

SELECTED PAPER AT THE ICCMIT'19 IN VIENNA, AUSTRIA

## Virtualized Network Management Laboratory for Educational Purposes

Oula L. Abdulsattar<sup>1,\*</sup>, and Emad H. Al-Hemiary<sup>1</sup>

<sup>1</sup>*Networks Engineering Department, College of Information Engineering, Al-Nahrain University, Iraq*

### ARTICLE INFO.

#### Keywords:

VNML, Network Management,  
Virtualization, Virtualbox, GNS3.

### Abstract

In this paper, we implement a Virtualized Network Management Laboratory named (VNML) linked to college campus network for educational purposes. This laboratory is created using Virtualbox virtualizer and GNS3 on Linux UBUNTU single HP DL380 G7 server platform. A total of 35 virtual devices (Routers, Switches and Virtual Machines) are created and distributed over virtualized campus network with seven network management tools configured and run. The proposed laboratory is aimed to overcome the limitations of network hardware existence in any educational facility teach network management subject in their curriculum. The other advantages include ease of managing the laboratory and overrides physical location setup within the same geographical area.

© 2019 ISC. All rights reserved.

## 1 Introduction

While large amounts of applications can be contained on a computer causing complexity in configuration, it seemed that there is a need to build servers in a way that each single application can be run on one physical server. Many benefits could be noticed using this approach and the most important is eliminating the amount of damage in case of failure and saving costs [1]. This approach could be achieved using virtualization technology [2].

Virtualization technology was invented long time ago in order to allow the facility of sharing large expensive mainframes among different application environments in an easy way. Recently, virtualization technology in all of its levels (network, system and

storage) is becoming very important for improving system availability, reliability and security, reducing costs, and providing greater flexibility [3].

Virtualization is a technique used to run more than one operating system simultaneously on the same computer, making one single computer appears as two, three or more computers. Virtualization usually used in case of doing something very hard or impossible to be performed in reality, or when not having the necessary equipment for it. Many different techniques are available today for virtualization and choosing the suitable one depends on system goals [4].

Virtualization software has proved itself to be efficient enough for the creation of virtual laboratories. There are multiple applications in these laboratories including the creation of experimentation environment of new technologies, as well as testing and developing of network software [5]. The creation of virtual laboratories mainly requires virtual machines which has nearly 100% duplication of each other, except

\* Corresponding author.

Email addresses: [oula.laith@coie-nahrain.edu.iq](mailto:oula.laith@coie-nahrain.edu.iq),  
[emad@coie-nahrain.edu.iq](mailto:emad@coie-nahrain.edu.iq)

ISSN: 2008-2045 © 2019 ISC. All rights reserved.

simple changes in configuration should be done, such as the identification information. Thus, in case of frequently duplicated installations, only one machine had to be configured and tested by the administrator, while the other machines will be cloned from it so quickly and easily [6]. Virtualization technology eliminates 90% of hardware devices required, which at the same time decreases all the concerning costs, required space, power etc. It also provides the facility of remote access to the laboratory making it a mobile laboratory that could be accessed easily from any location. Basically virtualization can be divided into multiple types: Server virtualization, Network virtualization and Desktop virtualization [7] but in VNML, server virtualization is the interest. There are a variety of software for server virtualization such as VirtualBox [8], VMware [9], KVM [10] etc. In VNML, VirtualBox is chosen as a server virtualization software because it is compatible with Linux [11] (operating system used in VNML), recommended by GNS3 [12] (network simulator used in VNML), simple, efficient and serves the desired requirements of VNML.

The remaining sections of the paper explain the importance of network management and highlights VNML used protocols and tools in Section 2, describe the design of VNML in Section 3, present VNML Laboratory manual used for installing and configuring tools in Section 4, show results obtained when running some of these tools in Section 5, and finally list the points concluded from VNML and mention the desired development on it in Section 6.

## 2 Network Management

With the fast growth and development in networking, network complexity becomes an important issue to interest. Thus, the whole network must be controlled by the network administrator who has a full access to it; this is called Network Managing [13].

In general, network management is a service that makes use of different protocols, applications, devices and tools to assist human administrators of networks in controlling and monitoring of network hardware and software resources and addressing network objectives and needs [14]. The important goal of network management is ensuring that network end users deliver IT services with the expected quality of service [15]. The protocol used in this paper for network managing is SNMP [16]. SNMP stands for Simple Network Management Protocol which is a protocol that operates in the application layer facilitating the delivery and exchange of management information among network devices [17]. SNMP enables network managers to find and solve problems, manage network performance, and plan network growth [18]. This protocol will be configured in the network by the stu-

dents according to the Laboratory manual already provided as a part of this virtual educational laboratory. Network management tools monitor the entire network and alert the manager in case of having any problem making the manager's job easier and save money and time [19]. Different tools could be used on the same network with different roles to have full control on the network connectivity, reachability, handling traffic etc. Generally, network management tools fall into three categories:

- Diagnostic tools which are used for testing connectivity, reachability and where a device is up or not [20]. Diagnostic tools used in VNML are Ping [21], TraceRoute [22] and TCPdump [23].
- Monitoring tools which run in the background to collect events and record the output according to a scheduled fashion [24]. Monitoring tools used in VNML are Smokeping [25], Nagios [26] and Cacti [27].
- Performance tools which inform the network manager about how the network handles the traffic flow [28]. Performance tools used in VNML is MRTG [29].

The selected tools are open source and can be downloaded from their provider, the students attending VNML are required to install, configure and observe response of each tool.

## 3 VNML Design

VNML is developed at Al-Nahrain University to use it as a teaching environment for Network Management course of bachelor students at the College of Information Engineering or any other network educational environment. The hardware components of proposed virtual Laboratory consist of: single physical server (HP ProLiant DL380 G7) with 32 GB RAM, Cisco Switch (Catalyst 2960G Series), Mikrotik Access Point (RB2011UAS-ZHND-IN), and a Laptop for each student in the Laboratory. Figure 1 shows the hardware devices used.

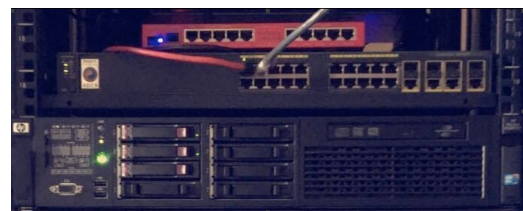


Figure 1. Hardware Devices Used in VNML

The software used are: Linux server (Ubuntu server 14.04 LTS [30]) with GUI as an operating system, GNS3 as a network simulator, VirtualBox for partitioning the physical server into virtual machines, Putty [31] for secure connections and network man-

agement tools which will be mentioned later in details. The proposed Laboratory is designed for 20 students (and could be expanded easily), it consists of two parts: physical part and a virtual one as shown in Figure 2, a single physical server matches the two parts. The figure shows that, in the physical part, each student has a laptop and the students are separated into 5 groups with 4 students in each group. All the laptops are connected wirelessly to an access point which is connected to a switch that is connected to our physical server to enter the virtual part. The virtual part partitions the physical server virtually into 20 virtual machines (VMs) and consists of a network created using network simulator GNS3. Using specific configurations, this network connects all these VMs together, connects the VMs to the Internet and connects the virtual part with the physical one making each VM acts as one of the students' laptops.

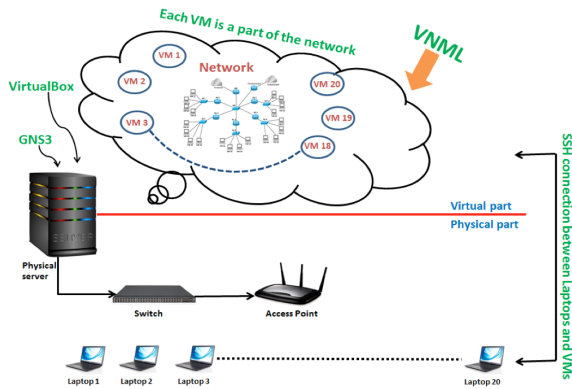


Figure 2. Physical and Virtual Parts of VNML

VirtualBox is used as virtual machine program installed on the physical server to partition it into multiple virtual machines, 20 VMs were created with 512 MBs of RAM, 8 GBs of hard memory, 12 MB of display card and Ubuntu server 14.04 as an operating system for each one. On the other hand, a virtual network was designed as a campus network for connecting these VMs and creating the required environment for performing network management. GNS3 was used as a virtual network creator with default cisco switches and 3725 cisco routers to be used. As mentioned before, the students in the Laboratory are separated into 5 groups with 4 students in each group and each VM in the virtual network is connected and acts as one of the student's Laptops. Thus, the 20 VMs are connected and separated in the virtual network as the same separation of the students in the real Laboratory. Using GNS3 options, the virtual machines created in VirtualBox were added as application templates in GNS3 to make the matching between the virtual network and the VMs. Figure 3 shows the proposed virtual network, each group (4 VMs) are connected directly to a switch (group's switch) which is

connected to a router (group's router). The 5 groups' routers are connected to a main switch (MS) to connect them to a main router (MR).

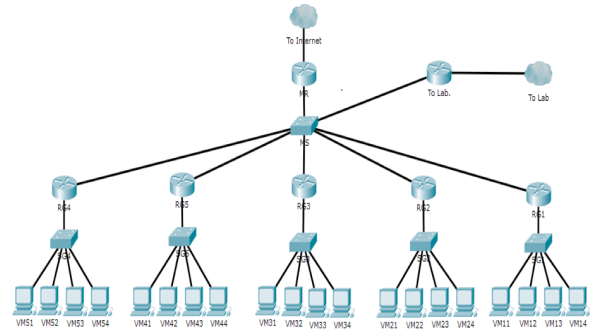


Figure 3. VNML Virtual Network inside the Server

Each machine was configured with static IP address, subnet mask and a gateway of the group's router interface, the separation of groups was done by using different routers and different IP networks for each group. Each router was configured with OSPF [32] as a routing protocol to have the reachability among all the nodes in the network. The IP address of the physical server used is a public IP in order to be accessed remotely and set on Ether 1of the server, while the IP addresses used in the network are private IPs, thus Nat method was activated in main router for mapping traffic from private network to public network.

The device that connects virtual environment to physical environment in GNS3 is the cloud, so a cloud was connected to the main router to connect the virtual network to the Internet by connecting it to Eth. 1 of the physical server which is the gate of the virtual network to the Internet. On the other hand, Eth. 2 of the server is used as the gate of the virtual network to the physical part of the Laboratory by connecting it to the physical switch previously mentioned in the physical part of the laboratory. Then a new cloud was added to the network to make the connection between the physical part and the virtual part of the Laboratory. The physical side of this cloud was connected to Eth. 2 of the physical server while the virtual part was connected to a router already connected to the man switch. By using all the previously enumerated connections and configurations, our virtual network had the reachability among all its nodes, connected to the Internet and connected to the physical part of the Laboratory. Installing SSH [33] on each VM makes each student in the real Laboratory ready to access his machine. Each student uses Putty to create the SSH channel between his laptop and his VM. Network management is performed by using Network Management Tools installed and run on the VMs by the students in the Laboratory according to instruc-

tions illustrated in a manual which is provided as a part of the laboratory.

#### 4 Laboratory Manual

In order to make the virtual Laboratory environment usable for network management course and to regulate it to the curricula and lectures of that course, 9 laboratory experiments are created, starting with the first experiment containing instructions for configuring the router of each group, then SNMP protocol is configured by instructions in the second experiment in order to run the network management tools. The next 7 experiments contain step by step instructions for installing and running 7 network management tools (Ping, Smokeping, TraceRoute, TCPdump, Cacti, Nagios and MRTG).

The structure of the experiment consists of five parts: purpose, theory, procedure, results and discussion. The purpose part explains the desired goal for performing the experiment. The theory part gives a brief explanation of the topic that will be learned in the experiment with its needs. The tired part, the procedure, illustrates step by step instructions for installing and running the topic of the experiment. While the results part clarifies how to get the outage of the running topic, explains the outage, and gives notes about how to change or enhance this outage. And finally, the last part, the discussion, contains problems to be solved by the students and some questions to discuss.

#### 5 Results

The results obtained in this virtual laboratory differ according to the tool used in the experiment. For example, this paper shows the output using one of the network management tools Smokeping. This tool draws a graph about the selected interface or DNS IP chosen to be monitored with the specified time of monitoring. Figure 4 shows the output of Smokeping value when chosen to monitor the reachability from one of the student's laptop (VM 23) to a web server (Google.com). Hence with each tool, results are obtained by using a tool and selecting the point required to be monitored.

#### 6 Conclusion and Future Work

In this paper, a virtual laboratory for network management was built using virtualization technology using single physical server to reduce the required devices for constructing it physically. Creating such a laboratory can be scalable and could be developed and expanded according to desired requirements, and integrate it in any campus network for educational purposes. The design implemented in this paper elim-

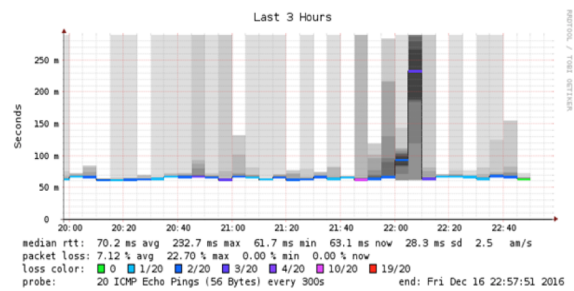


Figure 4. SmokePing tool used from VM23 to Google.com

inates 6 routers, 7 switches and emulate them inside the physical server. Thus, it saves costs, power and space required for all these eliminated equipment, and enable students operate on virtual devices overcoming any misconfigurations that could affect the real ones. The Laboratory can be accessed remotely overcoming the limitation of having the students and the devices at the same place, thus being a mobile Laboratory that could be moved and integrate with desired place without any restrictions. Finally, the performance of VNLM depends on the resource requirements of GNS3, thus VLNM reliability is restricted to GNS3 accuracy.

#### References

- [1] Pekka Toivanen, "Server Virtualization", Department of Information Technology, Lappeenranta University of Technology, October 2003.
- [2] Manel Bourguiba, Kamel Haddadou, Kamel Haddadou and Guy Pujolle, "Improving network I/O virtualization for cloud computing", IEEE Transactions on Parallel and Distributed Systems, Volume: 25, Issue: 3, March 2014.
- [3] Fábio Fabian Daitx, Rafael Pereira Esteves and Lisandro Zambenedetti Granville, "On the use of SNMP as a management interface for virtual networks", Integrated Network Management (IM) IEEE International Symposium, May 2011.
- [4] Espen Braastad, "Management of high availability services using virtualization", Department of Informatics, University of OSLO, May 2006.
- [5] Dalibor Dobrilovic, Vesna Jevtic, Zeljko Stojanov and Borislav Odadzic, "Usability of virtual network laboratory in engineering education and computer network course", IEEE, Serbia, 2012.
- [6] Evrim Guler, Suleyman Uludag, Murat Karakus and Stephen W. Turner, "Virtualized Lab Infrastructure on a Budget for Various Computing and Engineering Courses", IEEE, USA 2012.
- [7] Marisol García-Valls, Tommaso Cucinotta and Chenyang Lu, "Challenges in real-time virtualization and predictable cloud computing", Journal of Systems Architecture, August 2014.

- [8] Oracle VM VirtualBox User Manual.
- [9] V Meera, Meera Mary Isaac and C Balan, “Forensic acquisition and analysis of VMware virtual machine artifacts”, Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 IEEE International Multi-Conference, March 2013.
- [10] Moritz Raho, Alexander Spyridakis, Michele Paolino and Daniel Raho, “KVM, Xen and Docker: A performance analysis for ARM based NFV and cloud computing”, Information, Electronic and Electrical Engineering (AIEEE), 2015 IEEE 3rd Workshop on Advances, Nov. 2015.
- [11] J. Sanders, “Linux, open source, and software’s future”, IEEE Software, Volume: 15, Issue: 5, August 2002.
- [12] GNS3 Documentation, Release 1.4.5dev1, by GNS3 Team, March 2016.
- [13] Mani Subramanian, Timothy A. Gonsalves and N. Usha Rani, “NETWORK MANAGEMENT Principles and Practice”, PEARSON, India, 2010.
- [14] Andrea Bianco, Robert Birke, Fikru Getachew Debele and Luca Giraudo, “SNMP Management in a Distributed Software Router Architecture”, Communications (ICC) IEEE International Conference, June 2011.
- [15] Per Kreuger and Rebecca Steinert, “Scalable in-network rate monitoring”, Integrated Network Management (IM) IFIP/IEEE International Symposium, May 2015.
- [16] A.K.Y. Wong, An Chi Chen, N. Paramesh and P. Rav, “Ontology mapping for network management systems”, Network Operations and Management Symposium IEEE/IFIP, August 2004.
- [17] Vinicius Tavares Guimaraes, Glederson Lessa dos Santos, Guilherme da Cunha Rodrigues, Lisandro Zambenedetti Granville and Liane Margarida Rockenbach Tarouco, “A collaborative solution for SNMP traces visualization”, Information Networking (ICOIN) IEEE International Conference, April 2014.
- [18] Jurgen Schonwalder and Vladislav Marinov, “On the impact of security protocols on the performance of SNMP”, IEEE Transactions on Network and Service Management, Volume: 8, Issue: 1, March 2011.
- [19] Ya-Shiang Peng and Yen-Cheng Chen, “SNMP-based monitoring of heterogeneous virtual infrastructure in clouds”, Network Operations and Management Symposium (APNOMS) IEEE, September 2011.
- [20] Monowar H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, “Network Anomaly Detection: Methods, Systems and Tools, IEEE Communications Surveys & Tutorials, Volume: 16, Issue: 1, June 2013.
- [21] Amir R. Khakpour and Alex X. Liu, “Quantifying and Querying Network Reachability”, Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference, June 2010.
- [22] Corrado Possieri and Andrew R. Teel, “Weak reachability and strong recurrence for stochastic directed graphs in terms of auxiliary functions”, Dec. 2016.
- [23] Nabanita Mandal and Sonali Jadhav, “A survey on network security tools for open source”, Current Trends in Advanced Computing (ICCTAC), IEEE International Conference, March 2016.
- [24] Gabriel Iuhasz and Ioan Dragan, “An Overview of Monitoring Tools for Big Data and Cloud Applications”, Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2015 17th IEEE International Symposium, Sept. 2015.
- [25] Smokeping documentation. Available: <http://oss.oetiker.ch/smokeping/doc/index.en.html>, last visited 2nd of March 2017 8:40 AM.
- [26] Eduard Luchian, Paul Docolin and Virgil Dobrota, “Advanced monitoring of the OpenStack NFV infrastructure: A Nagios approach using SNMP”, Electronics and Telecommunications (ISETC), 2016 12th IEEE International Symposium, Oct. 2016.
- [27] C. C. Li, Z. S. Ji, F. Wang, P. Wang, Y. Wang and Z.C. Zhang, “The network monitoring system based on Cacti for EAST”, Real Time Conference (RT), 2016 IEEE-NPSS, June 2016.
- [28] Samira Homayouni, Vaclav Raida and Philipp Svoboda. “CMPT: A methodology of comparing performance measurement tools”, Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), 2016 8th IEEE International Congress, Oct. 2016.
- [29] MRTG documentation. Available: <http://oss.oetiker.ch/mrtg/doc/index.en.html>, last visited 2nd of March 2017 8:45 AM.
- [30] Ubuntu Server Guide. Available: <https://help.ubuntu.com/lts/serverguide/>, last visited 2nd of March 2017 9:00 AM.
- [31] Putty User Manual. Available: <https://the.earth.li/~sg-tatham/putty/0.63/html/doc/>, last visited 2nd of March 2017 9:15 AM.
- [32] Golap Kanti Dey, Md. Mobasher Ahmed and Kazi Tanvir Ahmmed. “Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol”, Computer and Information Engineering (ICCIE), 2015 1st IEEE International Conference, Nov. 2015.
- [33] Daniel J. Barrett, Richard E. Silverman, and Robert G. Byrnes, “SSH, the Secure Shell the Definitive Guide”, 2nd edition, O’REILLY, May 2005.



**Oula L. Abdulsattar** Oula L. Abdulsattar has B.S. in 2014, M.S. in 2017 from Department of Networks Engineering, College of Information Engineering at Al-Nahrain University Bagdad – Iraq. The work presented in this paper is a part of her M.Sc. project. She is currently working for Zain Mobile Operator in Iraq.



**Emad H. Al-Hemiary** Emad Al-Hemiary graduated from the College of Engineering at Al-nahrain University and have his B.S. (1993), M.S. (1996), and Ph.D. (2001) under the specialization of Electronics and Communications Engineering/Electronics Systems Engineering and Network Design. He participated in the establishment of the College of Information Engineering at Al-Nahrain University and worked as a faculty member there where he published many articles in related fields of Interests.