11TH INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2024
Serbia, Tara, 9-11 October 2024

PROPOSITION OF LABORATORY EQUIPMENT AND ITS UTILISATION FOR COMPLEX BATTLEFIELD IP NETWORK SIMULATION

ĐORĐE NEŠKOVIĆ
School of Electrical Engineering & Vlatacom Institute, Belgrade, djordje.neskovic@vlatacom.com

MARKO MARKOVIĆ
School of Electrical Engineering & Vlatacom Institute, Belgrade, marko.markovic@vlatacom.com

LARA KAŠCA
School of Electrical Engineering & Vlatacom Institute, Belgrade, lara.kasca@vlatacom.com

STEFAN STANKOVIĆ
School of Electrical Engineering & Vlatacom Institute, Belgrade, stefan.stankovic@vlatacom.com

MIROSLAV PERIĆ
Vlatacom Institute, Belgrade, miroslav.peric@vlatacom.com

MLADEN KOPRIVICA
School of Electrical Engineering, Belgrade, kopra@etf.rs

DEJAN DRAJIC
School of Electrical Engineering, Belgrade, ddrajic@etf.rs

Abstract: *This paper gives a proposition for laboratory equipment and its use for simulation of effects of network topology and link state reconfiguration during battlefield operations. All equipment presented in this paper is based on open source software solutions and well-known hardware development platforms in order to minimize equipment cost as well as provide a simulation environment that is independent of any single manufacturer. Utilization of open source solutions gives us a level of security as it lessens a chance of traditional vendor abuse in more unfortunate circumstances. The core of the laboratory is based on a GNS3 simulator, which can be installed on all three major operating systems (Linux, Windows and Mac) and has the capability of simulating a network that can be added in between two physical end devices that we wish to test in various battlefield scenarios using highly available network adapters. In addition to that, we will focus on network intermediate devices (switches and routers) that are not dependent on any single manufacturer and are open source solutions that can be used for future development of secure and fully-known equipment. We present expected results for the transition of encrypted and unencrypted traffic.*

Keywords: *Network Simulation, Open Source Solutions, Battlefield Communication, GNS3 Simulator, Secure Network Solutions.*

1. INTRODUCTION

Network simulation [1] plays a crucial role in testing and evaluating network performance, design, and security. It provides a controlled environment to model, analyze, and predict the behavior of real-world networks without the high costs and risks associated with live testing. In the modern world, where digital communication and data exchange form the backbone of various industries, ensuring the reliability, efficiency, and security of network infrastructures is paramount. Network simulation emerges as an indispensable tool for testing and evaluating network performance and behavior. It allows us to create virtual models of network environments. Setting up physical network infrastructures for testing purposes can be prohibitively expensive. Network simulation reduces the need for physical hardware, allowing for comprehensive testing and experimentation without significant financial investment. Testing new configurations, protocols, or security measures on a live network carries inherent risks, including potential downtime or data breaches. Network simulations provide a safe environment to test and validate changes before deploying them in a live setting. Simulations can easily scale to model networks of various sizes, from small local area networks (LANs) to vast wide area networks (WANs). This flexibility allows for testing different scenarios and configurations, ensuring the network can handle future growth and diverse conditions. By simulating network traffic and user behavior, we can analyze the performance of a network under various loads and conditions. This helps in identifying bottlenecks, optimizing resource allocation, and enhancing overall network efficiency. New networking protocols can be rigorously tested in a simulated environment before being

Corresponding author: Đ. Nešković;
E-mail: dejanjordjevic.vgi@gmail.com
DOI: 10.5937/OTEH24070N

rolled out. This ensures compatibility and performance standards are met, reducing the risk of deployment failures. Network simulations are invaluable for security testing, allowing for the assessment of network vulnerabilities and the effectiveness of security measures against potential threats. Simulated attacks and defenses help in building robust security protocols and incident response strategies. They facilitate learning and skill development in a risk-free setting. We can experiment with cutting-edge technologies and innovative network designs without the constraints of physical limitations. Simulations foster innovation by providing a sandbox environment for testing novel ideas and concepts. Network simulation is a powerful and versatile tool that enhances the capability to test, analyze, and optimize network performance, security, and scalability. It offers a risk-free, cost-effective, and flexible approach to network testing, ensuring that real-world deployments are reliable, efficient, and secure. This is all especially important in battlefield IP network simulations, which are the focus of this paper.

The focus of this paper is a proposal for network laboratory setup and its use for simulation of effects of network topology and link state for dynamic battlefield IP network simulation. The proposed solution allows network performance reconfiguration to simulate dynamic conditions and hard circumstances to simulate real-life problems in war. The laboratory proposed in this paper is based on free open source software and well-known and easily accessible hardware solutions.

The rest of the paper is organized as follows: The second section provides analysis of hardware and software needed for network simulation. The third will focus on open source hardware and software solutions for real-life network routers. The fourth section will focus on a simple laboratory proposition for battlefield IP network simulation. The fifth section concludes the paper and provides remarks on the expected performance of the proposed solution.

2. NETWORK SIMULATION SOLUTION

The core part of a network simulation laboratory is a network simulator itself. In this paper we will focus on GNS3 (Graphical Network Simulator-3) [2] [3], which is network simulation software that allows users to design, configure, and test complex network topologies. It provides a graphical interface where users can drag and drop various network devices, such as routers, switches, and firewalls, to create virtual network environments. One of the key features of GNS3 is its ability to integrate real network device images, enabling users to emulate real-world network hardware and software. This allows for highly realistic network simulations, making it an invaluable tool for learning, testing configurations, and troubleshooting network issues without the need for physical equipment. GNS3 supports a wide range of devices and can emulate Cisco IOS [4], Juniper [5], and other network vendors' operating systems. Additionally, it can integrate with other virtualization technologies [6] such as VMware [7] and VirtualBox [8], further expanding its utility and flexibility. Overall, GNS3 is a powerful platform for network simulation, offering a practical, cost-effective way to gain hands-on experience with network design and troubleshooting. Its extensive features and realistic emulation capabilities make it an essential tool for both experimentation and professional development in the field of networking.

Integrating real equipment in GNS3 enhances its simulation capabilities by connecting virtual networks with physical devices. This setup allows users to test configurations and troubleshoot issues in a hybrid environment, combining virtual and real-world elements. By connecting GNS3 to actual routers, switches, and firewalls, users can validate configurations and network designs with greater accuracy. This integration is beneficial for advanced network training, real-world scenario testing, and bridging the gap between theoretical simulations and practical implementations.

GNS3 simulator can be installed on all three major operating systems (Linux, Windows and Mac); this offers complete flexibility for use with a computer that might already be available. The computer used for network simulation in the example given in this paper was a laptop with a Linux-based operating system, Ubuntu 22.04.4 LTS [9]. Within GNS3, Cisco router IOS images were used for router emulation. Connection between devices in an emulated environment could be either local with simulated Ethernet cables or serial for longer link simulation; on those links, various network conditions could be simulated, like delay for long-distance communication, packet loss, corruption, packet drop frequency, and custom filter options. This represents a great tool for complex battlefield network simulation of hard conditions and unstable networks.

GNS3 has within its emulated components a dedicated component for Cloud; this component is capable of connecting physical Ethernet interfaces. Since most personal computers have only one, or no, physical Ethernet port, use of Ethernet-to-USB adapters is an adequate solution (speed of 1 Gbps is recommended but not necessary). These adapters allow the connection of real hardware and end devices into a simulated environment. For example, two devices for secure communication could be connected to points in a simulated network and tested in various conditions and against attacks.

3. OPEN SOURCE ROUTERS

Open source software for network routers offers a cost-effective and flexible solution for managing network infrastructure. Open source router software is free to use, significantly reducing the cost compared to proprietary solutions. Utilization of open source solutions gives us a level of security as it lessens a chance of traditional vendor abuse in more unfortunate circumstances, as we are fully aware of its source code and each function. Users can modify the source code to meet specific requirements, offering unparalleled flexibility and control over network configurations. Open source projects benefit from active communities that contribute to software development, security updates, and troubleshooting, ensuring continuous improvement and

support. This allows for transparency, where code can be audited for security vulnerabilities, leading to more secure implementations. Many open-source router platforms offer advanced features and capabilities typically found in high-end commercial products, making them suitable for a wide range of applications, from home use to enterprise-level deployments. Overall, open-source software for network routers empowers users with cost-effective, customizable, and robust solutions for managing network infrastructure. Most of these solutions are Linux-based [10], like OpenWrt [11], which provides a fully writable file system with package management, allowing users to customize the firmware to their needs. OpenWrt supports a wide range of devices and offers features like advanced network monitoring, QoS (Quality of Service), and VPN capabilities. One other notable solution is DD-WRT [12], which is designed to replace the stock firmware on many commercial routers. It enhances router capabilities with features like increased range, improved signal strength, VPN support, and extensive networking tools. It's particularly favored for its user-friendly interface and stability.

But some Linux-based operating systems have the capability of adding router-like capabilities like Ubuntu, which supports IP forwarding. For the purpose of this research, two Kria [13] [14] robotics development kits with Ubuntu OS have been set up as routers. The archived port speed was 1 Gbps, which matches the specified port speed of the development kit. In the ever changing environment of battlefield simulations, probably the best routing algorithm is OSPF since it only needs to be aware of neighboring networks to set up, and it is supported by Ubuntu.

4. LABORATORY FOR BATTELFIELD IP NETWORK SIMULATIONS

The basic idea for the proposed laboratory is to have one PC with GNS3 installed on it with two Ethernet to USB adapters (preferably 1 Gbps), and within GNS3 installed images for routers that are most commonly used in real-life networks that we are trying to emulate; for example, in case of the environment used for this paper, Cisco IOS images were used, and for the sake of testing, both 100 Mbs and 1 Gbps were used. For link variable state testing, we propose a simple network with two routers, each one connected to one physical interface through a cloud feature, and a serial link between them (a serial link is used so link state changes such as delay work as they should). As seen in figure 1.

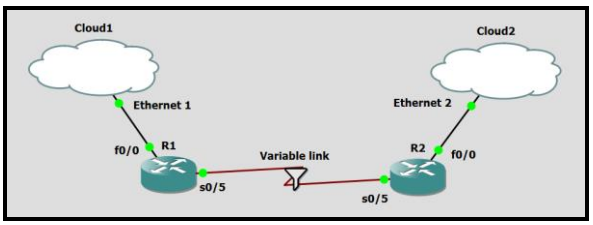

Figure 1. Simple emulated network for variable link state testing

The filtering feature allows for simulation of real-life link states like delay, packet corruption and packet loss. Adding those circumstances to the serial link allows us to test the behavior of devices or networks connected to physical interfaces in such conditions and to explore and develop necessary solutions on how to adapt devices and programs to overcome such situations. The proposition for what to connect to physical interfaces is to not connect just two end devices but to create networks that would be as close to the ones that would be used in real scenarios. For example, the first component behind the physical interface on each side should be a router, as it is most commonly the case in real life. Unlike an emulated one, a real hardware solution is the better option, since it is the only one that we have access to outside the laboratory environment. The router chosen for this research is the already mentioned Linux router based on Ubuntu with IP forwarding enabled and installed on a single-board computer development kit with two Ethernet ports. This allows us to be fully aware of router functionality and adapt it and configure it to specific needs. One port of the router is connected to a simulated network, which should, for experimentation purposes, be considered a public access network, while the other port should be connected to an Ethernet switch, so it would not limit us to just one device. The number of devices used for experimentation is limited by ports on the used switch; additionally, Wi-Fi access point could be used for testing wireless devices, but the best results are achieved when end devices are connected directly to the switch since this removes one more possible point of failure.

The other simple proposal that might be used for simulation of an environment with a lot of rerouting and circumstances when links are destroyed or down because of a power outage, might be simplified by emulating a slightly more complex network, as shown in figure 2. When testing the capabilities of our end devices and network devices, deleting links and connecting them again while communication is in progress would give a great idea of how a system of interest would function in such circumstances. These two simple network topologies give us a glimpse into the capability of such a laboratory solution. Furthermore, this could be expanded and combined to emulate complex networks weary close to the real-life scenario.

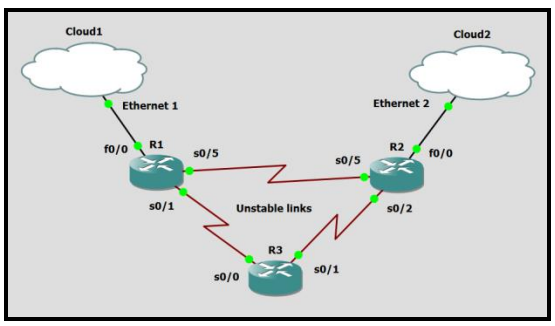

Figure 2. Simple emulated network for unstable link and rerouting testing

This is a simple and cheap solution for emulating complex and dynamic network environments. Also a great feature of GNS3 is that any link in a virtual

network can be analyzed separately via Wireshark [15], allowing for detailed traffic analysis. Also, for example, for testing of cryptography devices, this feature allows us to see what potential attacker that intercepted network traffic sees, and is helpful to figure out weaknesses in our systems.

One more notable feature that might be useful is the capability of GNS3 to connect to virtual machines hosted on the same device, which already has a virtual PC (VPC) as a component. This could be integrated into a simulated network to add traffic and take up resources to simulate a busy network. Example shown in figure 3.

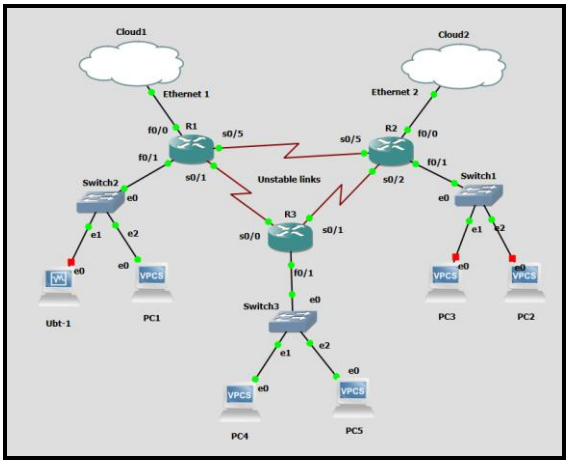

Figure 3. Example of virtual network with virtual PC to simulate realistic network conditions

This will allow us to add additional variability into simulated network conditions that reassemble real-life solutions more realistically. But users should keep in mind that the size of the simulated network is limited by the resources available to the device on which GNS3 is hosted. Each emulated device in a virtual network occupies resources, and the main limiter of network size is RAM memory. The utilization of RAM memory is defined by each component added to a network and GNS3 provides us with information on how much of it is occupied; it is not advisable for this value to pass 50%. Another important remark is that whenever a virtual network is connected to the real one, a significant loss of bandwidth will happen simply because the transition between networks is imperfect. Although all network equipment, real and emulated, is specified at 1 Gbps and works perfectly in normal conditions, the maximum network speed reached no more than 30 Mbps in a laboratory environment. Encryption of data between two end points was tested when implemented on real network hardware and emulated routers and gives expected results in limiting network speed. Also, there is a constant delay of approximately 10 ms for translation between a real and a virtual network per physical interface. These are serious limitations, but they themselves could be taken as part of wartime battlefield conditions and used as a baseline limitation of IP network.

5. CONCLUSION AND REMARKS

This paper highlights the critical role of network simulation in testing and evaluating network performance, design, and security, especially in the context of dynamic battlefield IP network simulations. By leveraging tools like GNS3, network simulations provide a cost-effective and risk-free environment for rigorous testing and validation of network configurations and protocols. The proposed laboratory setup, utilizing open-source software and accessible hardware, demonstrates a practical approach to simulating real-life network conditions, including the challenging scenarios encountered in warfare.

The use of GNS3 allows for realistic emulation of network hardware and the integration of physical devices, enhancing the simulation's accuracy and utility. By incorporating open-source router solutions like Linux-based routers, the laboratory setup remains flexible and customizable, supporting a wide range of testing scenarios. The proposed configurations for simulating network topology changes and link state variations offer valuable insights into the resilience and adaptability of network infrastructures under adverse conditions.

Despite some limitations, such as bandwidth reduction and latency when transitioning between virtual and real networks, these simulations provide a valuable baseline for understanding and improving network performance in critical environments. Overall, the methodology and tools discussed in this paper represent a significant advancement in network simulation, enabling robust testing and optimization of battlefield IP networks to ensure their reliability, efficiency, and security in real-world deployments.

The future work plan is to create a plug-and-play environment for testing complex network encryption devices to their limits with attack simulation along the simulation of network conditions.

6. ACKNOWLEDGEMENT

This paper was supported by Vlatacom Institute of High Technologies under the project P176.

References

[1] PETROVIĆ,R., SIMIĆ,D., STANKOVIĆ,S., PERIĆ,M.: Educational Platform for Examining the Influence of the Simulated Satellite Link on Overall Communication inside of Different IoT Systems, Proceedings of the 16th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), 2023

[2] https://www.gns3.com/

[3] P. Gil, G. J. Garcia, A. Delgado, R. M. Medina, A. Calderón and P. Marti, "Computer networks virtualization with GNS3: Evaluating a solution to optimize resources and achieve a distance learning," *2014 IEEE Frontiers in Education Conference (FIE) Proceedings*, Madrid, Spain, 2014, pp. 1-4, doi: 10.1109/FIE.2014.7044343.

[4] https://www.cisco.com/

[5] https://www.juniper.net

[6] G. Aryotejo, E. A. Sarwoko, A. Sugiharto and M. M. Hakim, "Performance of Virtual Machine Managers for Computer Network Learning," 2021 5th International Conference on Informatics and Computational Sciences (ICICoS), Semarang, Indonesia, 2021, pp. 155-159, doi: 10.1109/ICICoS53627.2021.9651899.

[7] https://www.vmware.com/

[8] https://www.virtualbox.org/

[9] https://releases.ubuntu.com/jammy/

[10] C. E. Palazzi, M. Brunati and M. Roccetti, "An OpenWRT solution for future wireless homes," 2010 IEEE International Conference on Multimedia and Expo, Singapore, 2010, pp. 1701-1706, doi: 10.1109/ICME.2010.5583223.

[11] https://openwrt.org/

[12] https://dd-wrt.com/

[13] M. A. Aslam, S. Kumar and R. Holsmark, "An Efficient Router Architecture and Its FPGA Prototyping to Support Junction Based Routing in NoC Platforms," 2013 Euromicro Conference on Digital System Design, Los Alamitos, CA, USA, 2013, pp. 297-300, doi: 10.1109/DSD.2013.121.

[14] https://www.amd.com/en/products/system-on-modules/kria/k26/kr260-robotics-starter-kit.html

[15] https://www.wireshark.org/