An open source network traffic performance monitoring and diagnostics tool.

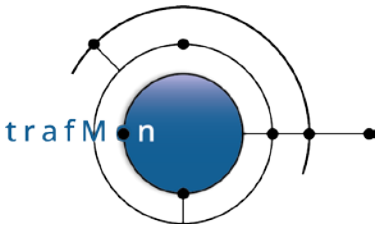

**www.trafmon.org**

# Use Case 2: Communications Troubleshooting & Diagnosis

**Thomas Grootaers, Luc Lechien**

**Software Release 1.0**

**2020-10**




An open source network traffic performance monitoring and diagnostics tool.

# COPYRIGHT, LICENSE AND TRADEMARKS



This material is based upon work funded and supported by the European Space Agency and the Belgian Federal Authorities (BELSPO) under GSTP Contract Nr ESRIN 4000128964/19/I-EF with AETHIS sa/nv, Belgium.

The view, opinions, and/or findings contained in this material are those of the authors and subsequent free contributors and should not be construed as an official ESA, Government or AETHIS position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by ESA or AETHIS.

NO WARRANTY. THIS AETHIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. AETHIS MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. AETHIS DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT] This material is for approved for public release and unlimited distribution under the terms and conditions of Open Source Apache License v2.0 (https://www.apache.org/licenses/LICENSE-2.0.txt, OSI Approved https://opensource.org/licenses/Apache-2.0), which governs its use, distribution, modification and re-publication.

# DOCUMENT HISTORY

| Release | Date | Change |
|---|---|---|
| 1.0 | October 2020 | First issue |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# ACKNOWLEDGEMENTS

The authors wish to acknowledge the valuable contributions of all ancient employees of the AETHIS® Company in Belgium, who have worked on the successive versions of the base software and its documentation from which the open source trafMon software is derived.

In particular, special recognition is given to Jacques Maes, David Orban, Jonathan Van den Schrieck, Benoît Liétaer, Julien Denis, Thomas Soupart, Fabien Coenegrachts, who have more specifically participated to its elaboration. Also, a thought is given in memory the authors' deceased associate, Luc Steenput, who has heavily promoted the initial idea and subsequent enhancements of the tool, within the European Space Agency and elsewhere.

Lastly, the authors wish to acknowledge the strong support of ESA staff members: Manfred Lugert, Erling Kristiansen, Johan Stjernevi, Manfred Bertelsmeier, Gioacchino Buscemi, Michele Iapaolo, Andrea Cogliandro and Claudia Neroni, as well as of officers of the Belgian BELSPO Federal Service, Jacques Nijskens, Agnès Grandjean and Hendrick Verbeelen.

# TABLE OF CONTENT

# 1. INTRODUCTION

In this example case of use, we illustrate through real-life examples the power of the trafMon tools in conducting communications trouble shooting.

This example tutorial document also highlights the relevant portions of the configuration file permitting to produce the types of traffic observations underlying the described troubleshooting scenarios.

# 2. ICMP ERRORS MAPPED TO A DATA FLOW

The ICMP protocol mostly encompasses error messages at IP network layers that are induced by one or several packets belonging to a given data flow. While decoding such ICMP error reporting packets, the trafMon probe retrieves the using data flow instance in order to increment its corresponding error counter part of its observed statistics.

In the figure below, the DNS (UDP port 53) responses data flow from server (141.253.221.224) to client (10.201.0.11) is experiencing a large amount of Unreached error: 1266 over the 6 weeks period where these DNS packets are generated during 2.3381 percent of the covered minutes.

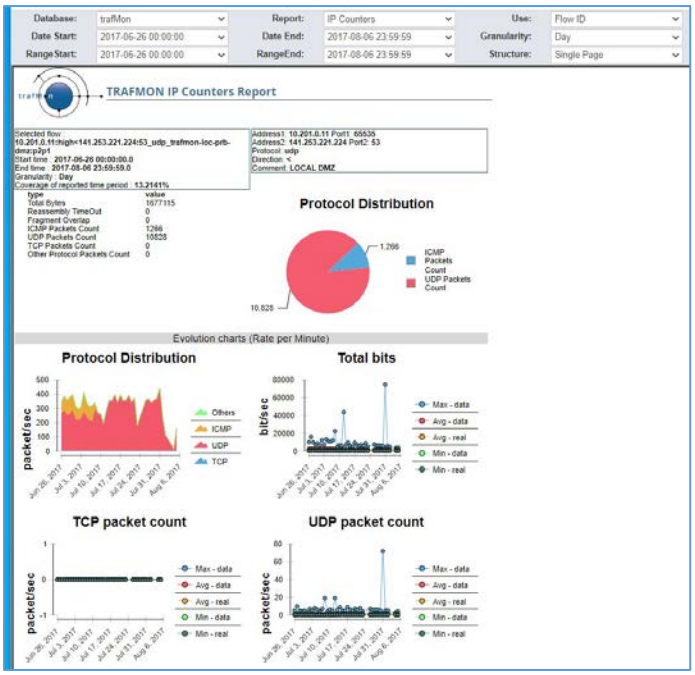
## TRAFMON ICMP Counters Report

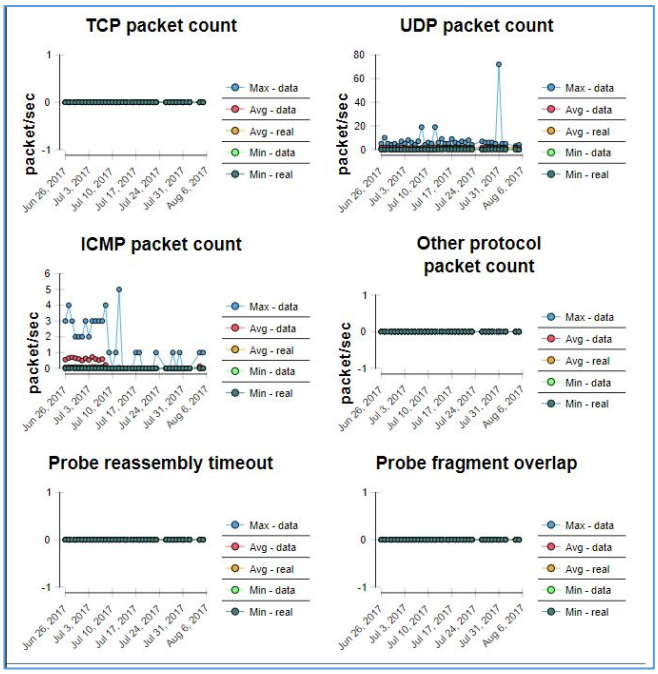
Selected flow :
**10.201.0.11:high<141.253.221.224:53_udp_trafmon-loc-prb-dmz:p2p1**
Start time : **2017-06-26 00:00:00.0**
End time : **2017-08-06 23:59:59.0**
Granularity : **Day**
Coverage of reported time period : **2.3381%**

Address1: **10.201.0.11** Port1: **65535**
Address2: **141.253.221.224** Port2: **53**
Protocol: **udp**
Direction: **<**
Comment: **LOCAL DMZ**

| type | value |
|---|---|
| Checksum Failures | 0 |
| Checksum Skipped | 29 |
| Echo Request | 0 |
| Echo Replies | 0 |
| Fragmentation Needed | 0 |
| Source Quench | 0 |
| TTL Expired | 0 |
| Reassembly TimeOut | 0 |
| UnReached | 1266 |
| Redirects | 0 |
| Other ICMP Errors | 0 |

But, by looking at the corresponding flow IP Counters and their evolution chart, It doesn't seem to be a permanent problem: indeed, there are far more data packets than ICMP error occurrences. So, the client side could experience network problems. Being a private IPv4 address, the root cause



could lie in the inter-LAN connectivity: intermittent VPN link or lack of static return route over one of the possible inter-LAN paths.

# 3. FTP FILE TRANSMISSION PROBLEMS

## 3.1 OPERATORS OR CONVERSATIONS REPORT PER SERVER

Thanks to the in-depth protocol dissection and FTP sessions follow-up, the tool permits to pinpoint problems occurring during file transfers with one particular remote client.

First, we start with the synthetic Operators report applied to a given FTP server: 141.253.221.106:21, and we look at its communications with peers (i.e. FTP clients in our case):

- Ingress traffic from 36.110.173.7 is not really big (17.92 MB), but experiences 1.23 % of retransmission, although consisting mostly in empty acknowledges (only 1.38 KB of TCP payload) of files that are actually traversing in the reverse direction (downloads):

INGRESS

| Host | Host DNS | Protocol | Application | Peer Location | Peer Address | Peer DNS | Bit Rate | Bytes | IP Bytes | Protocol Overhead | Percent Retransmit | Payload Bytes | Retransmitted Payload | Avg Last Window | Avg Max Window |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 141.253.221.106 | mgt-ftp.eo.company.com. | tcp | No Match | FINANCE | 141.253.149.110 | 141-253-149-110.local.company.com. | 6.27 Kb/s | 11.70 KB | | | | | | | |
| | | | | HRM | 141.253.221.11 | 141.253.221.11 | 1.48 Kb/s | 224.79 MB | | | | | | | |
| | | | | MGT | 141.253.196.17 | mgt-klauss.company.com. | 5.21 Mb/s | 5.58 GB | | | | | | | |
| | | | | | 172.19.11.219 | mgt-gfe-ref.esr.mmpds.company. | 19.31 Kb/s | 864 B | | | | | | | |
| | | | | | 172.28.96.140 | mgt_l2pro.mgt.mmpds.c | 95.09 Kb/s | 4.75 KB | | | | | | | |
| | | | | | 172.28.96.141 | mgt-mppf-pc3.mgt.mmpds.compan | 2.39 Mb/s | 912 B | | | | | | | |
| | | | | | 172.28.96.145 | mgt-mppf-pc5.mgt.mmpds.compan | 15.31 Mb/s | 1.18 GB | | | | | | | |
| | | | | OTHER | 123.127.64.6 | 123.127.64.6 | 6.57 Kb/s | 48.95 MB | | | | | | | |
| | | | | | 124.17.3.4 | 124.17.3.4 | 2.76 Kb/s | 1.67 MB | | | | | | | |
| | | | | | 136.159.160.156 | 136.159.160.156 | 2.60 Kb/s | 2.56 KB | | | | | | | |
| | | | | | 139.17.74.40 | mag45.gfz-potsdam.de. | 513.33 Kb/s | 3.98 KB | | | | | | | |
| | | | | | 159.226.22.8 | 159.226.22.8 | 19.78 Kb/s | 65.44 MB | | | | | | | |
| | | | | | 212.0.110.2 | caronte.mv.com. | 1.56 Kb/s | 3.40 KB | | | | | | | |
| | | | | | 36.110.173.7 | 36.110.173.7 | 3.49 Kb/s | 11.48 MB | | | | | | | |
| | | | | | 82.214.143.178 | 82-214-143-178.itsa.net.pl. | 190.09 Kb/s | 104.04 MB | | | | | | | |
| | | | | | 95.128.91.229 | cust-95-128-91-229.breedbanddelft.nl. | 30.62 Kb/s | 2.06 KB | | | | | | | |
| | | | ftp | FINANCE | 141.253.149.110 | 141-253-149-110.local.company.com. | 6.27 Kb/s | 6.22 MB | 6.21 MB | 10.80 % | 0.54 % | 3.11 MB | 12 B | 9,616 | 9,615.667 |
| | | | | MGT | 141.253.196.17 | mgt-klauss.company.com. | 5.21 Mb/s | 28.80 GB | 28.84 GB | 3.91 % | | 27.84 GB | 36.68 KB | 101,313 | 101,400.258 |
| | | | | | 172.19.11.219 | mgt-gfe-ref.esr.mmpds.company. | 19.31 Kb/s | 1.16 MB | 1.16 MB | 4.94 % | | 1.12 MB | | 12,517 | 12,516.5 |
| | | | | | 172.28.96.140 | mgt_l2pro.mgt.mmpds.c | 95.09 Kb/s | 104.53 MB | 104.53 MB | 4.13 % | | 4.90 MB | | 10,768 | 10,853.619 |
| | | | | | 172.28.96.141 | mgt-mppf-pc3.mgt.mmpds.compan | 2.39 Mb/s | 143.21 MB | 143.21 MB | 3.81 % | | 138.22 MB | | 31,102 | 31,102 |
| | | | | | 172.28.96.145 | mgt-mppf-pc5.mgt.mmpds.compan | 15.31 Mb/s | 8.01 GB | 8.02 GB | 3.89 % | | 7.74 GB | | 37,531 | 37,534.812 |
| | | | | OTHER | 123.127.64.6 | 123.127.64.6 | 6.28 Kb/s | 40.63 MB | 40.63 MB | 6.31 % | | 853 B | | 1,223 | 1,222.667 |
| | | | | | 136.159.160.156 | 136.159.160.156 | 2.60 Kb/s | 481.34 KB | 479.97 KB | 4.62 % | | 1.59 KB | | 3,040 | 3,040 |
| | | | | | 139.17.74.40 | mag45.gfz-potsdam.de. | 513.36 Kb/s | 246.50 MB | 246.50 MB | 40.91 % | | 237.81 MB | 7 B | 5,739 | 5,738.976 |
| | | | | | 159.226.22.8 | 159.226.22.8 | 19.78 Kb/s | 101.13 MB | 101.10 MB | 4.53 % | 0.27 % | 1.93 KB | 5 B | 2,538 | 41,468.464 |
| | | | | | 212.0.110.2 | caronte.mv.com. | 1.56 Kb/s | 2.76 MB | 2.76 MB | 6.84 % | | 750 B | | 3,680 | 3,680 |
| | | | | | 36.110.173.7 | 36.110.173.7 | 3.49 Kb/s | 17.92 MB | 17.91 MB | 7.14 % | 1.23 % | 1.38 KB | | 3,297 | 5,632.475 |
| | | | | | 82.214.143.178 | 82-214-143-178.itsa.net.pl. | 190.09 Kb/s | 221.85 MB | 221.82 MB | 6.66 % | | 210.71 MB | | 36,641 | 36,641.055 |
| | | | | | 95.128.91.229 | cust-95-128-91-229.breedbanddelft.nl. | 30.62 Kb/s | 3.68 MB | 3.68 MB | 4.47 % | | 2.11 KB | | 1,824 | 1,824 |
| | | | ssh | MGT | 172.19.11.196 | mgt-dvt-temp.mgt.mmpds.compa | 380.08 Kb/s | 304.88 MB | | | | | | | |

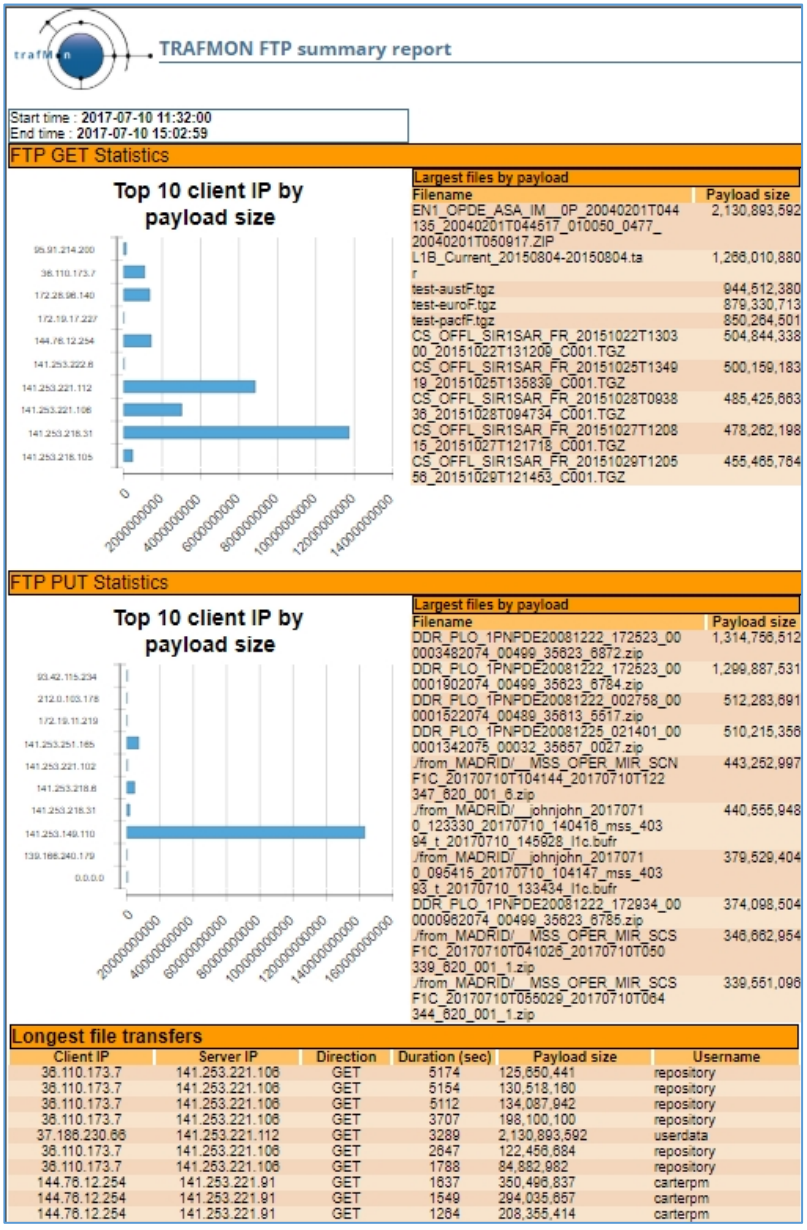
- But more significantly, egress traffic to 36.110.173.7 forms the bulk (1.10 GB) and experiences 3.05 % of retransmission in supporting the actual download of data files:

EGRESS

| Host | Host DNS | Protocol | Application | Peer Location | Peer Address | Peer DNS | Bit Rate | Bytes | IP Bytes | Protocol Overhead | Percent Retransmit | Payload Bytes | Retransmitted Payload | Avg Last Window | Avg Max Window |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 141.253.221.106 | mgt-ftp.eo.company.com. | tcp | No Match | FINANCE | 141.253.149.110 | 141-253-149-110.local.company.com. | 417.99 Kb/s | 63.56 KB | | | | | | | |
| | | | | MGT | 141.253.196.17 | mgt-klauss.company.com. | 17.13 Kb/s | 21.00 MB | | | | | | | |
| | | | | | 172.17.70.83 | 172.17.70.83 | 7.18 Kb/s | 15.48 KB | | | | | | | |
| | | | | | 172.28.96.140 | mgt_l2pro.mgt.mmpds.c | 14.52 Mb/s | 9.86 KB | | | | | | | |
| | | | | | 172.28.96.141 | mgt-mppf-pc3.mgt.mmpds.compan | 8.13 Kb/s | 8.31 KB | | | | | | | |
| | | | | | 172.28.96.145 | mgt-mppf-pc5.mgt.mmpds.compan | 65.26 Kb/s | 5.13 MB | | | | | | | |
| | | | | OTHER | 123.127.64.6 | 123.127.64.6 | 252.03 Kb/s | 1.89 GB | | | | | | | |
| | | | | | 124.17.3.4 | 124.17.3.4 | 67.01 Kb/s | 112.18 MB | | | | | | | |
| | | | | | 136.159.160.156 | 136.159.160.156 | 277.79 Kb/s | 15.19 KB | | | | | | | |
| | | | | | 139.17.74.40 | mag45.gfz-potsdam.de. | 14.12 Kb/s | 50.31 KB | | | | | | | |
| | | | | | 159.226.22.8 | 159.226.22.8 | 1.37 Mb/s | 4.10 GB | | | | | | | |
| | | | | | 212.0.110.2 | caronte.mv.com. | 72.15 Kb/s | 9.35 KB | | | | | | | |
| | | | | | 36.110.173.7 | 36.110.173.7 | 227.70 Kb/s | 716.60 MB | | | | | | | |
| | | | | | 82.214.143.178 | 82-214-143-178.itsa.net.pl. | 422.02 Kb/s | 101.64 MB | | | | | | | |
| | | | | | 95.128.91.229 | cust-95-128-91-229.breedbanddelft.nl. | 2.92 Mb/s | 34.94 KB | | | | | | | |
| | | | ftp | FINANCE | 141.253.149.110 | 141-253-149-110.local.company.com. | 417.99 Kb/s | 199.57 MB | 199.55 MB | 10.80 % | 1.97 % | 194.17 MB | 3.56 MB | 753,664 | 188,416 |
| | | | | MGT | 141.253.196.17 | mgt-klauss.company.com. | 17.13 Kb/s | 127.66 MB | 127.67 MB | 3.91 % | | 729.18 KB | | 25,272 | 3,610.35 |
| | | | | | 172.17.70.83 | 172.17.70.83 | 7.18 Kb/s | 1.72 MB | 1.72 MB | 16.27 % | | 1.65 MB | | 23,595 | 11,797.333 |
| | | | | | 172.28.96.140 | mgt_l2pro.mgt.mmpds.c | 14.52 Mb/s | 14.90 GB | 14.90 GB | 4.13 % | | 14.38 GB | 30.41 KB | 2,279,530 | 325,647.145 |
| | | | | | 172.28.96.141 | mgt-mppf-pc3.mgt.mmpds.compan | 8.13 Kb/s | 485.08 KB | 485.08 KB | 3.81 % | 5.45 % | 1.54 KB | | 1,840 | 1,840 |
| | | | | | 172.28.96.145 | mgt-mppf-pc5.mgt.mmpds.compan | 65.26 Kb/s | 34.05 MB | 34.09 MB | 3.89 % | 1.49 % | 7.09 KB | | 4,559 | 4,559.292 |
| | | | | OTHER | 123.127.64.6 | 123.127.64.6 | 250.27 Kb/s | 1.58 GB | 1.58 GB | 6.31 % | 1.26 % | 1.53 GB | 19.34 MB | 15,183 | 15,182.708 |
| | | | | | 124.17.3.4 | 124.17.3.4 | 22.35 Kb/s | 66.05 MB | 66.02 MB | 62.79 % | 43.26 % | 64.19 MB | 165.70 KB | 154,521 | 51,507.146 |
| | | | | | 136.159.160.156 | 136.159.160.156 | 277.79 Kb/s | 50.01 MB | 50.01 MB | 4.62 % | 0.04 % | 48.18 MB | 16.49 KB | 46,577 | 46,577.333 |
| | | | | | 139.17.74.40 | mag45.gfz-potsdam.de. | 14.14 Kb/s | 6.84 MB | 6.84 MB | 40.91 % | 1.26 % | 3.39 MB | | 19,747 | 9,873.481 |
| | | | | | 159.226.22.8 | 159.226.22.8 | 1.37 Mb/s | 6.70 GB | 6.70 GB | 4.53 % | 0.44 % | 6.52 GB | 25.98 MB | 2,329,377 | 1,164,688.375 |
| | | | | | 212.0.110.2 | caronte.mv.com. | 72.15 Kb/s | 127.64 MB | 127.64 MB | 6.84 % | 2.22 % | 124.22 MB | 2.75 MB | 119,603 | 119,603.2 |
| | | | | | 36.110.173.7 | 36.110.173.7 | 227.70 Kb/s | 1.10 GB | 1.10 GB | 7.14 % | 3.05 % | 1.08 GB | 32.73 MB | 142,686 | 142,685.634 |
| | | | | | 82.214.143.178 | 82-214-143-178.itsa.net.pl. | 422.02 Kb/s | 334.17 MB | 334.14 MB | 6.66 % | 2.44 % | 322.94 MB | 2.14 MB | 699,424 | 349,711.875 |
| | | | | | 95.128.91.229 | cust-95-128-91-229.breedbanddelft.nl. | 2.92 Mb/s | 350.01 MB | 350.01 MB | 4.47 % | | 337.86 MB | 1.45 KB | 9,877 | 9,877.413 |
| | | | ssh | MGT | 172.19.11.196 | mgt-dvt-temp.mgt.mmpds.compa | 2.16 Kb/s | 1.70 MB | | | | | | | |

## 3.2 FTP SUMMARY SHOWS TRANSFERS OF LONGEST DURATION

The files downloaded by this client take a relatively long time: 6 of the top-10 longest files transfers during the 3.5 hours!



TRAFMON FTP summary report

Start time : 2017-07-10 11:32:00
End time : 2017-07-10 15:02:59

FTP GET Statistics

Top 10 client IP by payload size




Largest files by payload

| Filename | Payload size |
|---|---|
| EN1_OPDE_ASA_IM__0P_20040201T044135_20040201T044517_010050_0477_20040201T050917.ZIP | 2,130,893,592 |
| L1B_Current_20150804-20150804.tar | 1,266,010,880 |
| test-austF.tgz | 944,512,380 |
| test-euroF.tgz | 879,330,713 |
| test-pacfF.tgz | 850,264,501 |
| CS_OFFL_SIR1SAR_FR_20151022T130300_20151022T131209_C001.TGZ | 504,844,338 |
| CS_OFFL_SIR1SAR_FR_20151025T134919_20151025T135839_C001.TGZ | 500,159,183 |
| CS_OFFL_SIR1SAR_FR_20151028T093836_20151028T094734_C001.TGZ | 485,425,663 |
| CS_OFFL_SIR1SAR_FR_20151027T120815_20151027T121718_C001.TGZ | 478,262,198 |
| CS_OFFL_SIR1SAR_FR_20151029T120556_20151029T121453_C001.TGZ | 455,465,764 |

FTP PUT Statistics

Top 10 client IP by payload size




Largest files by payload

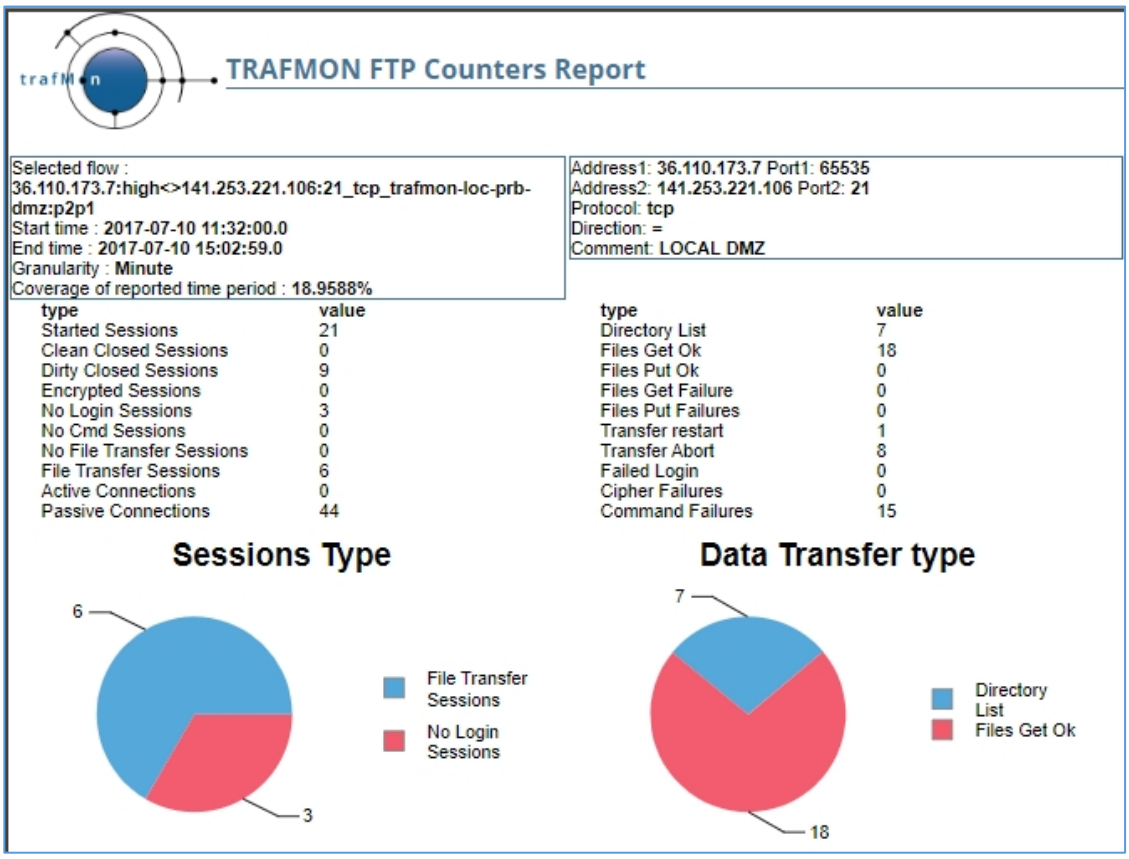
| Filename | Payload size |
|---|---|
| DDR_PLO_1PNPDE20081222_172523_00000348207 4_00499_35623_6872.zip | 1,314,756,512 |
| DDR_PLO_1PNPDE20081222_172523_00000190207 4_00499_35623_6784.zip | 1,299,887,531 |
| DDR_PLO_1PNPDE20081222_002758_00000152207 4_00489_35613_5517.zip | 512,283,691 |
| DDR_PLO_1PNPDE20081225_021401_00000134207 5_00032_35657_0027.zip | 510,215,356 |
| /from_MADRID/__MSS_OPER_MIR_SCNF1C_20170710T104144_20170710T122347_620_001_8.zip | 443,252,997 |
| /from_MADRID/__johnjohn_20170710_123330_20170710_140416_mss_40394_t_20170710_145928_l1c.bufr | 440,555,948 |
| /from_MADRID/__johnjohn_20170710_095415_20170710_104147_mss_40393_t_20170710_133434_l1c.bufr | 379,529,404 |
| DDR_PLO_1PNPDE20081222_172934_00000982074_00499_35623_6785.zip | 374,098,504 |
| /from_MADRID/__MSS_OPER_MIR_SCSF1C_20170710T041026_20170710T050339_620_001_1.zip | 346,662,954 |
| /from_MADRID/__MSS_OPER_MIR_SCSF1C_20170710T055029_20170710T064344_620_001_1.zip | 339,551,096 |

Longest file transfers

| Client IP | Server IP | Direction | Duration (sec) | Payload size | Username |
|---|---|---|---|---|---|
| 36.110.173.7 | 141.253.221.106 | GET | 5174 | 125,650,441 | repository |
| 36.110.173.7 | 141.253.221.106 | GET | 5154 | 130,518,160 | repository |
| 36.110.173.7 | 141.253.221.106 | GET | 5112 | 134,087,942 | repository |
| 36.110.173.7 | 141.253.221.106 | GET | 3707 | 198,100,100 | repository |
| 37.186.230.66 | 141.253.221.112 | GET | 3289 | 2,130,893,592 | userdata |
| 36.110.173.7 | 141.253.221.106 | GET | 2647 | 122,456,684 | repository |
| 36.110.173.7 | 141.253.221.106 | GET | 1788 | 84,882,982 | repository |
| 144.76.12.254 | 141.253.221.91 | GET | 1637 | 350,496,837 | carterpm |
| 144.76.12.254 | 141.253.221.91 | GET | 1549 | 294,035,657 | carterpm |
| 144.76.12.254 | 141.253.221.91 | GET | 1264 | 208,355,414 | carterpm |

## 3.3 FTP COUNTERS REPORT SHOWS ABORTS AND RESTART

When looking at the FTP Counters for the bi-directional data flow, we see that it incurs 8 FTP Aborts and 1 FTP Restart!



TRAFMON FTP Counters Report

Selected flow :
**36.110.173.7:high<>141.253.221.106:21_tcp_trafmon-loc-prb-dmz:p2p1**
Start time : **2017-07-10 11:32:00.0**
End time : **2017-07-10 15:02:59.0**
Granularity : **Minute**
Coverage of reported time period : **18.9588%**

Address1: **36.110.173.7** Port1: **65535**
Address2: **141.253.221.106** Port2: **21**
Protocol: **tcp**
Direction: **=**
Comment: **LOCAL DMZ**

| type | value |
|---|---|
| Started Sessions | 21 |
| Clean Closed Sessions | 0 |
| Dirty Closed Sessions | 9 |
| Encrypted Sessions | 0 |
| No Login Sessions | 3 |
| No Cmd Sessions | 0 |
| No File Transfer Sessions | 0 |
| File Transfer Sessions | 6 |
| Active Connections | 0 |
| Passive Connections | 44 |

| type | value |
|---|---|
| Directory List | 7 |
| Files Get Ok | 18 |
| Files Put Ok | 0 |
| Files Get Failure | 0 |
| Files Put Failures | 0 |
| Transfer restart | 1 |
| Transfer Abort | 8 |
| Failed Login | 0 |
| Cipher Failures | 0 |
| Command Failures | 15 |

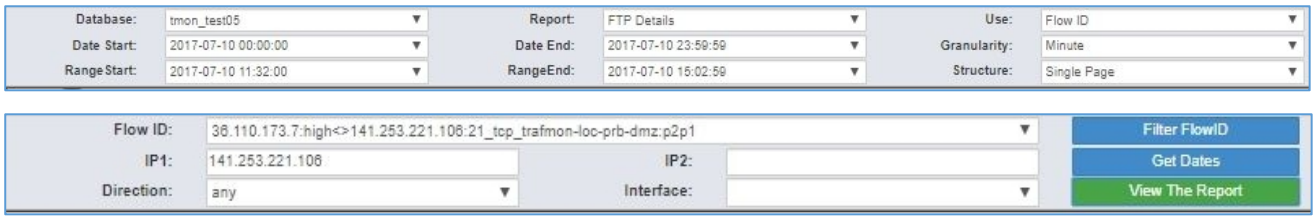
Sessions Type



Data Transfer type

## 3.4 LOOKING AT INDIVIDUAL FILE TRANSFERS – FTP DETAILS

Now, we can look at the individual file transfers for this client on that period of time:




It shows that the user "*repository*" has fetched, at '***2017-07-10 11:40:01***', the file "*SWB_FAC_MICE_20140504.cdf*" as part of its multi-file transfer session that started at '*2017-07-10 11:31:06*'; the file size has been announced to be 12 452 608 bytes and the TCP payload actually sent was 12 755 020 bytes (implying TCP retransmissions).

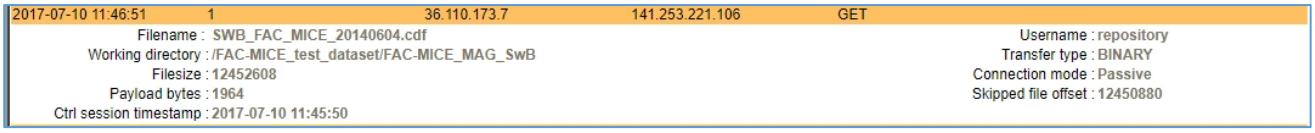
TRAFMON FTP details Report

Selected flow : 36.110.173.7:high<->141.253.221.106:21_tcp_trafmon-loc-prb-dmz:p2p1
Start time : 2017-07-10 11:32:00
End time : 2017-07-10 15:02:59

Address1: 36.110.173.7 Port1: 65535
Address2: 141.253.221.106 Port2: 21
Protocol: tcp
Direction: =
Comment: LOCAL DMZ

| First seen time | Transfer duration | Client IP | Server IP | File direction |
|---|---|---|---|---|
| 2017-07-10 11:32:23 | 241 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140422.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12886001<br>Ctrl session timestamp : 2017-07-10 11:31:06 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:33:04 | 3707 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140428_50.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 595217920<br>Payload bytes : 158100100<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:33:25 | 208 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140428.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12253440<br>Payload bytes : 12693358<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:33:45 | 194 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140504.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12742548<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:36:25 | 216 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140510.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12843655<br>Ctrl session timestamp : 2017-07-10 11:31:06 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:36:54 | 222 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140517.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12748285<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:37:00 | 155 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140529.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12252416<br>Payload bytes : 12542586<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:40:01 | 287 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140604.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12755020<br>Ctrl session timestamp : 2017-07-10 11:31:06 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:40:37 | 180 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140610.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12672234<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:43:38 | 287 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140617.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12745977<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:46:51 | 1 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140604.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 1964<br>Ctrl session timestamp : 2017-07-10 11:45:50 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 12450880 |
| 2017-07-10 11:46:53 | 264 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140711.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12862011<br>Ctrl session timestamp : 2017-07-10 11:45:50 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |
| 2017-07-10 11:48:26 | 233 | 36.110.173.7 | 141.253.221.106 | GET |
| Filename : $WB_FAC_MICE_20140730.cdf<br>Working directory : /FAC-MICE_test_dataset/FAC-MICE_MAG_$wB<br>Filesize : 12452608<br>Payload bytes : 12653070<br>Ctrl session timestamp : 2017-07-10 11:32:22 | | | | Username : repository<br>Transfer type : BINARY<br>Connection mode : Passive<br>Skipped file offset : 0 |

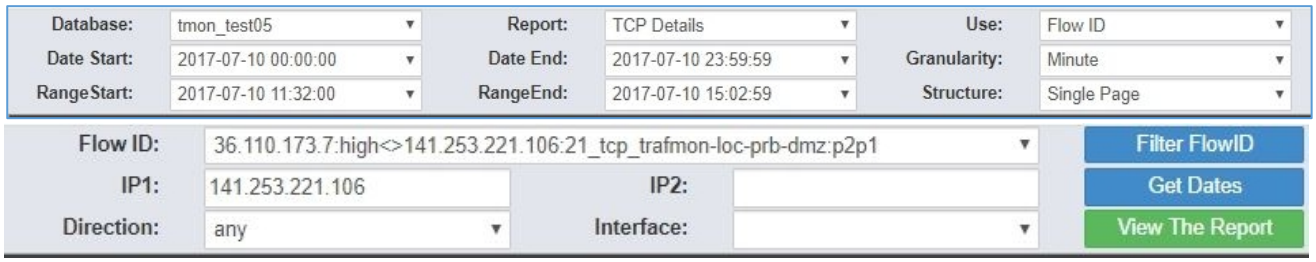
This wasn't apparently fully successful, because at "***2017-07-10 11:40:01***" the transfer of the same data file has been **restarted** at offset of 12 450 880 bytes – during a new session started at "*2017-07-10 11:45:50*" and commanding, thereafter, subsequent transfers of other files – resulting in a transfer of **1964 bytes**,




## 3.5 LOOKING AT INDIVIDUAL FILE TRANSFER CONNECTIONS – TCP DETAILS

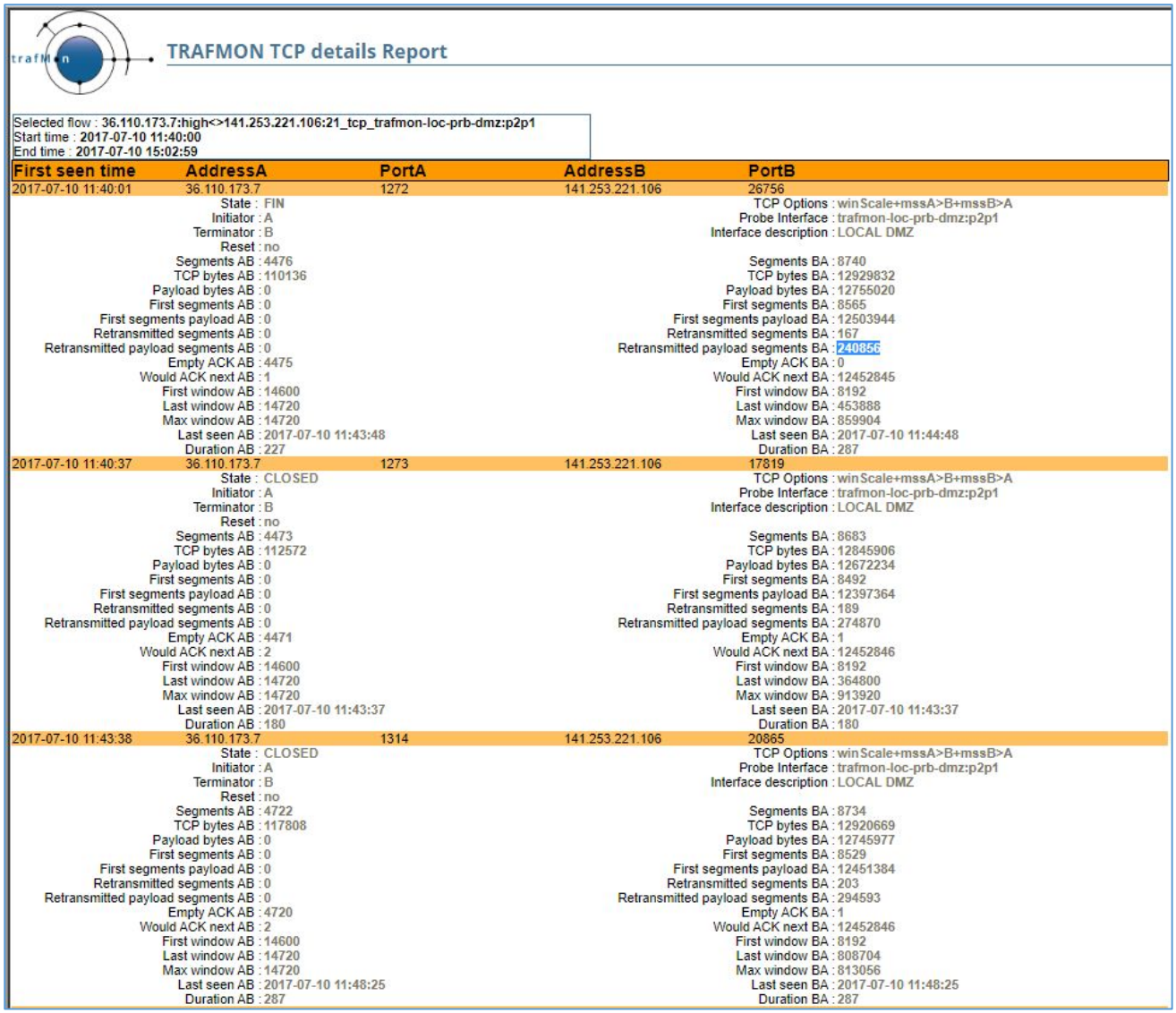
Now, we can analyse what has happened during those two corresponding TCP data connections, supporting the first and re-started transfers of the subject data file.

- We ask for the report on TCP Details covering the same FTP data flow from 11:32 until 15:03 on that day (2017-07-10):



- And we see that the first attempt to transfer the file has resulted in a non-negligible amount of retransmitted TCP segments and, consequently, the TCP window size has been significantly reduced compared to the maximum reached during the TCP connection lifetime.

  This does not only happen for the transfer of this data file, but also for the other (subsequent) TCP connections transferring other data files:

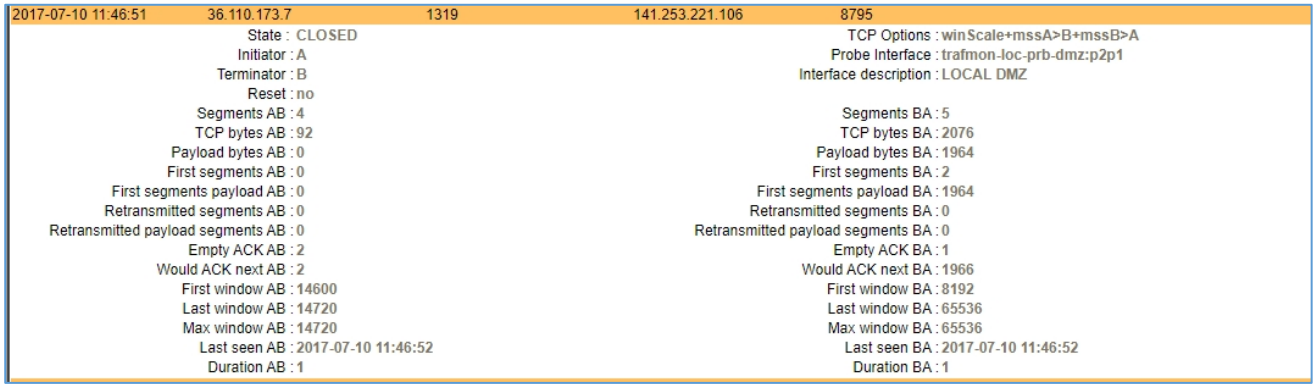


TRAFMON TCP details Report

Selected flow : 36.110.173.7:high<>141.253.221.106:21_tcp_trafmon-loc-prb-dmz:p2p1
Start time : 2017-07-10 11:40:00
End time : 2017-07-10 15:02:59

| First seen time | AddressA | PortA | AddressB | PortB |
|---|---|---|---|---|
| 2017-07-10 11:40:01 | 36.110.173.7 | 1272 | 141.253.221.106 | 26756 |
| State : FIN | | | TCP Options : winScale+mssA>B+mssB>A | |
| Initiator : A | | | Probe Interface : trafmon-loc-prb-dmz:p2p1 | |
| Terminator : B | | | Interface description : LOCAL DMZ | |
| Reset : no | | | | |
| Segments AB : 4476 | | | Segments BA : 8740 | |
| TCP bytes AB : 110136 | | | TCP bytes BA : 12929832 | |
| Payload bytes AB : 0 | | | Payload bytes BA : 12755020 | |
| First segments AB : 0 | | | First segments BA : 8565 | |
| First segments payload AB : 0 | | | First segments payload BA : 12503944 | |
| Retransmitted segments AB : 0 | | | Retransmitted segments BA : 167 | |
| Retransmitted payload segments AB : 0 | | | Retransmitted payload segments BA : 240856 | |
| Empty ACK AB : 4475 | | | Empty ACK BA : 0 | |
| Would ACK next AB : 1 | | | Would ACK next BA : 12452845 | |
| First window AB : 14600 | | | First window BA : 8192 | |
| Last window AB : 14720 | | | Last window BA : 453888 | |
| Max window AB : 14720 | | | Max window BA : 859904 | |
| Last seen AB : 2017-07-10 11:43:48 | | | Last seen BA : 2017-07-10 11:44:48 | |
| Duration AB : 227 | | | Duration BA : 287 | |
| 2017-07-10 11:40:37 | 36.110.173.7 | 1273 | 141.253.221.106 | 17819 |
| State : CLOSED | | | TCP Options : winScale+mssA>B+mssB>A | |
| Initiator : A | | | Probe Interface : trafmon-loc-prb-dmz:p2p1 | |
| Terminator : B | | | Interface description : LOCAL DMZ | |
| Reset : no | | | | |
| Segments AB : 4473 | | | Segments BA : 8683 | |
| TCP bytes AB : 112572 | | | TCP bytes BA : 12845906 | |
| Payload bytes AB : 0 | | | Payload bytes BA : 12672234 | |
| First segments AB : 0 | | | First segments BA : 8492 | |
| First segments payload AB : 0 | | | First segments payload BA : 12397364 | |
| Retransmitted segments AB : 0 | | | Retransmitted segments BA : 189 | |
| Retransmitted payload segments AB : 0 | | | Retransmitted payload segments BA : 274870 | |
| Empty ACK AB : 4471 | | | Empty ACK BA : 1 | |
| Would ACK next AB : 2 | | | Would ACK next BA : 12452846 | |
| First window AB : 14600 | | | First window BA : 8192 | |
| Last window AB : 14720 | | | Last window BA : 364800 | |
| Max window AB : 14720 | | | Max window BA : 913920 | |
| Last seen AB : 2017-07-10 11:43:37 | | | Last seen BA : 2017-07-10 11:43:37 | |
| Duration AB : 180 | | | Duration BA : 180 | |
| 2017-07-10 11:43:38 | 36.110.173.7 | 1314 | 141.253.221.106 | 20865 |
| State : CLOSED | | | TCP Options : winScale+mssA>B+mssB>A | |
| Initiator : A | | | Probe Interface : trafmon-loc-prb-dmz:p2p1 | |
| Terminator : B | | | Interface description : LOCAL DMZ | |
| Reset : no | | | | |
| Segments AB : 4722 | | | Segments BA : 8734 | |
| TCP bytes AB : 117808 | | | TCP bytes BA : 12920669 | |
| Payload bytes AB : 0 | | | Payload bytes BA : 12745977 | |
| First segments AB : 0 | | | First segments BA : 8529 | |
| First segments payload AB : 0 | | | First segments payload BA : 12451384 | |
| Retransmitted segments AB : 0 | | | Retransmitted segments BA : 203 | |
| Retransmitted payload segments AB : 0 | | | Retransmitted payload segments BA : 294593 | |
| Empty ACK AB : 4720 | | | Empty ACK BA : 1 | |
| Would ACK next AB : 2 | | | Would ACK next BA : 12452846 | |
| First window AB : 14600 | | | First window BA : 8192 | |
| Last window AB : 14720 | | | Last window BA : 808704 | |
| Max window AB : 14720 | | | Max window BA : 813056 | |
| Last seen AB : 2017-07-10 11:48:25 | | | Last seen BA : 2017-07-10 11:48:25 | |
| Duration AB : 287 | | | Duration BA : 287 | |

- Although, for the re-started transfer at '2017-07-10 11:46:51', the volume was small enough to avoid any retransmission, so that the last window size is equal to the maximum reached:



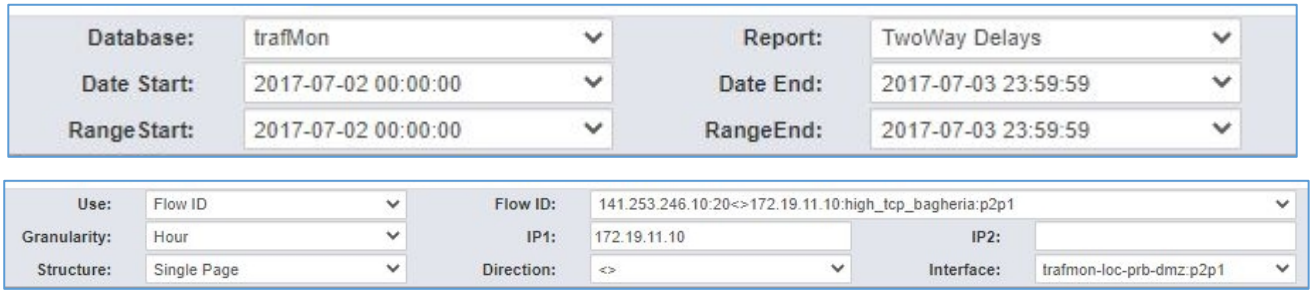
| 2017-07-10 11:46:51 | 36.110.173.7 | 1319 | 141.253.221.106 | 8795 |
|---|---|---|---|---|
| State : CLOSED | | | TCP Options : winScale+mssA>B+mssB>A | |
| Initiator : A | | | Probe Interface : trafmon-loc-prb-dmz:p2p1 | |
| Terminator : B | | | Interface description : LOCAL DMZ | |
| Reset : no | | | | |
| Segments AB : 4 | | | Segments BA : 5 | |
| TCP bytes AB : 92 | | | TCP bytes BA : 2076 | |
| Payload bytes AB : 0 | | | Payload bytes BA : 1964 | |
| First segments AB : 0 | | | First segments BA : 2 | |
| First segments payload AB : 0 | | | First segments payload BA : 1964 | |
| Retransmitted segments AB : 0 | | | Retransmitted segments BA : 0 | |
| Retransmitted payload segments AB : 0 | | | Retransmitted payload segments BA : 0 | |
| Empty ACK AB : 2 | | | Empty ACK BA : 1 | |
| Would ACK next AB : 2 | | | Would ACK next BA : 1966 | |
| First window AB : 14600 | | | First window BA : 8192 | |
| Last window AB : 14720 | | | Last window BA : 65536 | |
| Max window AB : 14720 | | | Max window BA : 65536 | |
| Last seen AB : 2017-07-10 11:46:52 | | | Last seen BA : 2017-07-10 11:46:52 | |
| Duration AB : 1 | | | Duration BA : 1 | |

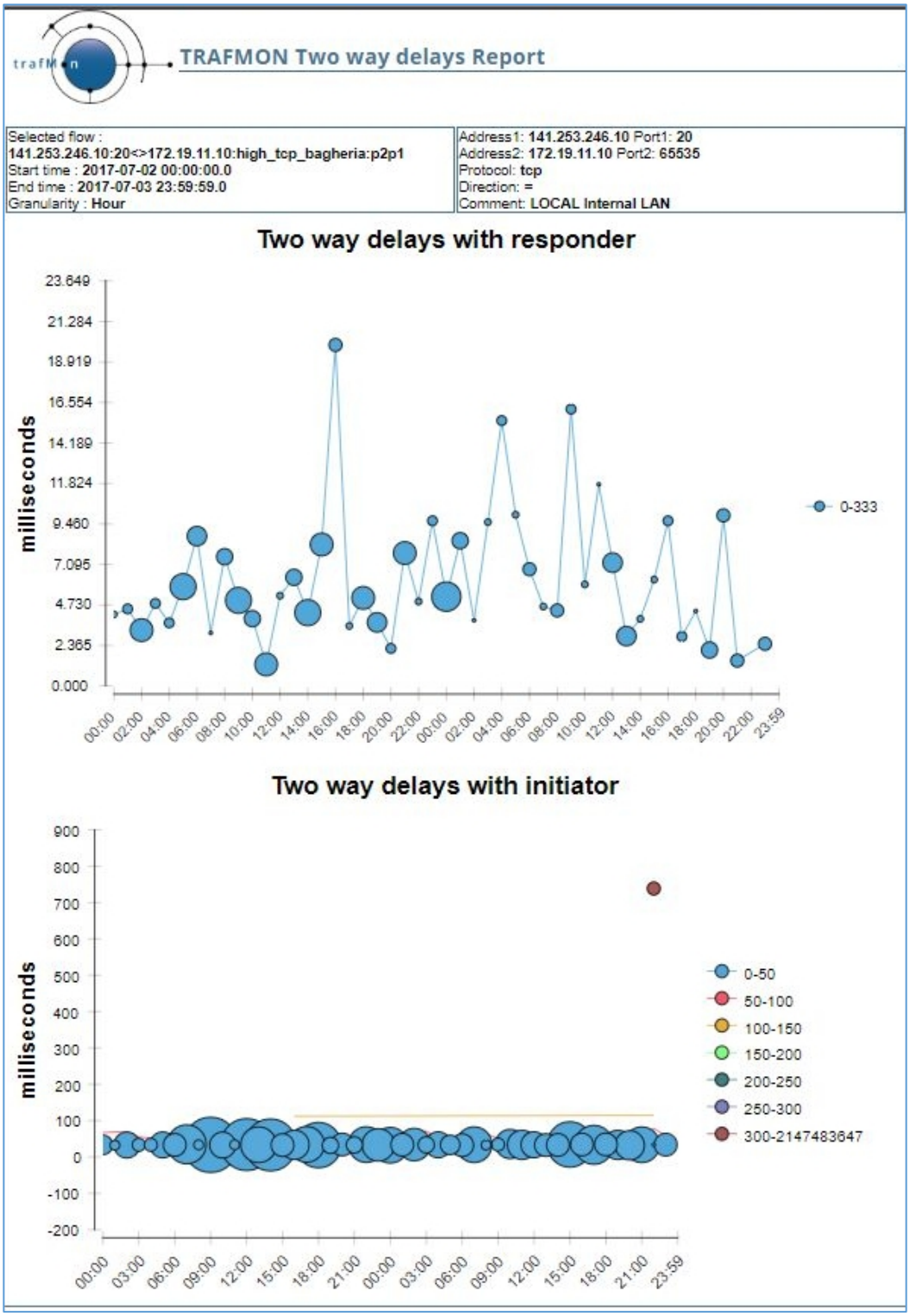
# 4. ABNORMAL INCREASE IN DELAYS AND PACKET LOSSES

## 4.1 DETECTING SLOWDOWN IN TWO-WAY DELAYS

By inspecting two-way delays with a remote private site, we look at the delays with one of our private address: 172.19.11.10. This is a FTP client that conducts file transfers in active mode based on server-side TCP port 20.

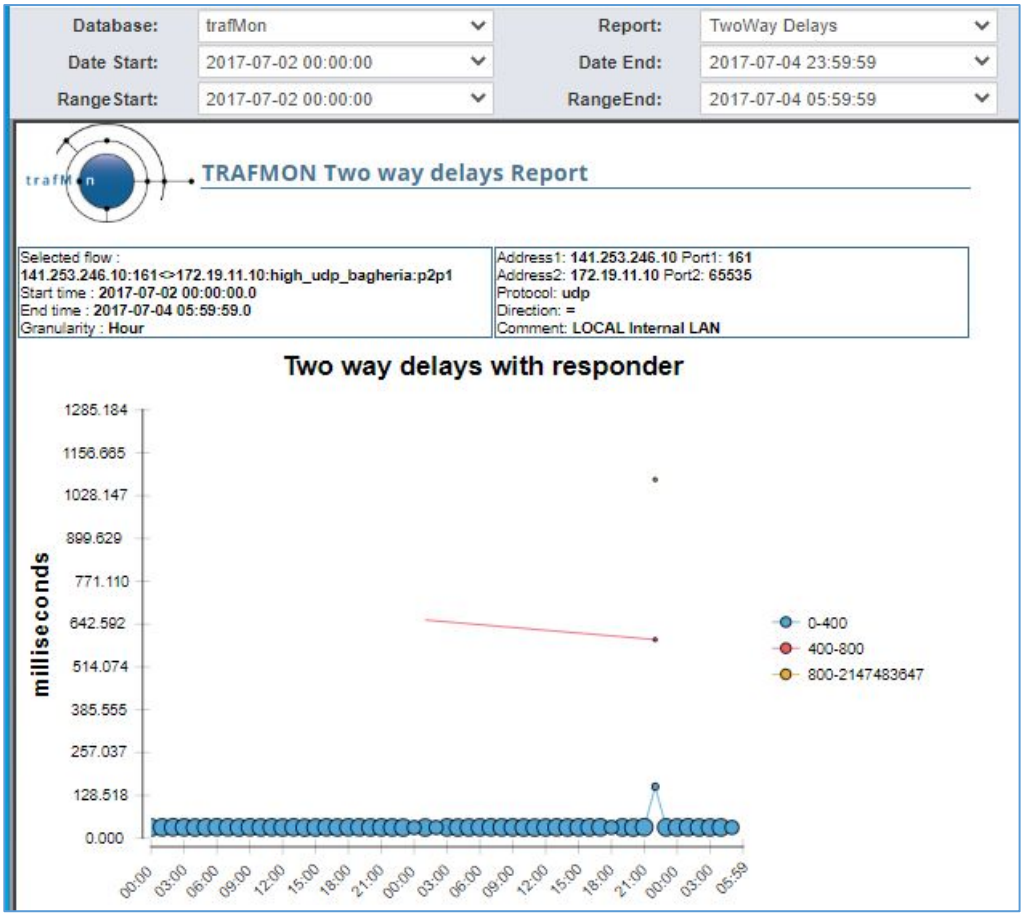
The **delay with** the local server is meaningless, but that with the remote client, acting as FTP data connection **initiator**, shows a surprising short **jump** in delays on '2017-07-03' **around 21:00 – 22:00**.




TRAFMON Two way delays Report
Selected flow :
141.253.246.10:20<>172.19.11.10:high_tcp_bagheria:p2p1
Start time : 2017-07-02 00:00:00.0
End time : 2017-07-03 23:59:59.0
Granularity : Hour
Address1: 141.253.246.10 Port1: 20
Address2: 172.19.11.10 Port2: 65535
Protocol: tcp
Direction: =
Comment: LOCAL Internal LAN
Two way delays with responder
milliseconds
23.649
21.284
18.919
16.554
14.189
11.824
9.460
7.095
4.730
2.365
0.000
0-333
Two way delays with initiator
milliseconds
900
800
700
600
500
400
300
200
100
0
-100
-200
0-50
50-100
100-150
150-200
200-250
250-300
300-2147483647

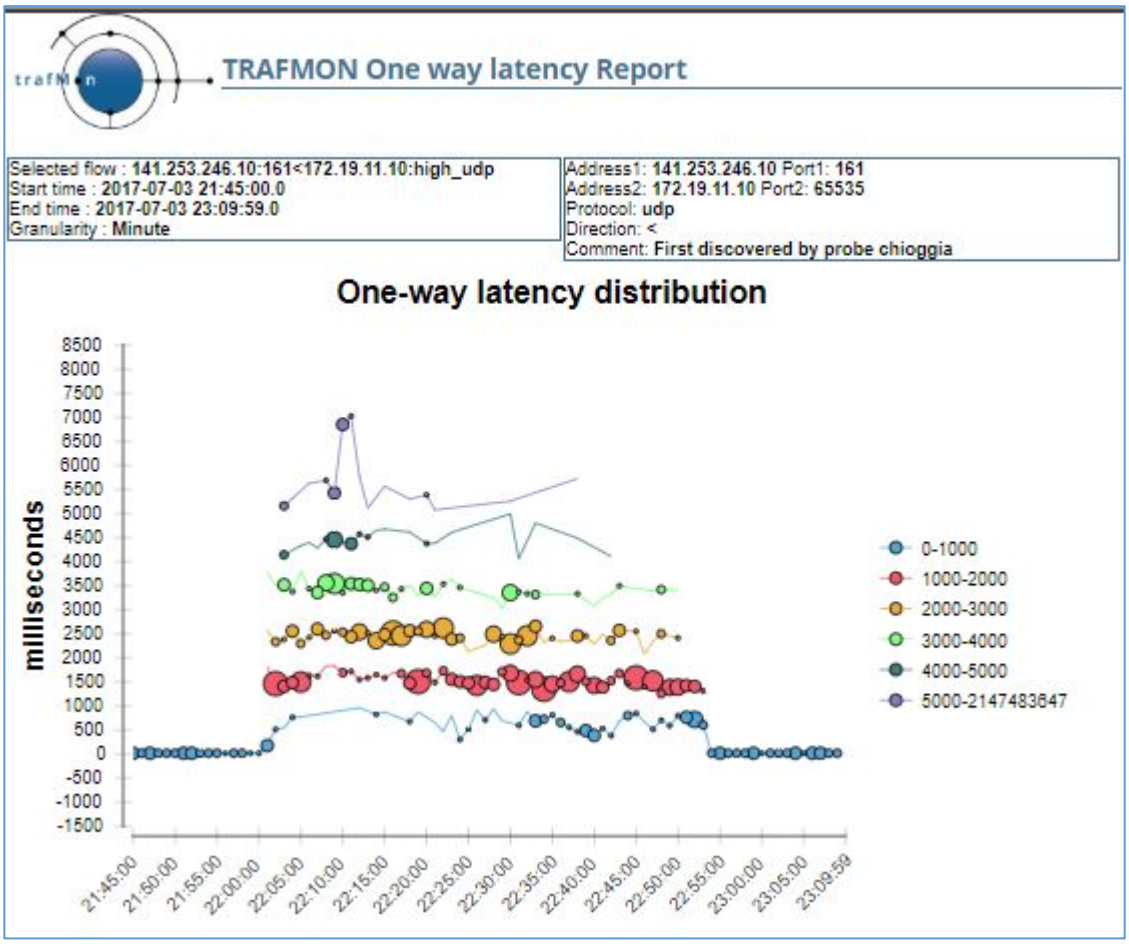
Fortunately, we are also monitoring this remote system through regular SNMP polling: regular SNMP get request/response pairs with IDP port 161.

So, we look at the two-way delays of the corresponding SNMP flow. And we observe a similar slowdown in the same time frame.

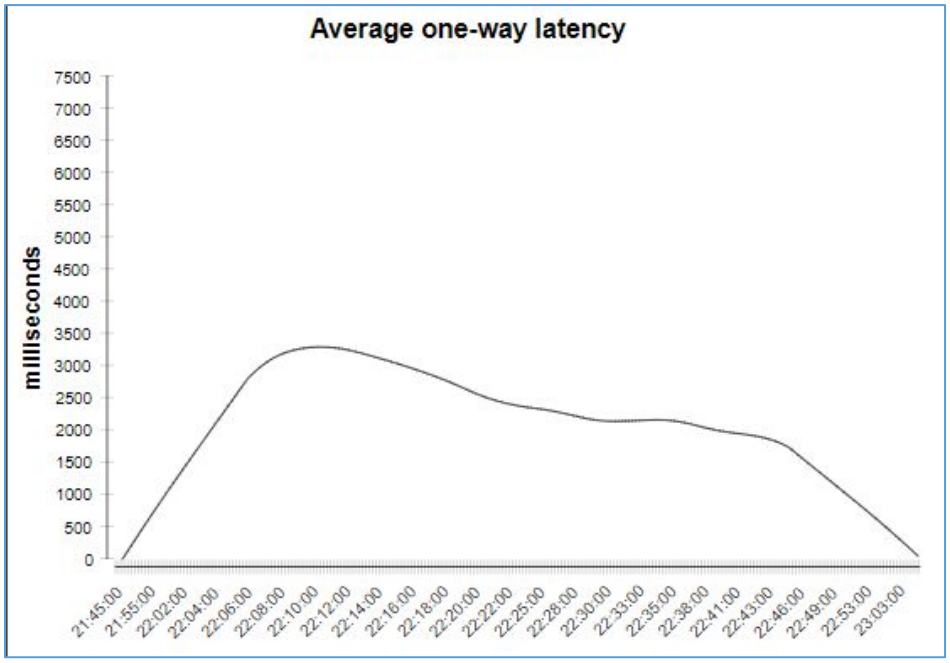


## 4.2 ANALYSING SLOWDOWN IN ONE-WAY LATENCY

By having installed another trafMon probe at our remote site, and having configured the one-way monitoring of this low volume SNMP data flow, we can further investigate the traffic abnormality.



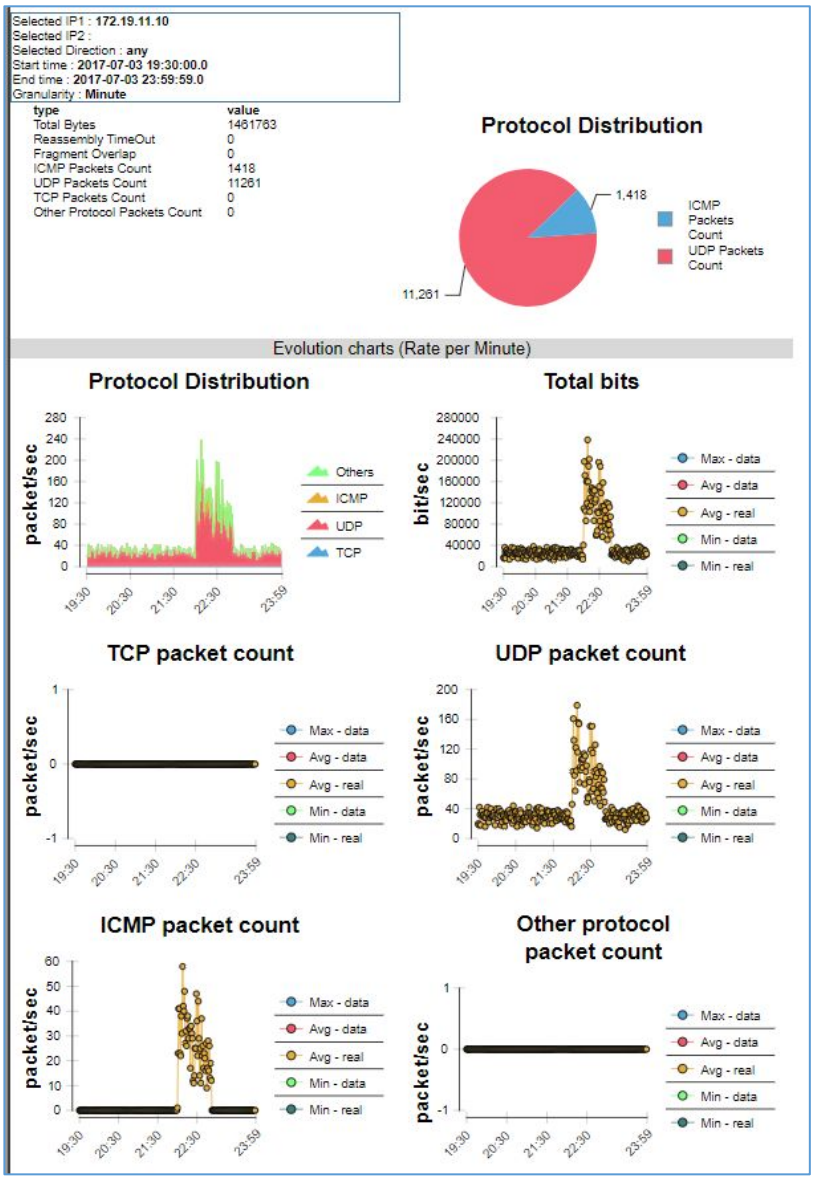
We see that the slowdown is really an abnormality compared to the 15 millisecond constant latency. But we can also see that the average and distribution of latency are quickly increased as is the number of packets, and that they slowly diminish, more or less in conjunction with the decrease of packets (look at the cumulated size of the bubbles and in the table of values).




| Date/Time | Observed packets | Latency |
|---|---|---|
| Jul 3, 2017, 9:45 PM | 19 | 15.26 |
| Jul 3, 2017, 9:46 PM | 12 | 15.42 |
| Jul 3, 2017, 9:47 PM | 16 | 15.25 |
| Jul 3, 2017, 9:48 PM | 14 | 15.14 |
| Jul 3, 2017, 9:49 PM | 14 | 15.36 |
| Jul 3, 2017, 9:50 PM | 11 | 15.18 |
| Jul 3, 2017, 9:51 PM | 17 | 15.24 |
| Jul 3, 2017, 9:52 PM | 17 | 15.35 |
| Jul 3, 2017, 9:53 PM | 13 | 15.31 |
| Jul 3, 2017, 9:54 PM | 15 | 15.20 |
| Jul 3, 2017, 9:55 PM | 14 | 15.21 |
| Jul 3, 2017, 9:56 PM | 9 | 15.33 |
| Jul 3, 2017, 9:57 PM | 13 | 15.31 |
| Jul 3, 2017, 9:58 PM | 14 | 15.29 |
| Jul 3, 2017, 9:59 PM | 10 | 15.10 |
| Jul 3, 2017, 10:00 PM | 10 | 15.70 |
| Jul 3, 2017, 10:01 PM | 28 | 705.96 |
| Jul 3, 2017, 10:02 PM | 57 | 1613.74 |
| Jul 3, 2017, 10:03 PM | 74 | 3241.84 |
| Jul 3, 2017, 10:04 PM | 53 | 1905.23 |
| Jul 3, 2017, 10:05 PM | 52 | 1839.13 |
| Jul 3, 2017, 10:06 PM | 27 | 2688.15 |
| Jul 3, 2017, 10:07 PM | 52 | 2816.17 |
| Jul 3, 2017, 10:08 PM | 57 | 3752.70 |
| Jul 3, 2017, 10:09 PM | 80 | 4031.39 |
| Jul 3, 2017, 10:10 PM | 57 | 3891.02 |
| Jul 3, 2017, 10:11 PM | 78 | 3550.03 |
| Jul 3, 2017, 10:12 PM | 61 | 3064.08 |
| Jul 3, 2017, 10:13 PM | 42 | 3226.05 |
| Jul 3, 2017, 10:14 PM | 47 | 2369.62 |
| Jul 3, 2017, 10:15 PM | 45 | 2848.22 |
| Jul 3, 2017, 10:16 PM | 54 | 2660.19 |
| Jul 3, 2017, 10:17 PM | 52 | 2433.81 |
| Jul 3, 2017, 10:18 PM | 47 | 2239.49 |
| Jul 3, 2017, 10:19 PM | 55 | 1918.93 |
| Jul 3, 2017, 10:20 PM | 68 | 3127.81 |
| Jul 3, 2017, 10:21 PM | 27 | 2531.81 |
| Jul 3, 2017, 10:22 PM | 53 | 2532.19 |
| Jul 3, 2017, 10:23 PM | 43 | 2039.21 |
| Jul 3, 2017, 10:24 PM | 43 | 1827.07 |
| Jul 3, 2017, 10:25 PM | 26 | 1278.50 |
| Jul 3, 2017, 10:26 PM | 32 | 1345.50 |
| Jul 3, 2017, 10:27 PM | 30 | 1279.87 |
| Jul 3, 2017, 10:28 PM | 43 | 2094.16 |
| Jul 3, 2017, 10:29 PM | 27 | 1909.85 |
| Jul 3, 2017, 10:30 PM | 83 | 2644.06 |
| Jul 3, 2017, 10:31 PM | 58 | 1799.71 |
| Jul 3, 2017, 10:32 PM | 47 | 2381.43 |
| Jul 3, 2017, 10:33 PM | 72 | 1925.14 |
| Jul 3, 2017, 10:34 PM | 52 | 1185.12 |
| Jul 3, 2017, 10:35 PM | 40 | 1401.80 |
| Jul 3, 2017, 10:36 PM | 35 | 1247.60 |
| Jul 3, 2017, 10:37 PM | 37 | 1343.78 |
| Jul 3, 2017, 10:38 PM | 64 | 2131.05 |
| Jul 3, 2017, 10:39 PM | 39 | 1282.92 |
| Jul 3, 2017, 10:40 PM | 49 | 1155.10 |
| Jul 3, 2017, 10:41 PM | 35 | 1406.57 |
| Jul 3, 2017, 10:42 PM | 37 | 1762.03 |
| Jul 3, 2017, 10:43 PM | 41 | 2279.66 |
| Jul 3, 2017, 10:44 PM | 22 | 1101.50 |
| Jul 3, 2017, 10:45 PM | 48 | 1581.42 |
| Jul 3, 2017, 10:46 PM | 14 | 1331.57 |
| Jul 3, 2017, 10:47 PM | 39 | 1497.41 |
| Jul 3, 2017, 10:48 PM | 46 | 2208.28 |
| Jul 3, 2017, 10:49 PM | 32 | 1211.47 |
| Jul 3, 2017, 10:50 PM | 43 | 1502.07 |
| Jul 3, 2017, 10:51 PM | 34 | 1112.03 |
| Jul 3, 2017, 10:52 PM | 44 | 1028.73 |
| Jul 3, 2017, 10:53 PM | 20 | 850.15 |
| Jul 3, 2017, 10:54 PM | 12 | 15.42 |
| Jul 3, 2017, 10:55 PM | 19 | 15.63 |
| Jul 3, 2017, 10:56 PM | 14 | 15.93 |
| Jul 3, 2017, 10:57 PM | 14 | 15.86 |
| Jul 3, 2017, 10:58 PM | 12 | 15.67 |
| Jul 3, 2017, 10:59 PM | 19 | 15.58 |
| Jul 3, 2017, 11:00 PM | 10 | 15.50 |
| Jul 3, 2017, 11:01 PM | 11 | 15.73 |
| Jul 3, 2017, 11:02 PM | 14 | 15.71 |
| Jul 3, 2017, 11:03 PM | 15 | 15.67 |
| Jul 3, 2017, 11:04 PM | 20 | 15.70 |
| Jul 3, 2017, 11:05 PM | 9 | 15.56 |
| Jul 3, 2017, 11:06 PM | 20 | 15.70 |
| Jul 3, 2017, 11:07 PM | 18 | 15.72 |
| Jul 3, 2017, 11:08 PM | 14 | 15.57 |
| Jul 3, 2017, 11:09 PM | 12 | 15.58 |

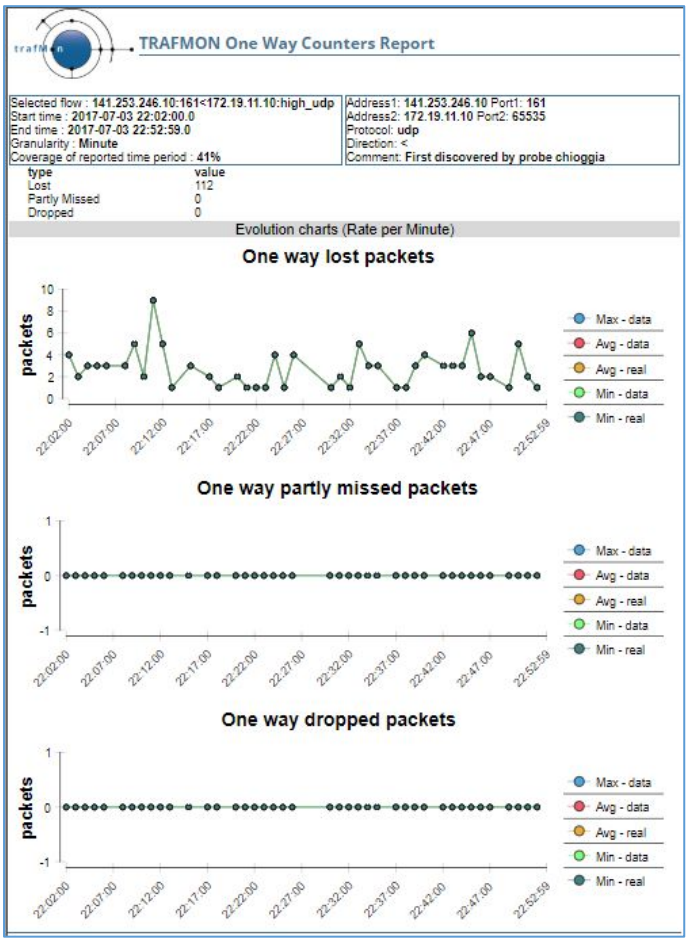
## 4.3 IP COUNTERS CONFIRM THE TRAFFIC BURST

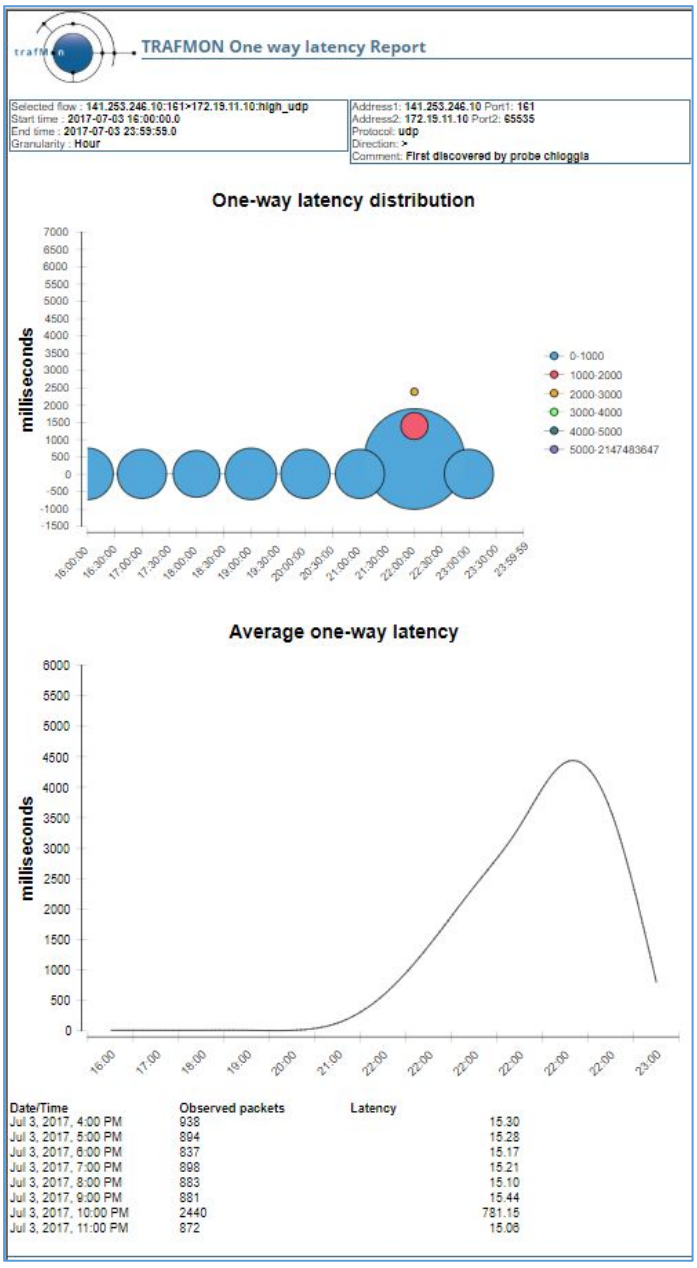
When looking at the IP Counters of the traffic with the concerned remote host, locally seen at the side of the SNMP manager, we get the confirmation of the sudden traffic burst, which is accompanied with frequent ICMP errors.



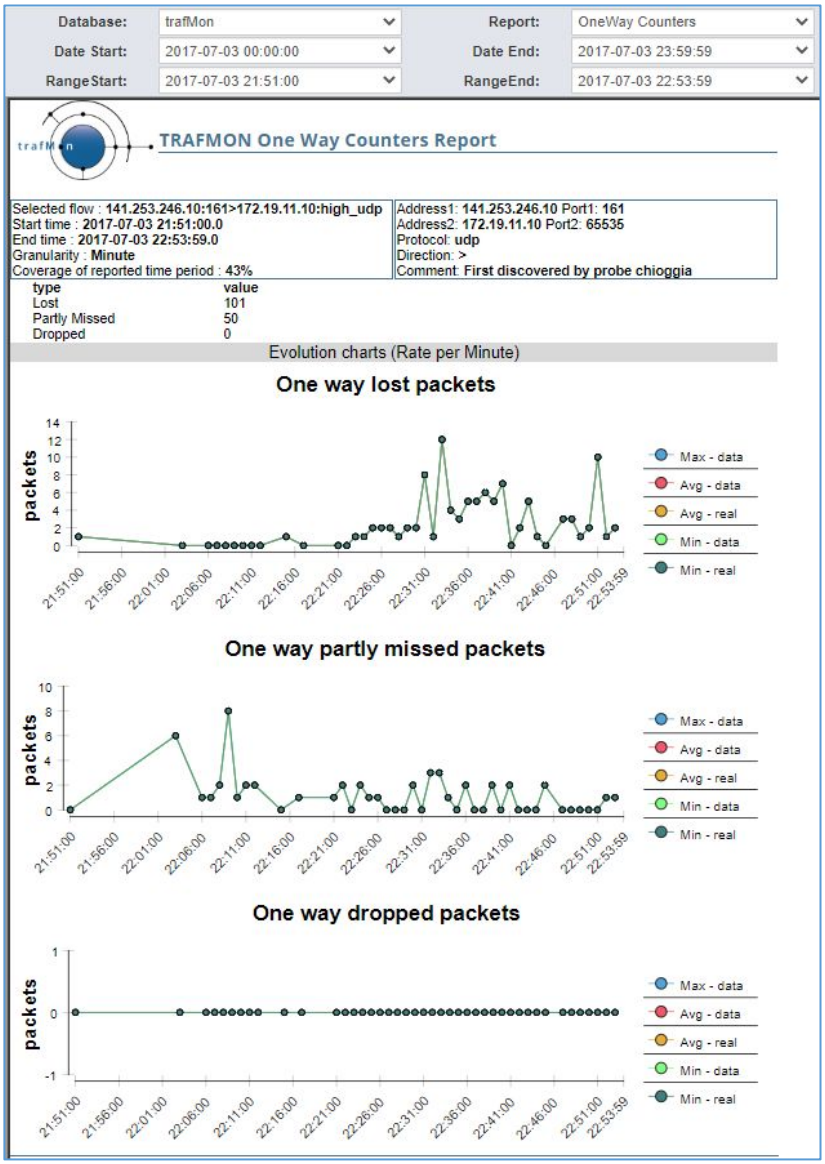
# 4.4 ONE-WAY COUNTERS REVEAL PACKET LOSSES

The latency analysis concludes to a network path saturation due to traffic increase. And the associated one-way counters show that this slowdown is accompanied with occurrences of **packet losses** in the manager-to-agent direction of the SNMP data flow.



In the reverse direction, the slowdown is also clearly visible in the latency report.




But, more surprisingly, few packets are detected at destination side while not seen at their source: one way **missed packets.**

## 4.5 TRAFMON PROCESSING EVENTS ARE KEPT WITH THE DATABASE OBSERVATIONS

Because we know that the cause is a bursty increase in packets, we look at the events published by the probe (named chioggia) at the agent source side, where packets have been missed. Maybe the packet capture buffer was overflowing, in which case the probe would have reported an event.

In order to let you participate to the continuous building of the tool, we haven't implemented ourselves any BIRT report that shows the event log. So, we go to query the MySQL the database directly: for instance, though the installation and use of the *phpMyAdmin* open source utility.

**SELECT * FROM `trafMon`.`eventtable` WHERE `time` BETWEEN '2017-07-03 21:00:00' AND '2017-07-03 23:10:00'**

```
SELECT *
FROM `eventtable`
WHERE `time`
BETWEEN '2017-07-03 21:00:00'
AND '2017-07-03 23:10:00'
```

Profiling [ Inline ] [ Edit ] [ Expl

Show : Start row: 0 Number of rows: 30 Headers every 100 rows

Sort by key: None

+ Options

| | time | type | severity | entity | probeInterface | flowName | eventMessage |
|---|---|---|---|---|---|---|---|
| Edit Copy Delete | 2017-07-03 21:01:28 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 48%) |
| Edit Copy Delete | 2017-07-03 21:02:56 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 41%) |
| Edit Copy Delete | 2017-07-03 21:02:57 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 48%) |
| Edit Copy Delete | 2017-07-03 21:26:04 | nominal | normal | trafmon-loc-prb-dmz | NULL | NULL | probe is back at nominal load: 41%) |
| Edit Copy Delete | 2017-07-03 21:28:57 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 45%) |
| Edit Copy Delete | 2017-07-03 21:48:46 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 41%) |
| Edit Copy Delete | 2017-07-03 21:51:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 1 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 21:53:42 | full speed | minor | voghera | NULL | NULL | probe is working at full speed (load 100%) |
| Edit Copy Delete | 2017-07-03 21:53:43 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 48%) |
| Edit Copy Delete | 2017-07-03 21:54:57 | nominal | normal | voghera | NULL | NULL | probe is back at nominal load: 44%) |
| Edit Copy Delete | 2017-07-03 22:02:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 4 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:03:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:04:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 3 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:05:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 3 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:06:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 3 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:07:00 | partial packet obs. | major | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 1 incomplete 1-way packet obs during 60s s... |
| Edit Copy Delete | 2017-07-03 22:08:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 3 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:09:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 5 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:10:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:11:00 | partial packet obs. | major | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 incomplete 1-way packet obs during 60s s... |
| Edit Copy Delete | 2017-07-03 22:12:00 | partial packet obs. | major | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 incomplete 1-way packet obs during 60s s... |
| Edit Copy Delete | 2017-07-03 22:13:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 1 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:15:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 3 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:17:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:18:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 1 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:20:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:21:00 | partial packet obs. | major | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 1 incomplete 1-way packet obs during 60s s... |
| Edit Copy Delete | 2017-07-03 22:22:00 | partial packet obs. | major | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 incomplete 1-way packet obs during 60s s... |
| Edit Copy Delete | 2017-07-03 22:23:00 | packet(s) lost | minor | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 1 1-way lost packet(s) during 60s since 03... |
| Edit Copy Delete | 2017-07-03 22:24:00 | partial packet obs. | major | rho | NULL | 141.253.246.10:161>172.19.11.10:high_udp | counted 2 incomplete 1-way packet obs during 60s s... |

In fact, we see the trafMon collector (*rho*) mentioning the lost and incomplete (missed) packets, but no message from the concerned probe about its load level or the saturation of its capture buffer**.**

Hence, this means that the missed packets are due to the saturation, upon burst of traffic, at the mirror port of the switch to which the probe is connected.

# 5. RELEVANT CONFIGURATION TUNING

One XML configuration file, common to all distributed trafMon probes, and to the central trafMon collectors, defines what observations to collect from the monitored traffic.

## 5.1 PACKET COUNTERS (INCLUDING ICMP ERRORS)

The below excerpt of configuration file produces all protocol packet counters about IPv4, ICMP and the UDP or TCP transport protocols.

```
  <GranularFlow name="uniDirAtProbeIf" >
    <DistinctIf /> <!-- mandatory when Counters, to avoid double records -->
    <DistinctAddr field="srcdst" />
    <DistinctPort field="portpair" portspec="privileged" />
    <GroupBy      field="ipproto"/>
  </GranularFlow>

  <!-- ALL Unidirectional packets (for volumes counting)
       ================================================
  -->
  <FlowClass id="200" name="ALL_packets"
                                    descr="ALL Unidirectional IP Fragments">
    <Measure interval="1min" >
      <Stats verifChksum="bestEffort">
        <PacketCounters for="allFragments"/>
      </Stats>
    </Measure>
    <FlowGrain ref="uniDirAtProbeIf" />
    <Filter>
      <On probe="trafMon-probe" if="p1p1" />
      <On probe="trafMon-probe" if="p1p2" />
      <PacketExpr>
        <AND>
            <Predicate field="src" op="betw"
                                    value="0.0.0.1" value2="255.255.255.254" />
            <Predicate field="dst" op="betw"
                                    value="0.0.0.1" value2="255.255.255.254" />
        </AND>
      </PacketExpr>
    </Filter>
  </FlowClass>
```

## 5.2 FTP AND TCP COUNTERS AND DETAILS

To measure the complete FTP session exchanges and the associated data transfers, including the stateful follow-on of underlying control and data TCP connections (**ftpdata="full"**), the following must be configured:

```
  <GranularFlow name="protoConversAtProbeIf" >
    <DistinctIf /> <!-- mandatory when Counters, to avoid double records -->
    <DistinctAddr field="addrpair" />
    <DistinctPort field="portpair" portspec="privileged" />
    <GroupBy      field="ipproto"/>
  </GranularFlow>

  <!-- FTP: TCP port 21
       ================
  -->
  <FlowClass id="21" name="FTP_port21" descr="TCP with port==21">
    <Measure interval="1min" >
      <Stats verifChksum="bestEffort">
        <PacketCounters for="firstFragment"/>
                        <!-- Don't ask for Dgram for TCP to avoid unnecessary
                             keeping of subsequent frags (of other flows)
                             between same IP address pair -->
        <TCPConnections granularity="each"/>
        <FileTransfers  protocol="FTP" granularity="each"
                        ftpdata="full"/>
      </Stats>
    </Measure>
    <FlowGrain ref="protoConversAtProbeIf" />
    <Filter>
      <On probe="voghera" if="eth0" />
      <On probe="bagheria" if="eth0" />
      <On probe="chioggia" if="eth0" />
      <On probe="chiavari" if="eth0" />
      <PacketExpr>
        <AND>
          <Predicate field="proto" op="eq" value="tcp"/>
          <Predicate field="port"  op="eq" value="21"/>
        </AND>
      </PacketExpr>
    </Filter>
  </FlowClass>
```

## 5.3 DELAY OBSERVATIONS: ROUND-TRIP AND ONE-WAY

In order to measure the two-way delays over TCP connections, following configuration should be specified:

```
<GranularFlow name="protoConversAtProbeIf" >
  <DistinctIf /> <!-- mandatory when Counters, to avoid double records -->
  <DistinctAddr field="addrpair" />
  <DistinctPort field="portpair" portspec="privileged" />
  <GroupBy      field="ipproto"/>
</GranularFlow>

<!-- Round trip delay measurement for TCP-RTTM
-->
<FlowClass id="8888" name="TCP-RTTM-RoundTrip-histo"
  descr="TCP RTTM Timestamps aggregated delay">
  <Measure interval="10s" >
    <Delay for="firstFragment" granularity="probeAggregated">
      <RoundTripDelay protocol="tcpOptRTTM" with="both" />
      <Histogram lowBound="0" highBound="300" sliceCount="8" />
    </Delay>
  </Measure>
  <FlowGrain ref="protoConversAtProbeIf" />
  <Filter>
    <On probe="bagheria" if="eth0" />
    <On probe="chiavari" if="eth0" />
    <PacketExpr>
      <AND>
        <Predicate field="proto" op="eq" value="tcp"/>
      </AND>
    </PacketExpr>
  </Filter>
</FlowClass>
```

In order to also measure the two-way delays of UDP/SNMP transactions, following configuration should be specified:

```
<!-- Round trip delay measurement for SNMP
-->
<FlowClass id="5555" name="SNMP-RoundTrip-histo"
  descr="SNMP Req/Rsp aggregated delay">
  <Measure interval="10s" >
    <Delay for="firstFragment" granularity="probeAggregated">
      <RoundTripDelay protocol="udpSNMP" />
      <Histogram lowBound="0" highBound="800" sliceCount="4" />
```

```
      </Delay>
    </Measure>
    <FlowGrain ref="protoConversAtProbeIf" />
    <Filter>
      <On probe="bagheria" if="eth0" />
      <PacketExpr>
        <AND>
          <Predicate field="proto" op="eq" value="udp"/>
          <Predicate field="port"  op="eq" value="161"/>
        </AND>
      </PacketExpr>
    </Filter>
  </FlowClass>
```

In order to measure one-way latency and to detect packet losses (or missed packets), the trafMon XML configuration should encompass the following type of measurements:

```
  <GranularFlow name="perProtoServicePort" >
    <DistinctAddr field="srcdst" />
    <DistinctPort field="portpair" portspec="privileged" />
    <GroupBy      field="ipproto"/>
  </GranularFlow>

  <!-- One-way Delay and Packet Loss on SNMP: LOCAL INT <> REMOTE DMZ
       ============================================================
       Request: SNMP from LOCAL INT to REMOTE DMZ
       ++++++++++++++++++++++++++++++++++++++++++
  -->
  <FlowClass id="1111" name="One-Way_SNMP_Requests"
    descr="SNMP Requests one-way aggregated delay and loss/partial counters">
    <Measure interval="1min" >
      <Delay for="allFragments" granularity="collectorAggregated">
        <OneWayDelay from="locint_rq" to="remdmz_rq" lost="count" >
          <Hop name="locint_rq"/>
          <Hop name="remdmz_rq"/>
          <Sign/>
        </OneWayDelay>
        <Histogram lowBound="0" highBound="5000" sliceCount="7" />
      </Delay>
    </Measure>
    <FlowGrain ref="perProtoServicePort" />
    <Filter>
      <On probe="bagheria" if="eth0" />
      <CaptureTimeStamp           hopName="locint_rq"/>
      <PacketExpr>
        <AND>
          <Predicate field="proto" op="eq" value="udp"/>
          <Predicate field="dport" op="eq" value="161"/>
          <Predicate field="dst"   op="eq" value="&remdmz1;"/>
        </AND>
```

```
      </PacketExpr>
    </Filter>
    <Filter>
      <On probe="chioggia" if="eth0" />
      <CaptureTimeStamp           hopName="remdmz_rq"/>
      <PacketExpr>
        <AND>
          <Predicate field="proto" op="eq" value="udp"/>
          <Predicate field="dport" op="eq" value="161"/>
          <Predicate field="dst"   op="eq" value="&remdmz1;"/>
        </AND>
      </PacketExpr>
    </Filter>
  </FlowClass>
  <!-- Response: SNMP from REMOTE DMZ to LOCAL INT
       ++++++++++++++++++++++++++++++++++++++++++
  -->
  <FlowClass id="2222" name="One-Way_SNMP_Responses"
    descr="SNMP Responses one-way aggregated delay and loss/partial counters">
    <Measure interval="1min" >
      <Delay for="allFragments" granularity="collectorAggregated">
        <OneWayDelay from="remdmz_rs" to="locint_rs" lost="count" >
          <Hop name="remdmz_rs"/>
          <Hop name="locint_rs"/>
          <Sign/>
        </OneWayDelay>
        <Histogram lowBound="0" highBound="5000" sliceCount="7" />
      </Delay>
    </Measure>
    <FlowGrain ref="perProtoServicePort" />
    <Filter>
      <On probe="chioggia" if="eth0" />
      <CaptureTimeStamp           hopName="remdmz_rs"/>
      <PacketExpr>
        <AND>
          <Predicate field="proto" op="eq" value="udp"/>
          <Predicate field="sport" op="eq" value="161"/>
          <Predicate field="dst"   op="eq" value="&locint1;"/>
        </AND>
      </PacketExpr>
    </Filter>
    <Filter>
      <On probe="bagheria" if="eth0" />
      <CaptureTimeStamp           hopName="locint_rs"/>
      <PacketExpr>
        <AND>
          <Predicate field="proto" op="eq" value="udp"/>
          <Predicate field="sport" op="eq" value="161"/>
          <Predicate field="dst"   op="eq" value="&locint1;"/>
        </AND>
      </PacketExpr>
    </Filter>
  </FlowClass>
```

And the IP Counters are obtained as per the configuration in section 5.1 above.