PRELIMINARY ORGANIZATION OF VIRTUAL NETWORK BASED ON PROGRAM MONITORING

Radi Romansky

Technical university – Sofia
Bulgaria

* Corresponding Author, e-mail: rrom@tu-sofia.bg

Abstract: Virtual Local Area Network (VLAN) is a logical organization of communication resources and objects for maintaining efficient information processes based on network traffic. It is known that in the contemporary global network, traffic can be generated from various physical sources, which requires preliminary analysis and adequate management with the provision of the necessary information security. In this aspect, the proposed paper presents an opportunity to analyse supported network traffic in a virtual network environment by using program monitoring. In the computer field, various products are offered for measurement of parameters of information processes, including network communications. In this sense, a preliminary review of the main features of network traffic was conducted and possible solutions for the organization of adequate program measurement of parameters of information processes were discussed.

Key words: virtual network, program monitoring, information processes, analysis.

1. INTRODUCTION

In modern computer networks, it is mandatory to analyse the supported communication traffic generated by active applications and users. Each active device in the network adds traffic elements that affect the overall load. A comprehensive traffic study is presented in [1], with a classification of the functional behaviour of the most common generators. An important issue for preliminary research when designing a network architecture is the level of performance, and particularly the preliminary calculation of the "end-to-end" delay. This should be done prior to the implementation of a proposed solution to ensure the required performance as stated in [2]. As highlighted in the paper, such analysis is particularly needed in real-time embedded systems and is considered key, proposing a model to calculate the expected average end-to-end delay for different abstraction layers of any network topology. Another approach to reduce the used routing resources in multi-channel wireless networks is presented in [3], where an efficient process simulation model is presented, and an algorithm is proposed to improve the network throughput. In this way, a reduction in failure rate and energy consumption during transmission is achieved compared to other algorithms. The problems related to

the algorithmizing processes is also presented in [4], where the subject of the discussion is an information management system for maintaining distributed services. A service optimization mechanism was studied under the analysis of organizational and economic constraints, with the aim of optimizing the processing of requests and increasing the overall performance.

The contemporary network world constantly poses topical problems to solve related to distributed information services. This necessitates conducting preliminary research to specify the intended results of the development of network structures by making an appropriate choice of software for networking, including simulation [5]. The choice of an appropriate research approach should depend on the set goal and the architectural characteristics of the object, one of the tasks being to increase the efficiency of routing [3], the study of information services in distributed environments [4], the characteristics of network processes, improving throughput and others.

Whether clustering is logically based on virtual computer networks or physical segmentation, the goal is to keep most of the network traffic between clients and servers on the local network segment. In network virtualization environments, fragmentation of resources and their isolation from others is often applied, and in [6] an approach is proposed to reduce the negative sides and an indicator "degree of resource fragmentation" is defined for its quantitative measurement.

Virtual Local Area Network (VLAN) is a mechanism for logical grouping of users, services, and network devices in local computer networks, as stated in [7], where a critical analysis of this type of networks is made and the advantages are systematized. One of them is that by creating multiple networks with a single IP address class and by restricting communication between VLANs, it is possible to allow or deny users access to a particular network. To ensure the effectiveness of the architectural design with a defined main goal, it is necessary to conduct a preliminary study of the information processes and analysis of the network traffic before the final implementation.

The purpose of the article is to present an opportunity to analyse network traffic in a virtual network environment using programmatic monitoring. For this purpose, some features of the network traffic were reviewed and possible solutions for measuring parameters of information processes were discussed.

2. AN OVERVIEW OF NETWORK TRAFFIC AND MONITORING MEANS

2.1. Features of network traffic

Modern computer networks generate diverse traffic, which requires correct identification to choose the correct management and security of network processes [8]. In this aspect, application of software tools for monitoring, registration and analysis of traffic and parameters of information processes is a suitable approach, ensuring adequacy of assessments. Using the right software can provide proper analysis, reconstruction and visualization of traffic and the behaviour of firewalls, routers, proxy servers and remote access servers. Analysing the collected data over time can show general trends, such as traffic growth, an increase in blocked connection attempts, attack attempts, etc. For example, in [8] the possibility of improving traffic identification using

samples is discussed from NetFlow data and investigating the impact of packet sampling on the accuracy of the applied identification method. Another research on traffic identification and anomaly detection is presented in [9], where "*an approach to improve the scalability of online machine learning-based network traffic analysis*" is proposed. The applied idea is to replace widely used supervised machine learning models for network traffic analysis with binary neural networks and their representation in NIC (N3IC), a system allowing to compile the model for direct integration in the data plane of SmartNICs.

Network traffic analysis is essential to ensure the required level of network security by allowing potentially dangerous communications links and possible anomalies to be identified. In general, it is not enough to only detect malicious links, but what is important is to determine which node is the generator of malicious traffic, as stated in [10]. This will allow appropriate actions to be taken to increase the cybersecurity of the system, and the paper proposes that the analysis of node behaviour be performed by using the graphical information encoded in a connection network with a triple approach:

✓ Applying temporal dissection to extract information, graphics-based.

✓ Introduction of two new techniques for graph data level preprocessing (R-hybrid and SM-hybrid).

✓ Using a neural network and two graph convolutional networks (GCNs) to classify the behaviour of nodes.

In a similar direction is the research discussed in [11] on the analysis of current methodologies for labelling network traffic data, with the authors indicating that in the field of network security this process is "*particularly challenging and costly*" because it needs very specialized knowledge to classify network traffic. As a result, they suggest using visual and statistical tools, as well as machine learning techniques.

The monitoring of network processes and the measurement of network traffic parameters are important components of network design and management, as the requirements are constantly being improved and as the latest developments in [12] are indicated "*sketch-based monitoring techniques and the deployment opportunities arising from the increasing programmability of network elements (e.g., programmable switches, SmartNICs, and software switches)*". However, the authors' conclusion is that, despite the diversity, many of the existing approaches are not practical and present HeteroSketch, a framework of two main components: (1) A profiling tool to automate the determination of the capabilities of a given tool through predictive; (2) A framework for optimization enabling the achievement of monitoring goals with analysis of the heterogeneous capabilities of devices. The growing interest in monitoring network processes is also confirmed in [13], discussing dynamic networks. The new methods, the authors claim, are mostly specialized for solving specific tasks in network management and are rarely compared with competing methods and suggest using simulation to compare the effectiveness of monitoring approaches and methods under different dynamic network changes.

2.2. Network monitoring tools

As mentioned above, there are many tools for monitoring network processes and traffic (Nagios, Wireshark, SolarWinds, Zabbix, Hyperc, Capsa free, IBM Tivoli,

Ganglia, Kiwi Monitor, etc.) [14], some are open source and others are commercial products that require license fees. However, usually the information they collect about all the events in the network is not always complete. On the other hand, it is possible to log multiple events, which defines a huge amount of data, and their value can be assessed by comparing them with events recorded from other sources. According to [14], monitoring depends on three general parameters - "*delay, jitter that is failure of synchronization, and bandwidth*". In addition, it states that the implementation of monitoring can help increase the efficiency and performance of the network by improving its reliability. This requires a monitoring tool that works continuously. A brief overview of several useful tools is presented below.

✓ Nagios is an open-source tool that can monitor applications, servers, and networks, allowing the addition of monitoring capabilities for almost any network process. When combined with Request Tracker (RT), effective and automatic network monitoring and problem location identification can be provided.

✓ SolarWinds has an excellent graphical user interface (GUI) and offers a set of monitoring tools, supporting operating systems such as Windows, Mac, Linux. Installation time depends on the complexity of the data, allowing customization by the user. Through a specialized tool, network traffic analysis can be performed, tracing network bandwidth down to a lower level and graphically presenting the results. The general purpose of the product is to perform failure analysis, resource availability and performance level of network communications.

✓ Wireshark is rated as one of the best open-source packages for examining traffic in wired and wireless networks, analysing all network traffic, and allowing filtering of traffic selected for monitoring. The tool is available in different versions (graphical and command) and works with Windows, UNIX, and Linux platforms.

✓ IBM Tivoli supports Windows, Linux, and Unix, allows for easy installation, but requires specific configuration and refinement of analytical functions and responses. It can use sensors in data centres, making it suitable for smart systems.

A basic requirement for monitoring tools is to be accurate and easy to use, correctly and correctly reflecting the processes in the network [15]. The review in the paper defines measurements as passive, active or hybrid, stating that passive network monitoring is an excellent tool for this, allowing the detection of problems in individual devices that affect the entire local network and allowing the generation of network statistics to measure productivity. The overview summarizes the basic terms and concepts of network monitoring, their quality of service and wireless network monitoring tools. Another overview of network monitoring capabilities is proposed in [16] but focused on Software Defined Networks (SDN) and discusses their challenges and development, including design concepts, research approaches, and open questions to address.

3. INITIAL PHASES OF MONITORING ORGANIZATION IN LAN

As a rule, conducting experiments for monitoring and researching network processes in local area network (LAN), including analysis of network traffic parameters, is carried out planned and with a specific purpose. The general organization of such

research unites sequential procedures, and the section presents phases when using a Windows Server environment and the tools provided by it.

3.1. Specifying the reason for monitoring the servers

One primary reason for conducting network process monitoring research is to troubleshoot server performance issues. An example situation is the inability of users to connect to a given server, which requires monitoring to discover the cause. Another reason is a need to increase the performance of a server, which can be done by improving disk I/O operations, reducing CPU utilization, and reducing network traffic loading the server. Solving such problems may require trade-offs in resource usage. One possible situation is a significant server load when the number of active users increases, which can be overcome by improving performance by distributing certain files over different devices.

3.2. Preliminary preparation for monitoring

Preliminary preparation requires at the beginning to establish the level of performance of a given server by measuring the parameters at different stages of its operation. For example, during periods of maximum and minimum load, or during stages when it is not being used by users. Benchmarking of accumulated data can identify weak points and possible problems, determining requirements for re-configuration and optimization. Based on a suitable preliminary analysis, an experimental plan can be formulated from sample steps:

1. Determining the main events in the monitoring server.
2. Establishing filters to reduce the amount of information collected.
3. Configuring monitors and alarms to monitor events.
4. Logging event data in a way that allows for easy subsequent analysis.
5. Analysing the recorded data from the measurements.

In principle, experiment planning is a necessary preliminary phase in all studies, but in some cases it is possible to simplify by skipping selected steps, for example, when the study does not require serious analysis of the measured data.

3.3. Network activity analysis using Performance Monitor

Windows Performance Monitor is a powerful and according to [17] “often underutilized” tool, and the publication also provides an overview of the available options. Performance Monitor displays graphical statistics for a selected set of performance parameters for a given server. For each of the parameters defined for monitoring, information is displayed and a separate graph is created, and the interval for its update can be configured. When using the environment, it is recommended to save the tracking information to a report file and configure alarms to send messages when certain events occur or when certain thresholds are reached.

An example of a study in a network with four servers is presented in Figure 1, with System Monitor (Performance Monitor tool) running for each of them. The object of performance monitoring are different groups of counters, the individual servers being respectively: ✓ the master domain controller (DNS & DHCP services); ✓ second domain controller (for print server); ✓ the Exchange server (for the objects Server,

Processor, System, Memory); ✓ Web server (for web services only with objects Server, Browser, System.

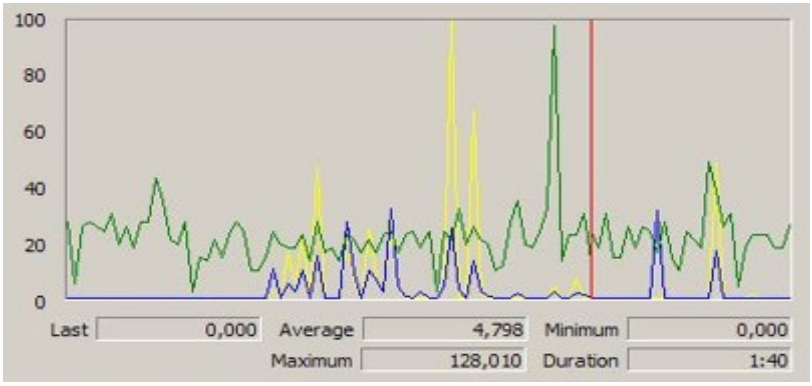

Figure 1. Graphical visualization of the observed counters

3.4. Network performance monitoring

In addition to the performance of each of the servers, the overall performance of the entire network needs to be monitored. One way to examine performance during initial network design is through the Task Manager (Figure 2). The basic information provided includes the name of the network adapter (Adapter Name), percentage of network utilization (Network Utilization), speed of interface connections (Link Speed) and working state (State). The figure represents the total amount of bytes of network traffic. Upon request, additional information can be provided about the percentage of files received as a fraction of the total connection caps, the total volume, as well as the current connection capacity used by all traffic on the network adapter.

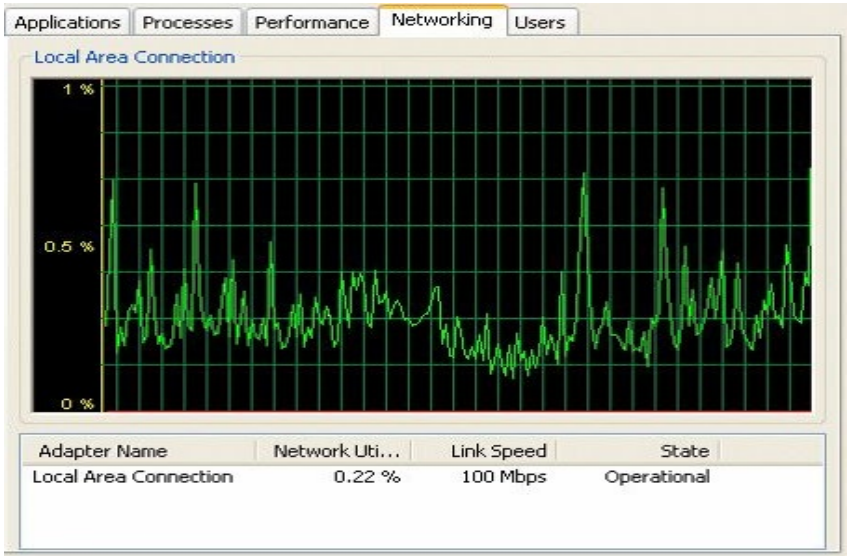

Figure 2. Monitoring network performance and server behavior

3.5. Registration of events

When monitoring is conducted, the recorded behaviour information is stored in files (event logs). The accumulated information enables decision-making to ensure the operability and security of the network system. Enabling the "Event Viewer" (Figure 3) provides an opportunity to actively manage event registration, as a quantitative and qualitative analysis of popular techniques and methods is done in [18]. A summary of the possibilities is presented in Table 1.

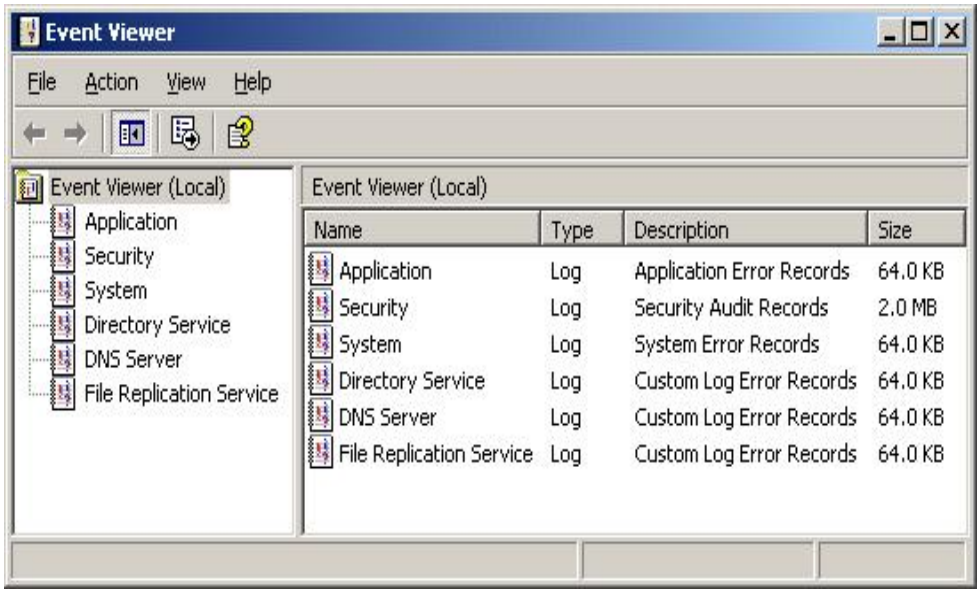

Figure 3. Visualization of event from different logs by Event Viewer

Table 1. Log options of Event Viewer

Name of Log option	***Comments***
Application	Events logged by applications and monitored for all servers
Security	Monitor and trace events with local or global group policies for all servers
System	Events logged by the operating system or its components
Directory	Registrations from Active Directory and related services
DNS Service	Registration (recording) of DNS requests, responses and other DNS activities (tracked only on domain controllers)
File Replication Service	Logs (records) system file replication activities (only tracked on domain controllers)

Event Viewer provides brief information about the occurrence of an event, such as individual events, such as: ✓ information about an event related to a successful action; ✓ audit for successful or unsuccessful implementation of an action; ✓ warning of possible network problems, providing details useful for prevention; ✓ error message when starting a service. Event logs include type, date and time, source, category, identifier, user, description, and data.

4. CONCLUSION

Preliminary monitoring of the behaviour of network components is a necessary stage when designing a virtual local network in a given corporation, and the main requirement is to choose an appropriate tool suitable for the specific network environment. A preliminary evaluation of possible software tools can be based on the following criteria.

• Ability to monitor all devices on the network from servers to end user devices.

• Relatively easy use of the offered options, which does not require additional training of technical support employees.

• Timely notification when a problem or failure of a given component occurs in the working network environment.

After specifying the selected criteria, they should be analysed on the basis of the proposed (existing) solutions (program monitors), analysing the overall value of the research and its effectiveness against the set goal. No less important is the subsequent maintenance of network management. In this respect, the main key aspects of data pre-processing are summarized in article [18] – grouping of existing techniques; analysis of pre-processing tools; choosing appropriate data structures for event logs; analysis of problems and imperfections; defining event log pre-processing tasks; the type of attributes or information.

REFERENCES

[1] Adeleke, O.A., Bastin, N., Gurkan, D. Network traffic generation: A survey and methodology. *ACM Computing Surveys (CSUR)*, vol. 55, no. 2, March 2023, art. 28 pp.1-23 (online: 18 Jan 2022) (https://doi.org/10.1145/3488375).

[2] Alsheikhy, A. Estimating end-to-end delay on a networking environment using developed framework. *International Journal on Information Technologies and Security*, vol. 14, no. 1, 2022, pp. 3-16.

[3] Mathad, K.S., Math, M.M. Inference and performance aware multi-channel scheduling and routing scheme with call admission control in wireless mesh networks. *International Journal on Information Technologies and Security*, vol. 15, no. 1, 2023, pp. 15-26. DOI: https://doi.org/10.59035/XUYS3831

[4] Zoraida, B.S.E., Indumathi, G.. Comparison of software defined networking with traditional networking using NS2 simulator. *International Journal on Information Technologies and Security*, vol. 15, no. 3, 2023, pp. 3-14. DOI: https://doi.org/10.59035/TBWW1651

[5] Kravets, O.Ja., Aksenov, I.A., Redkin, Yu.V., Mutin, D.I, Atlasov, I.V., Zaslavskiy, A.A. Algorithms and methods for managing request flows in a distributed service system. *International Journal on Information Technologies and Security*, vol. 15, no. 4, 2023, pp. 73-80. DOI: https://doi.org/10.59035/OBNY2037

[6] Lu, H., Zhang, F. Resource fragmentation-aware embedding in dynamic network virtualization environments. *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 936-948, June 2022, doi: 10.1109/TNSM.2022.3152309.

[7] Vakharkar, S., Sakhare, N. Critical analysis of virtual LAN and its advantages for the campus networks. In: Shakya, S., Bestak, R., Palanisamy, R., Kamel, K.A. (eds) *Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies*, vol 68, 2022, pp 733–748, Springer, Singapore. https://doi.org/10.1007/978-981-16-1866-6_56

[8] Dong, S. and Xia, Y. Network traffic identification in packet sampling environment. *Digital Communications and Networks,* vol. 8, no. 4, Aug 2022 (https://doi.org/10.1016/j.dcan.2022.02.003)

[9] Siracusano, G., Galea, S., Sanvito, D., et al. Re-architecting traffic analysis with neural network interface cards. *9th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22)*, April 2022, ISBN: 978-1-939133-27-4, Renton, WA, USA, pp. 513—533 (https://www.usenix.org/conference/nsdi22/presentation/siracusano)

[10] Zola, F., Segurola-Gil, L., Bruse, J.L., Galar, M., Orduna-Urrutia, R. Network traffic analysis through node behaviour classification: a graph-based approach with temporal dissection and data-level preprocessing. *Computers & Security*, vol. 115, April 2022, art.102632 (https://doi.org/10.1016/j.cose.2022.102632).

[11] Guerra, J.L., Catania, C., Veas, E. Datasets are not enough: Challenges in labeling network traffic. *Computers & Security*, vol. 120, Sep 2022, art. 102810 (https://doi.org/10.1016/j.cose.2022.102810)

[12] Agarwal, A., Liu, Z. Seshan, S. {HeteroSketch}: Coordinating Network-wide Monitoring in Heterogeneous and Dynamic Networks. *19th USENIX Symposium on Networked Systems Design and Implementation (NSDI 22),* 2022, pp. 719-741.

[13] Yu, L., Zwetsloot, I.M., Stevens, N.T., Wilson, J.D. and Tsui, K.L., Monitoring dynamic networks: A simulation-based strategy for comparing monitoring methods and a comparative study. *Quality and Reliability Engineering International*, vol. 38, no. 3, 2022, pp.1226-1250. (https://doi.org/10.1002/qre.2944)

[14] Chahal, D., Kharb, L., Choudhary, D. Performance analytics of network monitoring tools. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 8, 2019, pp. 2572-2577.

[15] Alkenani, J. and Nassar, K.A., 2022. Network Monitoring Measurements for Quality of Service: A Review. *Iraqi Journal for Electrical and Electronic Engineering*, Dec 2022, pp. 33-44. (DOI: 10.37917/ijeee.18.2.5)

[16] Tsai, P.W., Tsai, C.W., Hsu, C.W. and Yang, C.S. Network monitoring in software-defined networking: A review. *IEEE Systems Journal*, vol. 12, no. 4, 2018, pp.3958-3969. DOI: 10.1109/JSYST.2018.2798060

[17] Marcho, C. Windows Performance Monitor overview. Microsoft, Mar 2019 (https://techcommunity.microsoft.com/t5/ask-the-performance-team/windows-performance-monitor-overview/ba-p/375481)

[18] Marin-Castro HM, Tello-Leal E. Event Log Preprocessing for Process Mining: A Review. *Applied Sciences*. Vol. 11, no.22, 2021, art. 10556 (29 p.). https://doi.org/10.3390/app112210556

Information about the author:

Radi Romansky is a full professor at Technical University of Sofia, Doctor (Dr) in Computer Engineering and Doctor of Science (D.Sc.) in Informatics and Computer Science; Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has over 220 scientific publications and over 25 books. Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, privacy and data protection, etc.

Remark:

Manuscript has been received in May 2024 to take part in the 38th International Conference on Information Technologies (InfoTech-2024), IEEE conference, Rec. # 63258, Section C: "Networking and communication Technologies". It has been accepted and revised based no double-blind reviewing and has not been published in full text elsewhere.