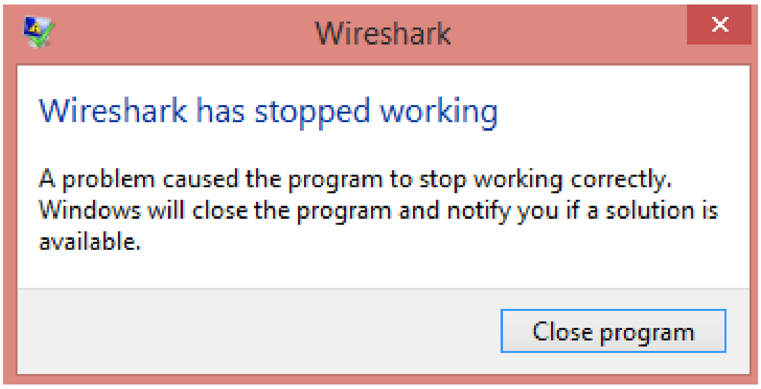
The parameters used for the one million packets generated are:

- 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


*Qualcomm Atheros Ar81xx series PCI-E Etherne
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source        Destination    Protocol  Length  Info
  314 0.001416  104.28.6.171  10.44.10.122   HTTP         738  Continuation
  315 0.000001  104.28.6.171  10.44.10.122   HTTP          74  Continuation
  316 0.000025  10.44.10.122  104.28.6.171   TCP           54  51516 → 80 [ACK] Seq=415
  317 0.002904  10.44.10.122  10.44.10.255   NBNS          92  Name query NB WPAD<00>
```

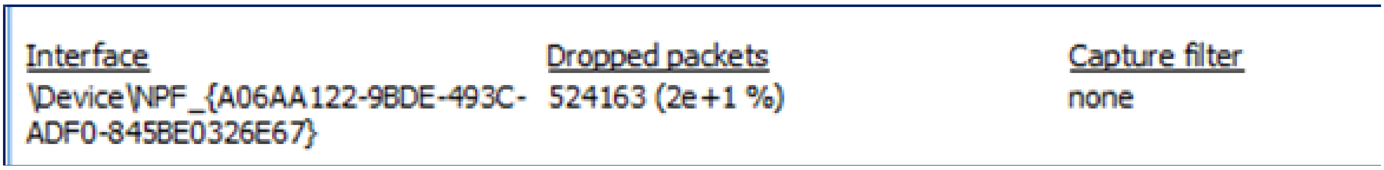
► **Note:** We noticed that Wireshark displayed the following error message when the incoming data rate overwhelmed the Wireshark GUI.



Wireshark has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

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 was created using our standard testing methodology:

1. Five tests were recorded
2. The worst and best values were discarded
3. 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. Since packet loss was recorded we did not see the value in performing a full line rate test in this scenario.

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%

TRAFFIC GENERATOR TO LAPTOP - TSHARK

Wireshark - tshark

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

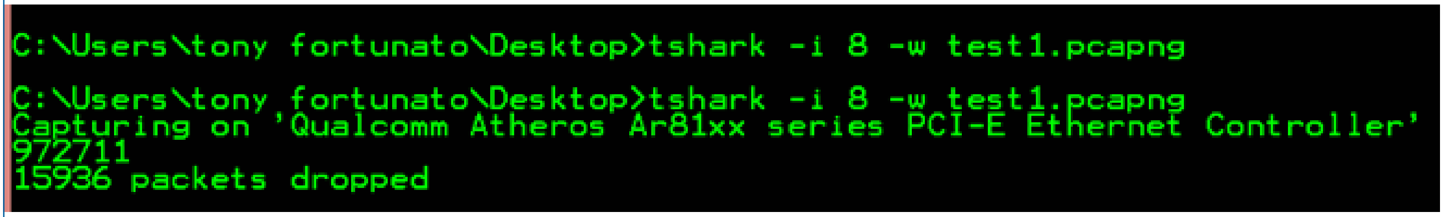
The parameters used for the one million packets generated are:

- 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

► Note: 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 was created using our standard testing methodology:

1. Five tests were recorded
2. The worst and best values were discarded
3. 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. Since packet loss was recorded we did not see the value in performing a full line rate test in this scenario.

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%

TRAFFIC GENERATOR TO LAPTOP - USB ETHERNET

PrimeCable USB 3.0 Adapter

The traffic generator 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;

1. Five tests were recorded
2. The worst and best values were discarded
3. The remaining three values were averaged

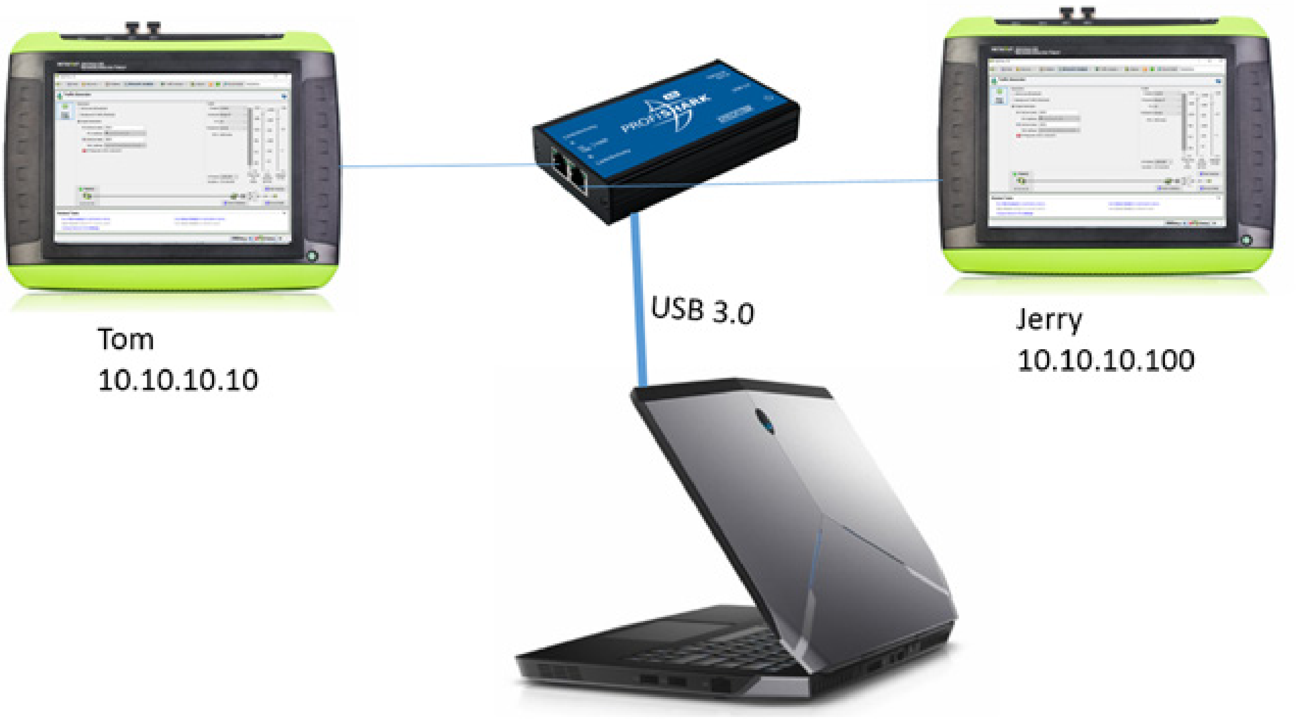
These tests resulted in a consistently higher packet loss compared to the built in NIC. Since packet loss was recorded we did not see the value of performing a full line rate test.

			Built in NIC	USB Ethernet
Frame Size	Rate/Second	Utilization	Percent Lost	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%

TRAFFIC GENERATOR 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

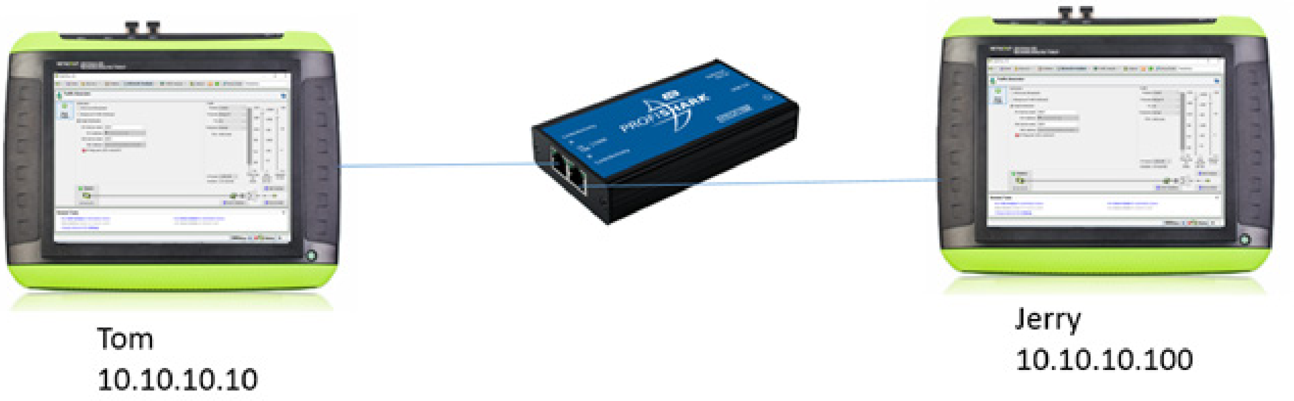
The ProfiShark 1G did not drop any packets regardless of load or packet sizes tested.

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%

TRAFFIC GENERATOR WITH PROFISHARK 1G

Service Test

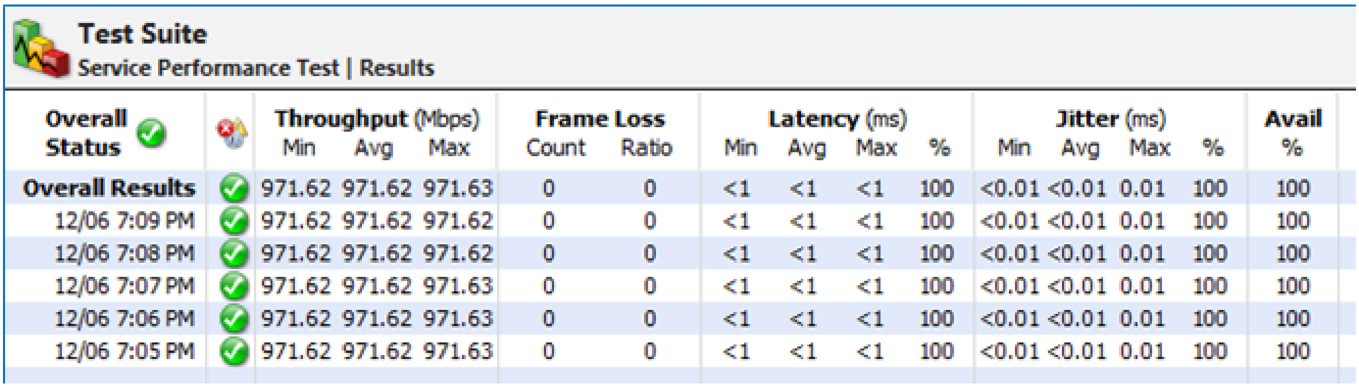
The two traffic generators that are connected to the ProfiShark 1G with CAT-6a cables were configured to perform a 'service test' to document if the ProfiShark 1G adds any noticeable delay.



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 OptiViews. The test was repeated five times to confirm our results.



Test Suite
Service Performance Test | Results

Overall Status ✓		Throughput (Mbps)			Frame Loss		Latency (ms)				Jitter (ms)				Avail
		Min	Avg	Max	Count	Ratio	Min	Avg	Max	%	Min	Avg	Max	%	%
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

TAP BASELINE

Traffic Generator TAP

Both traffic generators were connected to a tap using a CAT-6a cable.

The goal is to document if the tap affects the performance between the traffic generators 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 traffic generator 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 traffic generator 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%

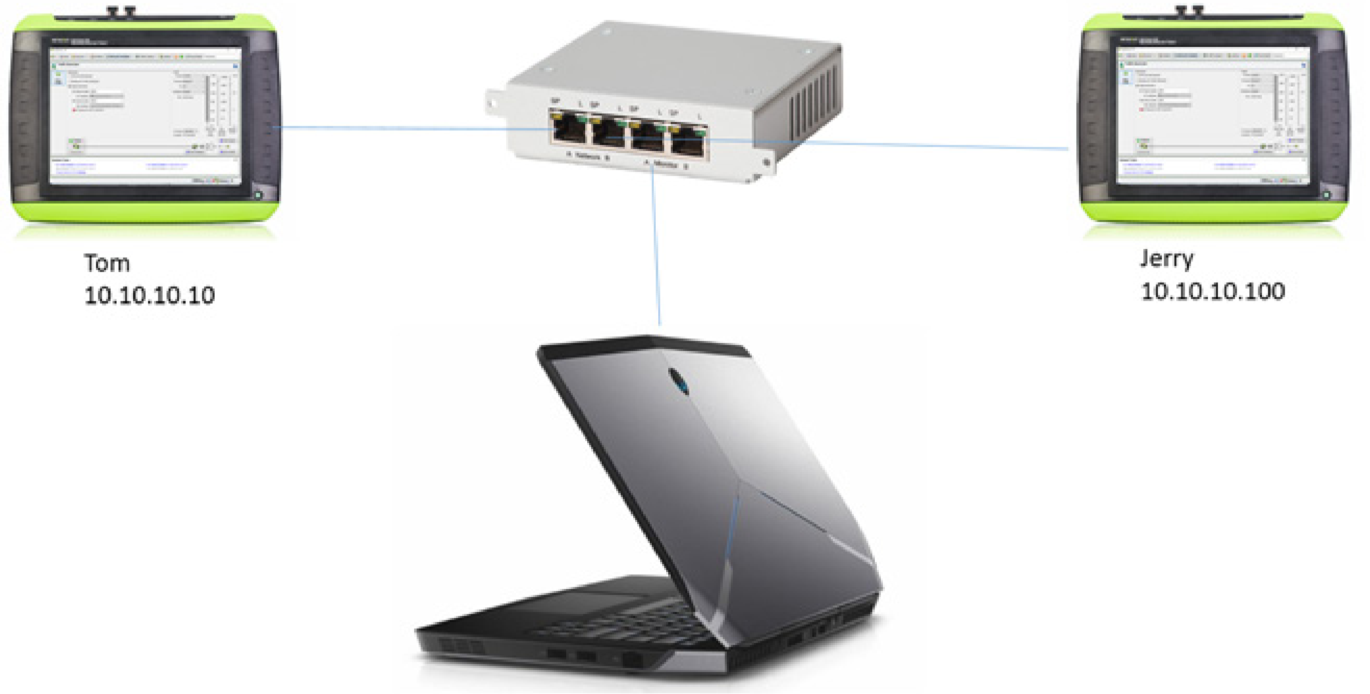
TRAFFIC GENERATOR TAP TO LAPTOP - WIRESHARK

Traffic Generator TAP and Laptop – GUI and tshark

Both traffic generators 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 Traffic generators 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;

1. Five tests were recorded
2. The worst and best values were discarded
3. The remaining three values were averaged

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

			Built in NIC	USB Ethernet
Frame Size	Rate/Second	Utilization	Percent Lost	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%

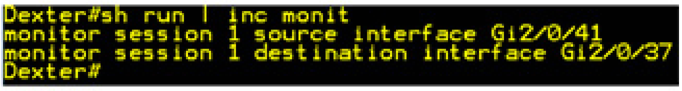
SPAN PORT

Traffic Generator TAP and Laptop – GUI and tshark

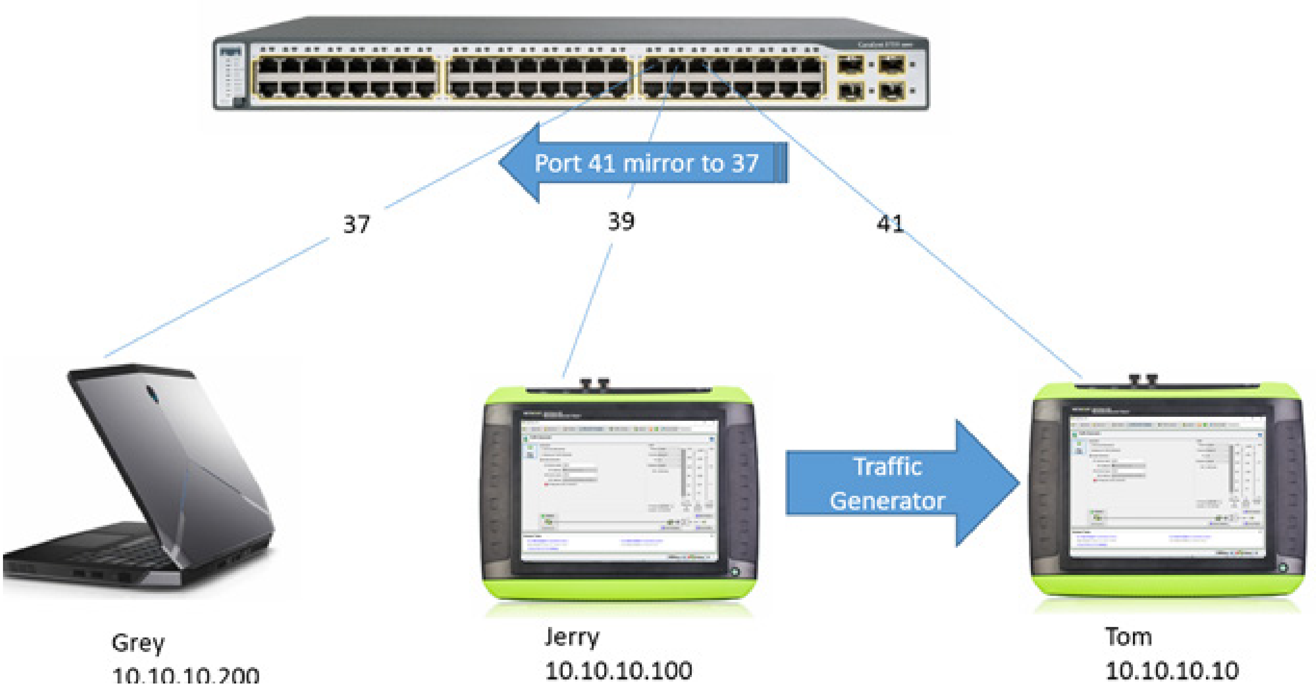
Both traffic generators were connected to a Cisco 3750 as well as the test laptop using a CAT-6a cable.
The goal is to document if the switch's span port affects the laptop capturing packets. One theory out there is that switches can buffer and decrease the number of dropped packets.

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

Latency test



```
Dexter#sh run | inc monit
monitor session 1 source interface Gi2/0/41
monitor session 1 destination interface Gi2/0/37
Dexter#
```



RESULTS

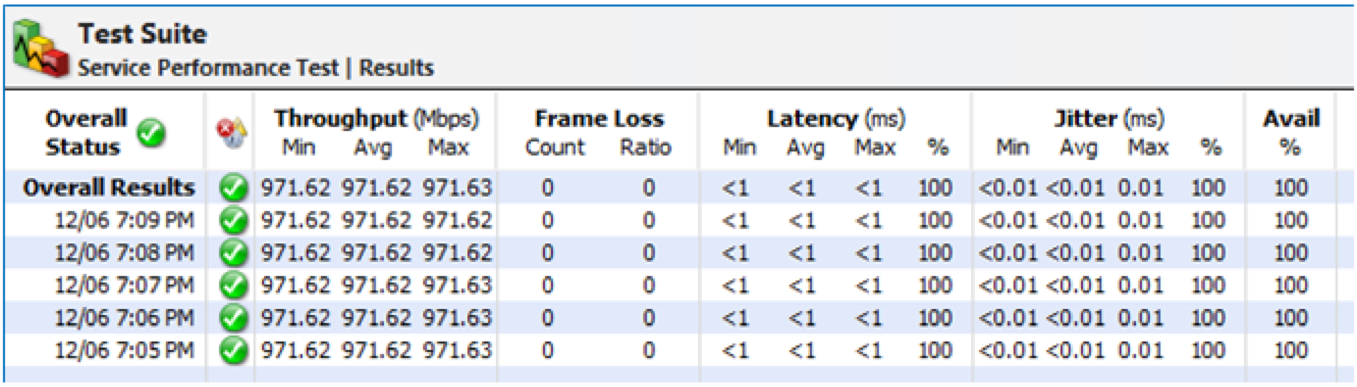
The table below was created using our standard testing methodology:

1. Five tests were recorded
2. The worst and best values were discarded
3. The remaining three values were averaged

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

			GUI	tshark
Frame Size	**Rate/Second**	**Utilization**	**Percent Lost**	**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%

The ProfiShark 1G introduced no noticeable latency, jitter or packet loss a full line rate.



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

CONCLUSION

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

			GUI	*tshark*	*ProfiShark 1G*
Frame Size	*Rate/Second*	*Utilization*	*Percent Lost*	*Percent Lost*	*Percent Lost*
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%

The ProfiShark 1G also provides the following features

- SPAN and In-Line modes
- 8 ns hardware timestamp
- Direct capture to disk (ProfiShark Manager)
- Real time statistics (ProfiShark Manager)
- By connecting a NAS to the ProfiShark's USB port, you can capture for extended periods of time
- The unit itself Dual Core Processor and 4 GB memory
- Compatible with Wireshark, ClearSight, OmniPeek, Packetyzer, OptiView, and other analyzers
- PoE compliant so capture packets from POE devices such as access points, phones, webcams, etc.
- Split capture to different files, based on time or size

PROFISHARK OVERVIEW

PROFISHARK 1G

PROFISHARK 10G

The ProfiShark 1G and 10G can capture any traffic, frames of any size and type, in-line or SPAN, for analysis and monitoring with Wireshark, or any major software analyzer. The included ProfiShark Manager software provides additional information, statistics, and configuration and capture options.

PROFISHARK 1G+

PROFISHARK 10G+

The ProfiShark 1G+ and 10G+'s GPS/GLONASS function can tag packets with accurate UTC timestamps. The ProfiShark 1G+ and 10G+ can also receive or generate a PPS signal, enabling accurate timestamp synchronization in various topologies.

PROFISHARK 100M

The ProfiShark 100M is designed for the capture of 10/100M Ethernet traffic. It is the perfect tool for troubleshooting Real-Time Industrial Ethernet protocols. As an all-in-one network TAP in a pocket-sized box, this portable traffic capture device gives you all the flexibility and ease of use you require for the monitoring of industrial networks.

- USB powered, no adapter required
- Lightweight and portable
- Hardware aggregation
- SPAN and In-Line modes
- 8 ns hardware timestamping
- Capture any type of frames
- Low level error and bandwidth monitoring
- Hardware filtering, deep packet inspection
- CRC error capture
- Packet slicing
- Non-intrusive, fail-safe monitoring
- Real time statistics
- Direct capture to disk
- Very low CPU usage
- Quick setup and easy to use
- Invisible to the network

COMPATIBILITY

- Wireshark
- ClearSight
- OmniPeek
- Packetyzer
- OptiView
- NetSpector
- NetDecoder
- Ethertest

And many more...

IT ALL STARTS WITH VISIBILITY

PROFITAP

Profitap develops a wide range of state-of-the-art and user-friendly network monitoring tools for both SMEs and the enterprise sector. Our wide range of high-density network TAPs, field service troubleshooters and network packet brokers are extremely performant, providing complete visibility and access to your network, 24/7.

We've been creating monitoring solutions for network analysis and traffic acquisition for more than 33 years. Therefore, we are experts in our field and our award-winning ProfiShark® 1G stands to prove it. This lightweight, advanced and portable network TAP is one the most innovative products on the market.

With more than 1,000 clients from 55 countries, PROFITAP has become a must-have solution for many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

Profitap

@Profitap

profitap-international