Lessons Learned from ASNET-AM Network Simulation

Arusyak Manasyan
IIAP NAS RA
Yerevan, Armenia
e-mail: armanasyan@iiap.sci.am

Robert Tadevosyan
IIAP NAS RA
Yerevan, Armenia
e-mail: robert@sci.am

Hrachya Astsatryan
IIAP NAS RA
Yerevan, Armenia
e-mail: hrach@sci.am

***Abstract*—The article presents an evaluation and benefits of modeling National Research and Education Networks (NREN) facilities in the Armenian NREN ASNET-AM (Academic Scientific Network of Armenia) case. Several models and operational variants have been developed and evaluated using the GNS3 (Graphical Network Simulator-3) network modeling platform. The study demonstrates the benefits of using the modeling platform as an excellent substitute for complex and expensive network equipment.**

***Keywords*—Network Simulation, network modeling, GNS3, ASNET-AM, devices, traffic.**

I. Introduction

High-performance, secure, and reliable communication networks are crucial in meeting the increasing demands of research centers and universities. NRENs effectively leverage communication and modern computer technology to interconnect data communication across continents through the pan-European GÉANT network [1]. NRENs provide academic and educational institutions with computationally intensive resources like high-performance computing and cloud computing, as well as data-related infrastructures such as data centers and repositories [2]. These services are built on robust computer networks that ensure network interconnectivity, large data transfer capabilities, and high-performance large-scale simulations. Managing these multi-level and heterogeneous infrastructures presents challenges, including configuration management, updates, monitoring, and troubleshooting. Traditionally, network administrators have used testbed infrastructures comprising physical components like cables, switches, routers, and servers to develop and evaluate new network devices and configurations. However, this approach is time-consuming and expensive due to the need for configuration, updates, and maintenance.

Network virtualization techniques [3] enable the abstraction of network resources, either by consolidating multiple physical networks into a single virtual software-based network or by dividing a single physical network into independent virtual networks. This virtualization software allows seamless access to virtual machines across different domains without network reconfiguring. By creating a network overlay, the software enables the operation of distinct virtual network layers on top of the same physical network fabric. Network virtualization saves time by streamlining the infrastructure provisioning process for supporting new applications.

Network emulators [4] provide an opportunity to emulate the network using open-source, modular, extensible, programmable, community-supported, and community-driven simulation tools or frameworks. It allows network administrators to create simulated network environments (special equipment, routers, switches, workstations, and servers) using simulation models, enabling them to test and evaluate network configurations without needing physical infrastructure. While implementing these simulation-based solutions in real networks can be complex, they provide a cost-effective and efficient approach to network testing and experimentation.

This paper addresses the challenges of ensuring flow security, monitoring, early error detection, and collision reduction in developing diverse systems and services, including new node management software and tools. This study presents the evaluation results and valuable lessons from the ASNET-AM network simulation, shedding light on practical approaches to enhancing network performance. The ASNET-AM backbone interconnects more than 70 organizations in six towns of Armenia with speeds up to 10 Gbps, among which there are research institutions of NAS RA, universities, libraries, museums, and governmental agencies.

II. Methodology

The basic ASNET-AM network topology (see fig. 1), consisting of core routers and their interconnected nodes, was utilized for the simulations.

The backbone network emulation utilized 10 Gbps links to ensure optimal connectivity between the core routers located in the PoPs (Point of Presence) and the connected nodes. In terms of routing protocols, the network topology incorporated distributed routing protocols such as BGP (Border Gateway Protocol) and OSPF (Open Shortest Path First). These protocols facilitate efficient routing and network management within the ASNET-AM network. Table 1 shows the network

https://doi.org/10.51408/csit2023_57

topology consists of several Mikrotik routers with RouterOS L6 operating system and Tilera processors.

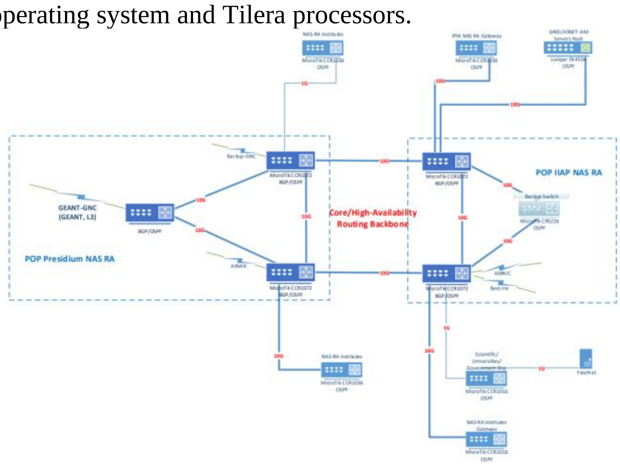

Figure 1. ASNET-AM network topology.

Model	CPU	SFP+ ports	RAM (GB)
CCR1072	72 x 1GHz	10G	16
CCR1036-12G-4S	36 x 1GHz	10G	4
CCR1016-12G	16 x 1GHz	10G	2

Table 1: The network topology hardware configuration.

The GNS3 network simulation platform [5] replicates the ASNET-AM network topology for experimental purposes. The simulations conducted using an open-source GNS3 emulator provide essential insights into the behavior and performance of ASNET-AM network topology. The GNS3 network emulator is a popular platform offering the possibility to federate various platforms for virtualizing operating systems, providing a tool to define the topology of the network and many other tools like the packet analyzer and some network equipment models. By evaluating factors like connectivity, link utilization, and routing efficiency, this research contributes to optimizing and enhancing the ASNET-AM network infrastructure.

In network monitoring systems, many problems are becoming visible faster, and solving these problems is fast and easy. For network monitoring, administrators need more helpful network traffic monitoring and analysis tools to maintain the network system stability and availability, such as to fix network problems on time or to avoid network failure, ensure network security strength, and make good decisions for network planning. The open-source Zabbix network monitoring system [6] has been used for evaluation based on Simple Network Management Protocol and IP network multipathing monitoring. Zabbix includes an alerts system and community plugins.

The local and remote GNS3 VM RouterOS version runs as a virtual machine for Mikrotik CHR topology. The CPU and memory utilization, temperature, fan status, device availability, latency and packet loss, network interface, and device-specific metrics network KPIs are benchmarks by which optimal network performance is determined.

The resources of CloudLab [5] provided the necessary infrastructure and computing capabilities to replicate the ASNET-AM network topology. By leveraging the power of CloudLab, we could simulate realistic network conditions and evaluate various aspects, including network connectivity, scalability, and performance metrics.

III. Network Evaluation

The study examined the failures, packet loss and latency that occur during network operation, we increased the traffic to see how the network would behave in such a case, we closed one part, giving priority to another part of the network, and vice versa, again, observing the change in the results. About Network Monitoring we used Zabbix where we have gotten all the needed information from ICMP ping (see fig 3) to Devices CPU Temperature and etc.

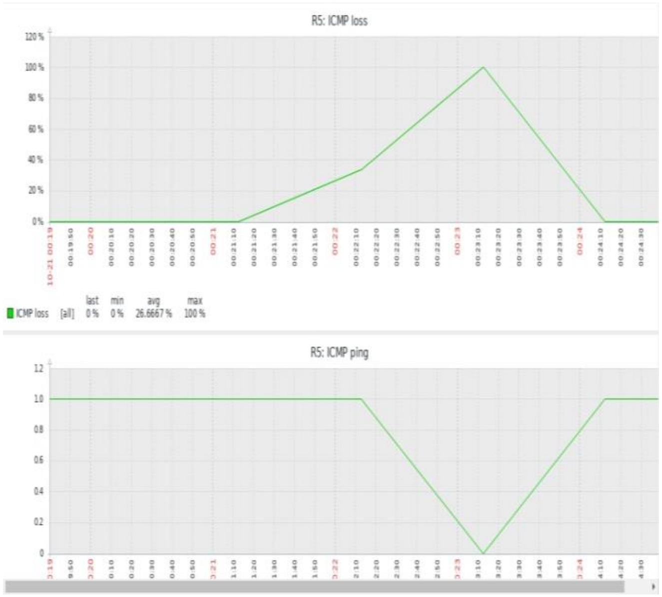

Fig3. ICMP packets

IV. Conclusion

The result of the research is a tested and fully pre-configured network. The case we are able to get a pre-configured and tested network, using the large resources available on the cloud, and then based on the results of the experiments and already understanding the risks, we implement the same in the real network.

References

[1] A. Yaver, J. M. Sánchez-Torres, M. A. Amórtegui, and L. Giraldo-Ríos, “A participatory foresight for national research and education networks”, *European Journal of Futures Research*, vol. 4(1), pp. 1-11, 2016.

[2] H. Astsatryan, W. Narsisian, V. SahaNyan, and Y. ShouNourian, “Collaborative Cloud Computing in Armenia: Challenges and Opportunities”, *Collaborative Technologies and Data Science in Smart City Applications*, vol. 20, 2018.

[3] J. Ramakrishnan, M. S. Shabbir, N. M. Kassim, P. T. Nguyen, and D. Mavaluru, “A comprehensive and systematic review of the network virtualization techniques in the IoT”, *International Journal of Communication Systems*, vol. 33(7), e4331, 2020.

[4] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, and H. Yu, "Advances in network simulation", *Computer*, vol. 33(5), pp. 59-67, 2000.

[5] R. Mohtasin, P. W. C. Prasad, A. Alsadoon, G. Zajko, A. Elchouemi, and A. K. Singh, "Development of a virtualized networking lab using GNS3 and VMware workstation", *In 2016 International conference on wireless communications, signal processing and networking (WiSPNET)*, IEEE, pp. 603-609, March 2016.

[6] P. Tader, "Server monitoring with Zabbix", *Linux Journal*, vol. 7, pp. 195, 2010.

[7] D. Duplyakin, R. Ricci, A. Maricq, G. Wong, J. Duerig, E. Eide, and P. Mishra, "The design and operation of {CloudLab}", *In 2019 USENIX annual technical conference (USENIX ATC 19)*, pp. 1-14, 2019.