

Journal Scientific and Applied Research, Vol. 30, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

INTERNET TRAFFIC ANALYSIS WITH QOS POLICY

Dimitar R. Iliev

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: dimitar25_8000@abv.bg

Abstract: *The present study presents an analysis of Internet traffic captured using Wireshark during a file download, before and after the application of a data prioritization condition. The condition is configured on a router through which the data traffic passes to the client device - a desktop computer. The main objective is to examine the quantitative characteristics of the recorded traffic and to compare individual groups of data using statistical indicators and numerical relationships. The analysis covers the total number of packets, capture duration, volume of transferred data, average packet size, packet rate, average bitrate, protocol structure, dominant communication flows. The results show that the examined data consist almost entirely of TCP-based Internet traffic and a single primary secure client–server communication session. At the same time, differences are observed in terms of the temporal concentration of traffic, and the average intensity of the exchange. The results from the comparison aim to assist the analysis of the effect from prioritizing Internet traffic to a specific device, achieved through a Quality of Service algorithm, with the aim of improving transmission efficiency.*

Key words: *Wireshark, Pcapng, Network traffic analysis, TCP/IP (Transmission Control Protocol/Internet Protocol), Statistical processing, Comparative analysis, Quality of Service (QoS), Traffic prioritization.*

1. Introduction

Network traffic analysis is an essential component in the study of modern computer networks, as it enables both diagnostic monitoring of communication processes and a quantitative description of data exchange between network nodes. In the context of the increasing complexity of internet services and the growing requirements for security, reliability, and efficiency of communication infrastructure, the interpretation of real network traffic has become increasingly important [1, 3, 5, 9].

Wireshark is a tool for capturing and analyzing network packets. It allows captured traffic to be stored in the .pcapng format, which contains detailed information about each packet - arrival time, size, protocol affiliation, source, destination, and transport parameters. These data can be considered a basis for statistical and mathematical analysis.

The present study aims to combine the results from the analysis of four .pcapng files and to provide a unified academic interpretation of their quantitative parameters. In addition to the individual mathematical analysis of each file, a comparative evaluation between them is also performed.

2. Experiment

Fig. 1 shows two computers that are connected to a router which has five Gigabit ports - one WAN (Wide Area Netwrok) port for the Internet connection and four ports for end devices. Two computers, PC1(Personal Computer) and PC2, are connected to two of the router's ports. Both end devices simultaneously download a file of 287 MB from the Internet via HTTP/HTTPS (Hypertext Transfer Protocol). First, the file is downloaded without enabling QoS, after which the download is repeated with QoS configured to prioritize the traffic to and from PC2. During the experiment, communication relies primarily on TCP to ensure reliability, guaranteeing that the data arrives without errors and in the correct order. UDP (User Datagram Protocol) is not used, since in the event of packet loss TCP enables retransmission of the lost data (error correction), whereas this mechanism is not available in UDP. [2, 8, 14, 18]

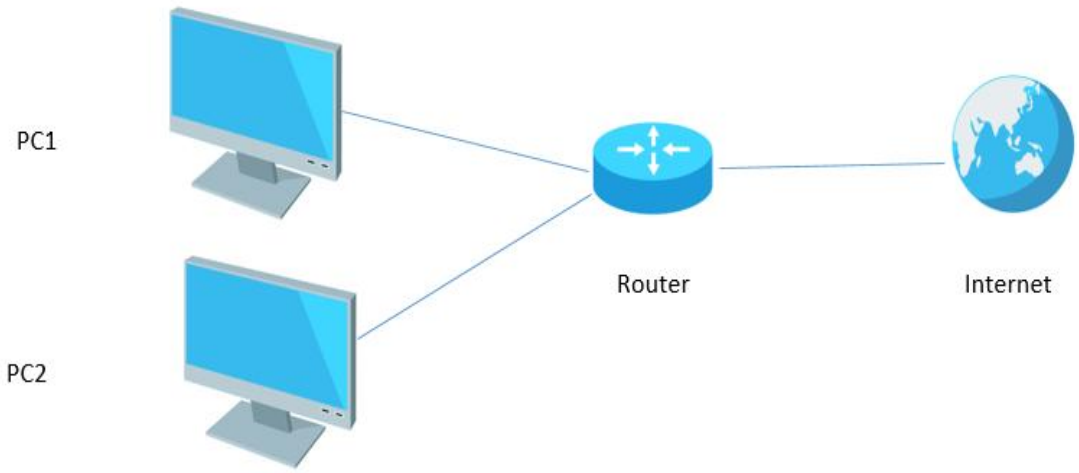


Fig. 1. Topology

- Steps in the data transmission:

TCP Handshake (Three - way handshake): Before the actual file download begins, a reliable TCP connection is established through the exchange of SYN (Synchronize), SYN-ACK, and ACK(Acknowledgment) packets. An example of this is Fig. 2.

```
TCP        66 59573 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
TCP        66 443 → 59573 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PER
TCP        54 59573 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
TLSv1.2   283 Client Hello (SNI=self.events.data.microsoft.com)
```

Fig. 2. Real packets during the data capture

HTTP Request: The client sends an HTTP GET request for the file, as shown in Fig. 3. Since HTTP operates over TCP, this request is encapsulated in TCP segments.

Source	Destination	Protocol	Length	Info
192.168.0.177	2.22.113.123	HTTP	281	GET / HTTP/1.1

Fig. 3. GET request

Data Transfer (TCP - intensive): The server begins sending the file divided into small segments (TCP packets) with a size of 1514 bytes, so that they fit within the network's Maximum Transmission Unit (MTU). Most packets are TCP Data, carrying fragments of the file. The client returns TCP ACK packets to acknowledge each or several received segments as seen in Fig. 4.

```
TCP      1514 443 → 59573 [ACK] Seq=1 Ack=230 Win=4194304 Len=1460 [TCP PDU reassembled in 17]
TCP      1514 443 → 59573 [ACK] Seq=1461 Ack=230 Win=4194304 Len=1460 [TCP PDU reassembled in 17]
TCP      1514 443 → 59573 [ACK] Seq=2921 Ack=230 Win=4194304 Len=1460 [TCP PDU reassembled in 17]
TCP        54 59573 → 443 [ACK] Seq=230 Ack=4381 Win=262144 Len=0
TCP      1514 443 → 59573 [ACK] Seq=4381 Ack=230 Win=4194304 Len=1460 [TCP PDU reassembled in 17]
```

Fig. 4. TCP Data and TCP ACK

Connection termination: After the file has been downloaded, FIN(Finish) packets are sent to close the TCP session, shown in Fig. 5.

```
TCP      54 [TCP Retransmission] 59574 → 443 [FIN, ACK] Seq=2754 Ack=11422
```

Fig. 5. FIN packet

- Data capture:

The subject of the study consists of four files containing captured internet traffic: pc1noprio.pcapng, pc1prio2.pcapng, pc2nopri.pcapng, pc2prio2.pcapng. Each of them contains a record of real network communication captured within different time intervals, and a similar overall volume of registered data. The first two files represent data from the Ethernet interfaces of PC1 and PC2 during the file download without QoS, while the second two contain data from the same interfaces after QoS has been enabled for PC2.

- Metrics Used:

The mathematical metrics used are:

N— total number of packets;

T— capture duration;

B— total volume of captured packet data in bytes;

S_f—.pcapng file size;

$\bar{x}$— average packet size;

Me— median packet size;

n_k— number of packets of a given protocol;

- Mathematical Relationships Used:

The average number of packets per second is determined by:

$$\text{pps} = \frac{\text{N}}{\text{T}} \tag{1}$$

The average data transfer rate is calculated using the formula:

$$\text{R} = \frac{8\text{B}}{\text{T}} \tag{2}$$

where the factor 8 converts bytes into bits.

The average packet size is determined as:

$$\bar{x} = \frac{B}{N} \tag{3}$$

The relative share of a given protocol is determined by:

$$p = \frac{n_k}{N} \cdot 100 \tag{4}$$

The overhead of the .pcapng format is determined by:

$$O = S_f - B \tag{5}$$

and its relative share is:

$$O_r = \frac{S_f - B}{B} \cdot 100 \tag{6}$$

These relationships allow an objective comparison between the four captures. [4, 11, 17]

3. Results

-Overall quantitative profile of the captures:

- The analysis of four files in .pcapng format, representing captured data packets from Internet traffic in a local network, shows that the total volume of captured data is similar, while the duration of the recordings varies, and the number of packets is close in value across the four captures.
- The file pc1noprio.pcapng contains 319,103 packets with a total volume of 321,249,180 bytes and a duration of 178.856 s.
- The file pc1prio2.pcapng contains 312,988 packets with a total volume of 319,188,380 bytes and a duration of 560.194 s.
- The file pc2nopri.pcapng contains 348,018 packets with a total volume of 323,034,380 bytes and a duration of 220.132 s.
- The file pc2prio2.pcapng contains 347,145 packets with a total volume of 322,368,243 bytes and a duration of 162.018 s.

The volume of data is approximately the same in all cases, but it is distributed over different time intervals. This means that the differences between the files are not due to the amount of information, but to the intensity and organization of the data transfer.

-Mean data traffic intensity:

Average number of captured packets per second is:

pc1noprio.pcapng:

$$\frac{319103}{178.856} \approx 1784.12$$

pc1prio2.pcapng:

$$\frac{312988}{560.194} \approx 558.71$$

pc2nopri.pcapng:

$$\frac{348018}{220.132} \approx 1580.95$$

pc2prio2.pcapng:

$$\frac{347145}{162.018} \approx 2142.63$$

These values show that pc1prio2.pcapng has the lowest packet rate, while pc2prio2.pcapng has the highest. Therefore, the latter file describes the most time-concentrated network exchange.

-Average Data Transfer Rate:

pc1noprio.pcapng:

$$\frac{8 \cdot 321249180}{178.856949} \approx 14.37\ Mbit/s$$

pc1prio2.pcapng:

$$\frac{8 \cdot 319188380}{560.194} \approx 4.56\ Mbit/s$$

pc2nopri.pcapng:

$$\frac{8 \cdot 323034380}{220.132} \approx 11.74\ Mbit/s$$

pc2prio2.pcapng:

$$\frac{8 \cdot 322368243}{162.018} \approx 15.92\ Mbit/s$$

Once again, it is confirmed that pc2prio2.pcapng is the most intensive file in terms of data transfer rate.

-Data packet size analysis:

Average data packets size is:

pc1noprio.pcapng: 1006.73 bytes
pc1prio2.pcapng: 1019.81 bytes
pc2nopri.pcapng: 928.21 bytes
pc2prio2.pcapng: 928.63 bytes

In all four files, the median packet size is 1514 bytes. The comparison between the mean value and the median indicates that the distribution of packet sizes is asymmetric. The median is higher than the mean in all cases, which suggests the presence of a significant proportion of small packets that lower the arithmetic mean. Nevertheless, the main portion of the traffic consists of standard-sized packets, which is typical for the transmission of payload data.

-Protocol structure:

In all four files, the protocol analysis shows a predominance of IPv4 and TCP packets. The share of TCP packets is:

pc1noprio.pcapng: 99.77%
pc1prio2.pcapng: 99.55%
pc2nopri.pcapng: 99.77%
pc2prio2.pcapng: 99.85%

All recordings are practically entirely TCP-based, as expected during a file download. The share of UDP, ARP (Address Resolution Protocol), IPv6, and other auxiliary protocols is minimal and does not significantly affect the overall structure of the traffic.

-Analysis of Dominant Connections:

The four files represent one main TCP session, which encompasses almost all of the traffic:

In pc1noprio.pcapng the dominant traffic is between 207.241.227.92:443(Server) and 192.168.0.137:3138(IPv4 address of PC1).

In pc1prio2.pcapng — between 207.241.233.32:443 and 192.168.0.137:3495.

In pc2nopri.pcapng — between 204.62.247.172:443(Server) and 192.168.0.177:59302(IPv4 address of PC2).

In pc2prio2.pcapng — between 204.62.247.172:443 and 192.168.0.177:59575.

In all four cases, communication is carried out through port 443, which is commonly used in the secure Internet traffic of the HTTPS/TLS (Transport Layer Security) type. This is an additional indicator that all recordings describe a communication process of a similar nature.

-Comparative Analysis:

All recordings share an almost identical overall profile: a similar total volume of transferred data, nearly complete dominance of IPv4/TCP, a large proportion of packets with a size of approximately 1514 bytes, and a clear concentration around a single secure TCP connection. This allows the conclusion that all files describe the same general class of internet communication—mass data transfer from a remote server to a local client.

There are substantial differences between the files in terms of the temporal concentration of traffic. The longest capture is pc1prio2.pcapng, which explains its lowest packet rate and lowest average bitrate—a direct result of the prioritization of data intended for PC2. This recording reflects the reduction in the amount of data transferred per unit time during the file download on PC1, in contrast to the increase in the data rate toward PC2, indicating that the prioritization mechanism is functioning as intended. The capture pc2prio2.pcapng, which describes the packets of PC2 after QoS was enabled, combines a relatively short duration with a similar overall volume of data, resulting in the highest intensity of exchange.

Overall, pc2prio2.pcapng can be defined as the most intensive and most time-concentrated file.

-Discussion of the Prioritization Algorithm:

The comparative analysis of the files pc2nopri.pcapng and pc2prio2.pcapng shows that traffic prioritization has led to a significant improvement in transmission efficiency. This improvement is not achieved through an increase in the total volume of transferred data, but rather through a better temporal organization of their transmission.

In both files, the total volume of recorded packet data is almost identical. In pc2nopri.pcapng, it amounts to 323,034,380 bytes, while in pc2prio2.pcapng it is 322,368,243 bytes. The number of packets is also practically the same—348,018 in pc2nopri.pcapng and 347,145 in pc2prio2.pcapng. The average packet size remains nearly unchanged—928.21 bytes and 928.63 bytes, respectively. These facts indicate that the nature and scale of the traffic itself have not changed significantly, since the same file size was downloaded in both cases.

The significant difference between the two captures is observed in the temporal parameters. The duration of the transfer decreases from 220.132 s in pc2nopri.pcapng to 162.018 s in pc2prio2.pcapng. The reduction is:

$$220.132 - 162.018 = 58.114\ s$$

As a relative share, this represents:

$$\frac{58.114}{220.132} \cdot 100 \approx 26.4\%$$

Therefore, in the case of prioritized traffic, the total transfer time is reduced by approximately 26.4%. At the same time, the average number of packets per second increases from 1580 pps to 2142 pps. The increase is:

$$2142 - 1580 = 562\ pps$$

and its relative expression is:

$$\frac{562}{1580} \cdot 100 \approx 35.5\%$$

A similar trend is observed in the average bitrate, which increases from 11.74 Mbit/s to 15.92 Mbit/s. The difference is:

$$15.92 - 11.74 = 4.18\ Mbit/s$$

or a relative increase of:

$$\frac{4.18}{11.74} \cdot 100 \approx 35.6\%$$

These results show that pc2prio2.pcapng achieves more efficient utilization of network bandwidth. Since the amount of data and the number of packets remain practically constant, the improvement in efficiency must be attributed to the mechanism used for packet handling. From a networking perspective, this is achieved through a Quality of Service (QoS) algorithm based on queue management. A traffic prioritization algorithm is used, in which packets from the higher-priority class gain faster access to the channel and spend less time waiting in buffers. The algorithm that enables this is Priority Queuing (PQ). The total transmission time can be considered as the sum of several components:

$$T = T_{tx} + T_{queue} + T_{proc} + T_{other}$$

where:
T_{tx} the pure time required for the physical transmission of the data;
$T_{queue}$the time spent waiting in network queues;
$T_{proc}$the processing time;
T_{other} summarizes the remaining delays;

Since the total volume of data in both files is almost identical, the component T_{tx} cannot explain the significant difference in the overall duration. Therefore, the reduction in total time is mainly due to a decrease in T_{queue}.In pc2prio2.pcapng, the packets were served with a shorter waiting time. This leads to a faster completion of the transfer and a higher effective throughput. The observed improvement is consistent with the logic of priority-based traffic management. In the absence of prioritization, the flow competes equally with other packets for access to the network resource. When prioritization is applied, however, traffic marked as more important is served earlier and more frequently, which reduces queue accumulation and increases transmission efficiency. This happens when the router handles a packet with a 6—bit DSCP (Differentiated Services Code Point) field with a value of 0x40, which is prioritized by the enabled QoS policy and the packets leave the queues first. Therefore, the comparison between pc2nopri.pcapng and pc2prio2.pcapng shows that the improved data transmission observed in pc2prio2.pcapng is the result of a QoS prioritization algorithm based on priority

queue management. The effect of this algorithm is expressed in a statistically significant reduction in transfer time, accompanied by an increase in packet rate and average bitrate.

This allows the conclusion that prioritization has led to a more efficient use of network resources and improved transmission quality. [6, 10, 13, 15]

4. Conclusion

The conducted comparative mathematical analysis of the four files containing captured internet traffic allows several general conclusions to be drawn.

First, all recordings describe a similar type of network communication, characterized by an almost complete dominance of the TCP protocol, a high concentration of large packets, and the presence of a single primary secure client–server connection that forms practically the entire volume of transferred data. This is a direct consequence of the file download process.

Second, despite the similar total volume of data, the four files differ significantly in terms of the temporal organization of the traffic. The highest intensity is observed in pc2prio2.pcapng, while the lowest intensity occurs in pc1prio2.pcapng.

Third, the comparison between pc2nopri.pcapng and pc2prio2.pcapng shows that traffic prioritization has led to a significant improvement in transmission efficiency. This improvement is expressed through a reduction in transfer time of approximately 26.4%, an increase in packet rate of about 35.5%, and a rise in the average bitrate of approximately 35.6%, without a substantial change in the total volume of data. On this basis, it can be concluded that the use of a QoS prioritization algorithm based on queue management has resulted in more efficient utilization of network resources and improved transmission quality. [7, 12, 16]

In conclusion, the four files can be considered different realizations of the same general type of internet traffic—mass data transfer, specifically the download of a file from a remote secure server to a local client, carried out through a strongly dominant TCP session, but with different degrees of temporal concentration.

References:

[1] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., Weiss, W., An Architecture for Differentiated Services. RFC 2475, Internet Engineering Task Force (IETF), 1998, p. 36.

[2] Demers, A., Keshav, S., Shenker, S., “Analysis and Simulation of a Fair Queueing Algorithm.” Proceedings of ACM SIGCOMM, 1989, pp. 1-12.

[3] Denev D., Tsankov Ts. Analyzing data and testing the single wire handover capabilities of category 8 cables. Proceedings of International Scientific Conference “Defense Technologies” DefTech 2022, ISSN 2367-7902, pp. 343-352.

[4] Denev D., Tsankov Ts. Design and Implementation of a Field Level of an Industrial Communication Network for the Needs of the Industry. 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2022), Ohrid, North Macedonia, ISBN 978-166548500-5.

[5] Denev D., Tsankov Ts. Development of a virtual private network in computer networks and communication environments. International scientific refereed online journal with impact factor SocioBrains, Issue 71, 2020, ISSN 2367-5721, pp. 11-19.

[6] Denev D. R., Tsankov Ts. Model of a terminal network device based on a single-chip microcontroller and Ethernet interface. Journal Scientific and Applied Research, vol. 22, 2022, ISSN 1314-6289, pp. 66-71.

[7] Floyd, S., Jacobson, V., “Random Early Detection Gateways for Congestion Avoidance.” IEEE/ACM Transactions on Networking, vol. 1, no. 4, 1993, pp. 397-413.
[8] Kurose, J. F., Ross, K. W., Computer Networking: A Top-Down Approach. 8th ed. Pearson, ISBN-13 978-0136681557, 2021, p. 864.
[9] Nichols, K., Blake, S., Baker, F., Black, D., Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474, Internet Engineering Task Force (IETF), 1998, p. 12.
[10] Nikolova S., Tsankov Ts. Intelligent resource management systems in computer networks. Annual of Konstantin Preslavsky University of Shumen, vol. XIV E, Faculty of technical sciences, 2024, ISSN 1314-8818, pp. 210-220, https://doi.org/10.46687/YT24SIS.
[11] Sanders, C., Practical Packet Analysis Using Wireshark to Solve Real-World Network Problems. 3rd ed. No Starch Press, ISBN-13 978-1593278021, 2017, p. 368.
[12] Stallings, W., Data and Computer Communications. 11th ed. Pearson, ISBN-13 978-0135182796, 2017, p. 880.
[13] Stevens, W. R., TCP/IP Illustrated, Volume 1: The Protocols. Addison-Wesley Professional, ISBN-13 978-0201633467, 1994, p. 600.
[14] Tanenbaum, A. S., Wetherall, D. J., Computer Networks. 5th ed. Pearson, ISBN-13 978-0132126953, 2011, p. 960.
[15] Tsankov Ts., Hatib I. Analyse network traffic and improve security with Wireshark and Cisco Packet Tracer. Annual of Konstantin Preslavsky University of Shumen, vol. XIV E, Faculty of technical sciences, 2024, ISSN 1314-8818, pp. 74-81, https://doi.org/10.46687/YT24CEC.
[16] Tsankov Ts., Staneva L., Vardeva I., Iliev D. Generalized net model of a communication network using the Port Knocking method. Scientific Conference with international participation MATTEH 2022, Conference proceeding, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 29-34.
[17] Uzun M. B., Atanasov V. T. Common conception of software-defined networks. Annual of Konstantin Preslavsky University of Shumen, vol. XIII E, 2023, pp. 112-119, ISSN 2815-4703 (online).
[18] Varghese, G., Network Algorithmics: An Interdisciplinary Approach to Designing Fast Networked Devices. Morgan Kaufmann, ISBN-13 978-0120884773, 2004, p. 512.