ISBN: 978-628-96613-1-6. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2025.1.1.2357

Performance and Security Enhancement Evaluation of Virtual Networks in VMware Workstation

Harrison.Carranza[1]; Miguel Bustamante[2]; Aparicio Carranza[3]
[1]*Bronx Community College - CUNY, USA, Harrison.Carranza@bcc.cuny.edu*
[2,3]*Vaughn College of Aeronautics and Technology, USA, Miguel.Bustamante@vaughn.edu, Aparicio.Carranza@vaughn.edu*

Abstract– ***In this growing age of technological improvements, we have seen how communications and management of computer networks have changed. Recently, we have seen the increased use of virtual networking for interacting online and doing remote work. Therefore, we have investigated virtual networking within VMware Workstation Pro with emphasis on performance analysis and security, by implementing ways to improve various aspects of them. Our effort has been to create a virtual network with four virtual machines (VMs) that interact with each other. Then, we conducted performance analysis, created and included optimization strategies, evaluated its security measures, and located potential threats as we simultaneously managed comparing the before and after results made through the extensive testing and validations for potential improvements and effectiveness.***

Keywords-- *Virtual Networking, VMware Workstation, Performance Improvement, Network Security, Network Optimization.*

I. Introduction

Virtualization is a process that allows for more efficient utilization of physical computer hardware and is the foundation of cloud computing [1]. Virtualization, a transformative technology has revolutionized modern computing by enabling the creation of virtual instances of both hardware and software within physical machines. Central to this technology are Virtual Machines (VMs), self-contained computer simulations running within a host machine. These VMs emulate the functions of physical computers, allowing multiple operating systems to run concurrently on a single server or workstation. This technological leap optimizes resource utilization, reduces hardware requirements, and enhances flexibility.

In the context of networking, virtualization takes on a new dimension through the creation of virtual networks. Much like VMs, virtual networks replicate the characteristics of physical networks, facilitating communication among various VMs within a digital ecosystem. Virtual networks are networking systems that emulate a physical network by combining the hardware and software network resources to form a single administrative unit, that are used in various ways ranging from testing and development to creating isolated, controlled environments for a multitude of applications [2].

Our approach is significant as it provides an overview that delves into the intricate landscape of virtual networking within VMware Workstation. Our primary objectives are to optimize performance and strengthen the security of virtual networks by constructing a virtual network environment.
The rest of this report is structured as follows: Section 2, provides background information on virtualization and what VMware Workstation Pro is and does, Section 3, discusses the key utilities that will be used in our solution, Section 4, shows the steps to creating the virtual environment needed to achieve our objectives, Section 5, discusses about what performance and security is before going into Section 6, that breaks down the challenges and failures of our project, the overall discussion about the project is concluded in Section 7.

II. Background on Virtualization

Virtualization is a process that allows for more efficient utilization of physical computer hardware and is the foundation of cloud computing [1]. At its core, virtualization enables the creation of virtual instances of physical hardware, allowing multiple operating systems and applications to run independently on a single physical server or host machine. This technology abstracts and isolates the underlying hardware, making it appear as if each virtual instance has dedicated access to the resources, including CPU, memory, storage, and network, while sharing them efficiently. Virtualization has become a critical component in data centers, cloud computing, and even on personal computers, providing benefits such as improved resource utilization, flexibility, scalability, and enhanced security. Fig. 1, depicts virtualization technology.

In the following subsections we present important descriptive terminologies to enable the readiness of the reader to the world of virtualization and virtual networking.

A. Types of Virtualizations

There are various types of virtualizations, each tailored to specific use cases and requirements. Server virtualization, the most common form, is the process of using software to divide physical hardware into separate unique virtual servers [3]. Each VM operates independently with its own operating system, applications, and configuration. Network virtualization abstracts and virtualizes network resources, allowing for the creation of virtual networks that can be isolated and customized to suit different purposes. Storage

virtualization abstracts physical storage devices, enabling centralized management and dynamic allocation of storage capacity.

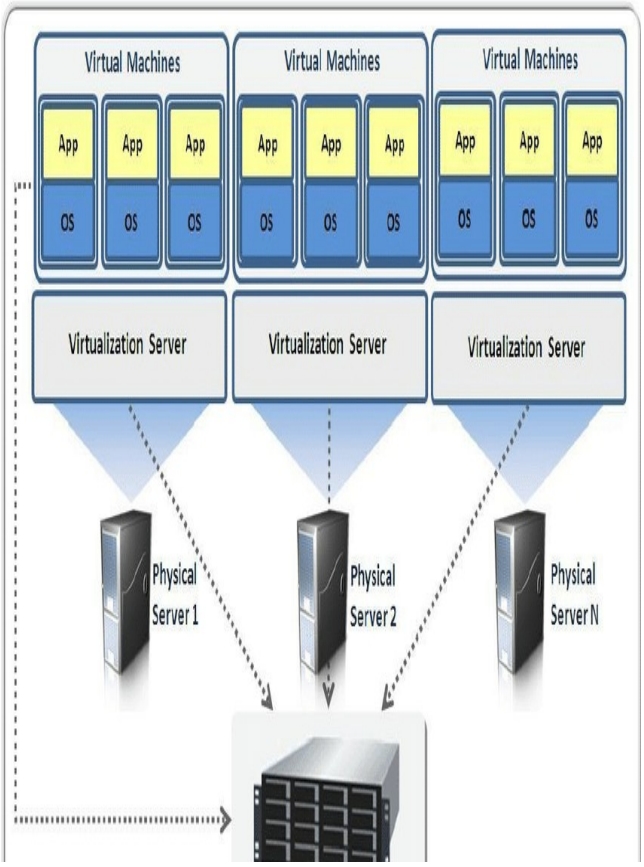

Fig. 1 Virtualization Technology

B. Benefits and Applications of Virtualization

Virtualization offers numerous advantages, making it a fundamental technology in modern computing environments. It enhances resource utilization by allowing multiple workloads to share the same hardware efficiently, reducing hardware costs and energy consumption. Virtualization enables workload mobility and disaster recovery is made easier. In such an environment, the backup and recovery of virtual machines is made feasible by consistent snapshots to provide up-to-date data [4]. Beyond data centers, virtualization extends to desktops, enabling remote access and management of Virtual Desktop Infrastructure (VDI) for improved flexibility and security. Overall, virtualization has transformed the way we deploy and manage IT infrastructure, providing businesses and individuals with greater agility and cost savings.

C. What is VMware Workstation Pro

VMware Workstation, a prominent and versatile virtualization software, stands as a linchpin in the realm of virtualization technology. VMware Workstation supports bridging existing host network adapters and sharing physical disk drives and USB devices with a virtual machine [5]. This robust software platform offers users an array of tools and functionalities to create, configure, and optimize Virtual Machines (VMs) and networks. It enables IT professionals, system administrators, developers, and researchers to harness the full potential of virtualization within a user-friendly and feature-rich environment. VMware Workstation allows users to create and manage VMs, each operating with its own operating system and applications, seamlessly within a single physical computer. Users can customize the virtual hardware, allocate resources, and configure networking options to simulate complex and diverse network scenarios. Moreover, the software facilitates the creation of snapshots, which capture the state of a virtual machine at a specific point in time, enabling easy restoration and testing. VMware Workstation serves as a cornerstone for proof of concept research and practical application of virtual networks, offering a stable and versatile platform to design, optimize, and evaluate virtualized network environments.

III. Key Utilities

In the context of virtual networking on a Windows platform, several key tools and built-in Windows applications are instrumental in achieving our objectives. To manage virtualization efficiently, we rely on VMware Workstation Pro as the central hub, facilitating the seamless setup and administration of virtual machines and networks within the Windows environment. Within these VMs, various operating systems are employed, with pfSense being particularly notable. When operated within a VMware environment on Windows, pfSense transforms into a powerful firewall and router, enhancing the security perimeter of the virtual network.

To evaluate network performance, Wireshark serves as our primary tool, providing valuable insights into metrics such as throughput and latency. Wireshark is a network protocol analyser, or an application that captures packets from a network connection [6]. For comprehensive security assessments, we utilize Nessus, which conducts thorough scans for vulnerabilities across the network, ensuring no aspect of our quest for a secure virtual environment is overlooked.

Meanwhile, PassMark Performance Test aids in gauging the overall system performance. Passmark Performance Test is an award winning PC hardware benchmark utility that allows everybody to quickly assess the performance of their computer and compare it to a number of standard 'baseline' computer systems [7], Prime95 is employed for CPU stress testing and stability assessment, Perfmon serves as a built-in Windows application for monitoring various performance metrics, and Windows Security features are harnessed to bolster security measures. Together, these tools, combined with built-in Windows utilities, form the backbone of our solution implementation, ensuring both its performance and security are maintained at the highest standards.

IV. Virtual Network Setup

Below we detail the steps to implement our virtual environment:

Step 1:

- *Understand the VMware Workstation Pro Environment*
- *Familiarize yourself with the VMware Workstation Pro interface.*
- *Explore tools and functionalities offered for virtual networking.*

Step 2:

- *Define the Network Architecture*
- *Plan to set up four Virtual Machines (VMs) within the VMware Workstation environment.*
- *Decide on the roles and responsibilities of each VM (e.g., Web Server, Database Server, Application Server, etc.).*

Step 3:

- *Create the Virtual Machines*
- *Allocate appropriate resources to each VM, including CPU, memory, and storage.*
- *Install the desired operating systems and applications on each VM.*

Step 4:

- *Configure Network Settings for Each VM*
- *Establish the mode of network connection for each VM: NAT (Network Address Translation), Bridged, or Host-only.*
- *Assign IP addresses, either statically or through DHCP, ensuring no conflicts in IP assignments.*

Step 5:

- *Interconnect the VMs*
- *Utilize virtual switches and routers within VMware Workstation to facilitate communication between the VMs.*
- *Ensure proper routing and DNS configurations for seamless data flow.*

Step 6:

- *Test Basic Connectivity*
- *Conduct simple "ping" tests to check if VMs can communicate with each other.*
- *Verify that all VMs can access external networks if required.*

Step 7:

- *Implement Network Segmentation (Optional)*
- *If necessary, divide the network into smaller segments for optimized performance and security.*
- *Configure virtual firewalls to regulate traffic between these segments.*

Step 8:

- *Monitor and Validate Network Performance*
- *Monitor the virtual network's performance using built-in VMware tools.*
- *Identify any potential bottlenecks or performance issues.*

Step 9:

- *Conduct a Preliminary Security Assessment*
- *Use tools like Nessus or OpenVAS to check the initial security posture of the virtual network.*
- *Address any vulnerabilities or issues discovered.*

Step 10:

- *Document all configurations, settings, and changes made during the network setup.*
- *Maintain a change log to track modifications and updates for future reference.*

Fig. 2 and Fig 3 show the results of the process of setting up the virtual network.

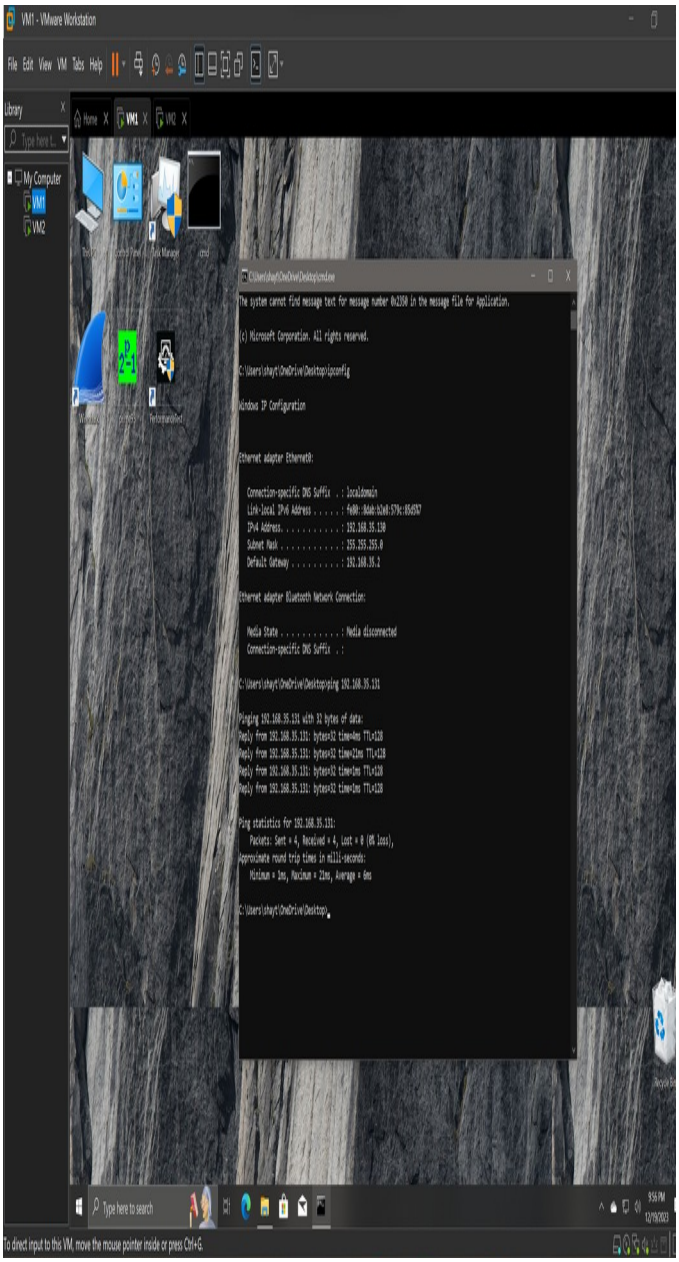

Fig. 2 Network Setup

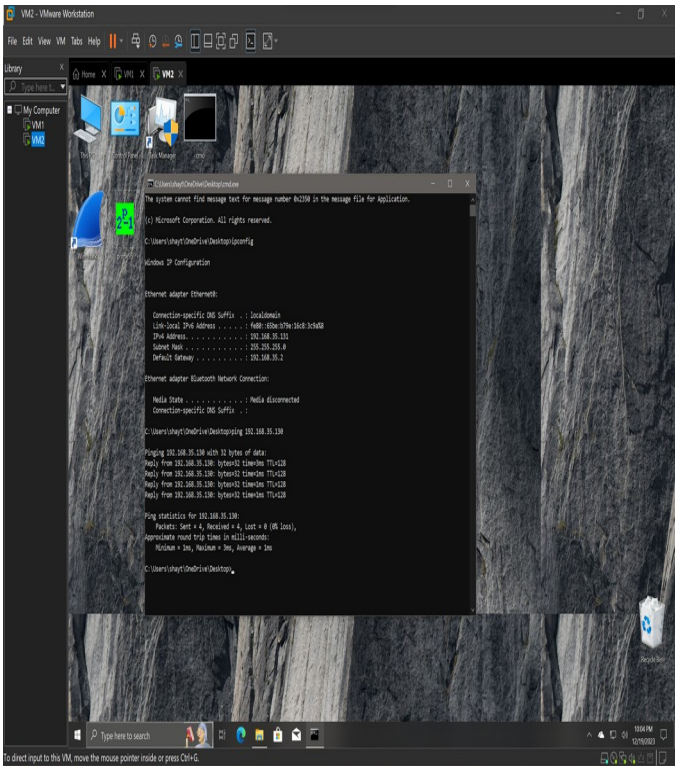

Fig. 3 Displaying Windows IP Configuration

V. Performance and Security

The challenge in crafting an efficient virtual network within VMware Workstation Pro lies at the intersection of performance and security. Both elements are paramount, but they often pose competing challenges. From a performance perspective, our virtual network's design prioritized seamless communication between the four VMs, ensuring that data transmission occurred with minimal latency and maximum throughput. Benchmarking tools were employed to quantify these metrics, providing a comprehensive view of how well the network responded to various loads and tasks. Additionally, strategies like network segmentation were contemplated not only for enhanced performance by reducing unnecessary broadcast traffic but also as a conduit for improved security.

Security, undeniably, stands as a cornerstone in the virtual networking landscape, especially in an era marked by escalating cyber threats. While constructing our network, it was essential to ascertain its resilience against potential vulnerabilities. An initial assessment using tools like Nessus unveiled areas demanding attention. Consequently, robust security measures, including firewalls and intrusion detection systems, were incorporated. These systems acted as vigilant guards, monitoring network traffic for any malicious activities or anomalies. Furthermore, by segmenting the network, which is the process of dividing a computer network into smaller subnetworks, or segments [8], we introduced an additional layer of security, ensuring that even if one segment faced a threat, the entirety of the network would not be compromised, as shown in Fig 4 and Fig 5. This dual focus on performance and security ensures that our virtual network operates at peak efficiency without compromising its defensive stance against cyber threats.

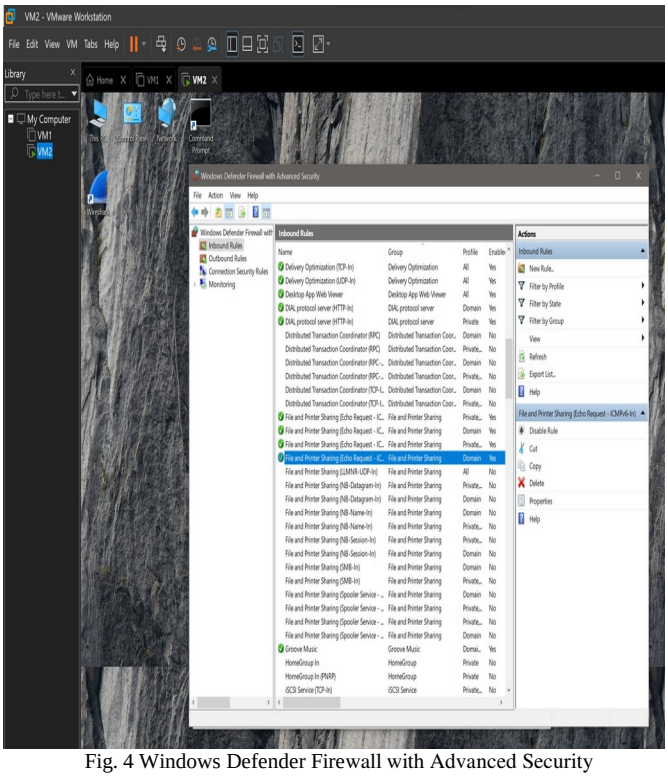

Fig. 4 Windows Defender Firewall with Advanced Security

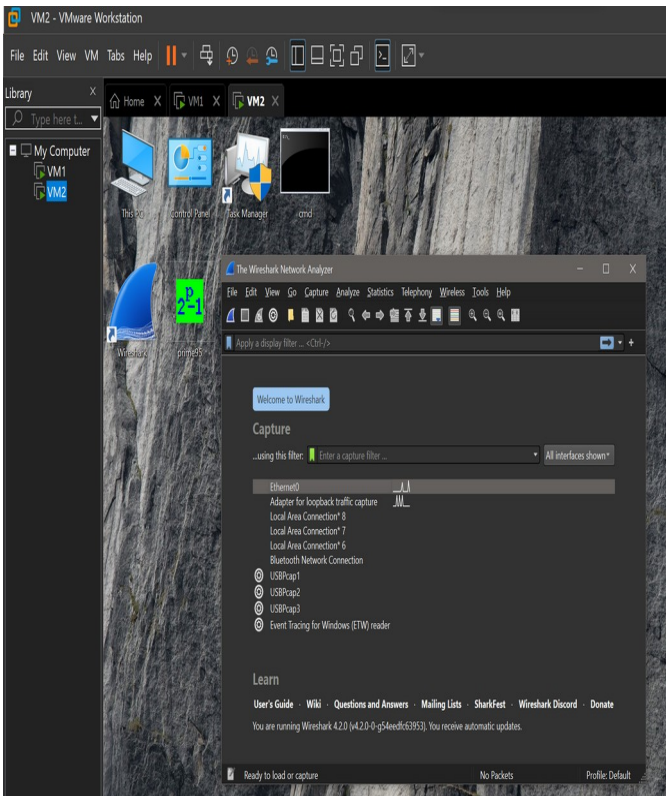

Fig. 5 Wireshark Network Analyzer

VI. Challenges and Failures in Improving VM Performance and Security

Our project aimed at enhancing the performance and security of Virtual Machines (VMs) running Windows 10 on a Surface Pro 6 with standard settings encountered significant challenges and ultimately faced failure. The endeavour, initially well-intentioned, faced insurmountable hurdles that led to unexpected outcomes, despite efforts to optimize performance and security.

A. *Resource Limitations and Hardware Constraints*

One of the primary reasons for the project's failure was the limited hardware resources of the Surface Pro 6 used as the host machine. With only 8GB of RAM and a dual-core Intel Core i5 processor, the Surface Pro 6 struggled to handle the resource-intensive demands of multiple Windows 10 VMs, each allocated with 2GB of memory and processor cores. The VMs' resource requirements exceeded the available capacity, leading to frequent crashes, overworking the host, and causing instability. This constrained environment severely limited the ability to implement security and performance enhancements effectively.

B. *Inadequate Network Adapter Configuration*

The use of Network Address Translation (NAT) for network adapters in the VMs posed another significant challenge. NAT, while useful for basic networking, can introduce performance bottlenecks and security concerns when multiple VMs communicate extensively with external networks. The Surface Pro's NAT configuration may not have been well-suited to handle the network traffic generated by the VMs, further degrading performance and potentially impeding security enhancements that relied on effective network communication.

C. *Limited Impact of Software Changes*

Despite making changes aimed at improving performance and security, the project did not yield the desired results. This outcome could be attributed to the inherent limitations of the host hardware. Enhancements within the VMs may have been overshadowed by the hardware constraints, rendering them ineffective in significantly enhancing the overall system. Additionally, the standard Windows 10 settings, such as 2GB of memory and limited processor cores, may have inherently limited the VMs' capabilities, regardless of software changes.

D. *Ineffectiveness of Wireshark for Network Monitoring*

The inclusion of Wireshark as a network monitoring tool in the solution brought about unexpected challenges. While Wireshark is a powerful tool for packet analysis and network monitoring, its continuous and comprehensive packet capture placed a considerable load on the already resource-constrained Surface Pro 6 host. The extensive packet analysis required substantial CPU and memory resources, contributing to the host's overworking and frequent crashes. Furthermore, the results obtained from Wireshark's packet captures did not provide actionable insights due to the limited capacity of the VMs and the Surface Pro 6 itself. This ineffective network monitoring hindered efforts to identify and resolve network-related performance and security issues. The results are shown in Fig 6 and Fig 7.

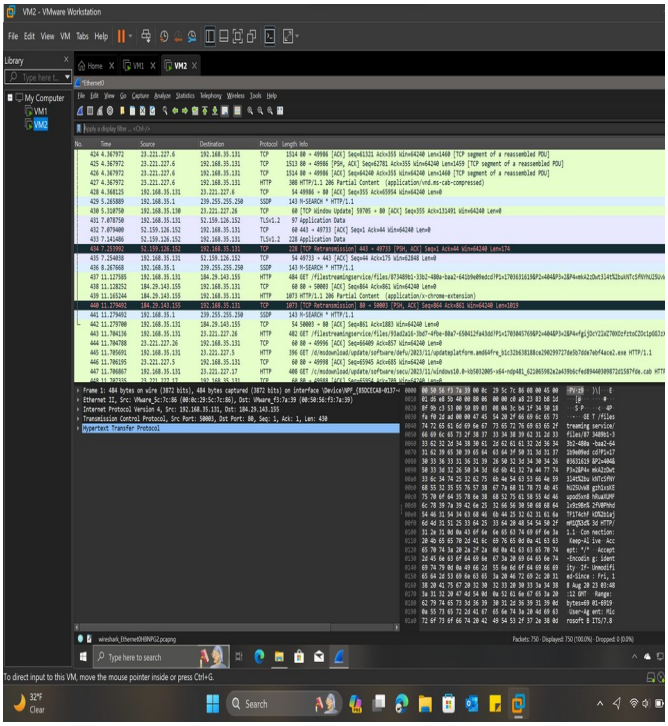

Fig. 6 Wireshark Packet Capture

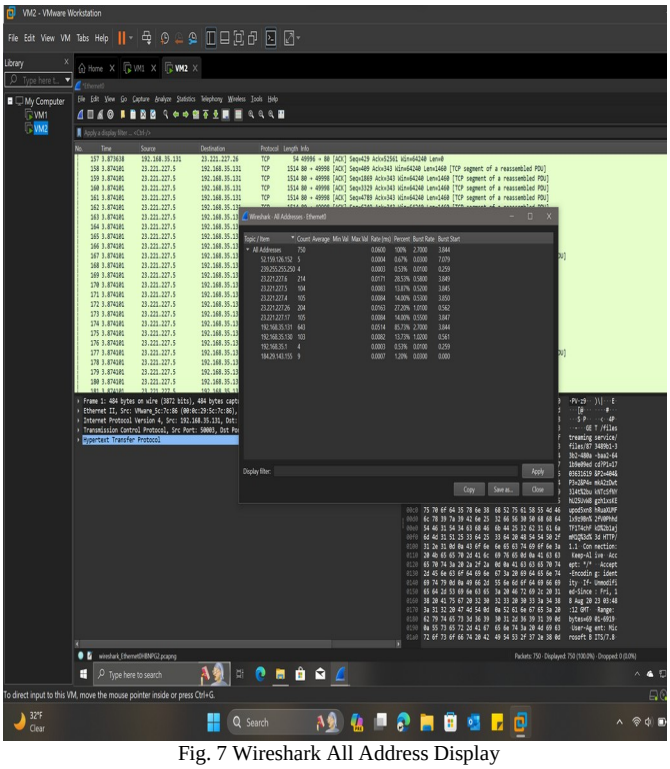

Fig. 7 Wireshark All Address Display

E. PassMark PerformanceTest and Resource Constraints

The incorporation of PassMark PerformanceTest for evaluating overall system performance encountered significant roadblocks. While the tool is valuable for assessing system capabilities comprehensively, it demands substantial computing resources. Running the tests on VMs with limited memory (2GB) and a constrained processor exacerbated the issue, as the VMs struggled to execute the benchmarks effectively. The results obtained from the performance tests did not provide a meaningful basis for improvements, as they were heavily influenced by the hardware constraints. Consequently, the VMs' performance remained suboptimal, and the intended performance enhancements fell short of expectations.

F. Prime95 and CPU Stress Testing Limitations

The project's inclusion of Prime95 for CPU stress testing and stability assessment unveiled unforeseen challenges. Prime95 is a valuable tool for evaluating CPU performance and system stability, but it pushed the limited capabilities of the Surface Pro 6 to their limits. The CPU-intensive stress tests induced high levels of thermal throttling, causing the host's processor to reduce its clock speed to prevent overheating. This not only hindered the VMs' performance but also contributed to the host's instability and frequent crashes. Consequently, the CPU testing yielded inconclusive results, as the CPU's performance was heavily impacted by thermal constraints, preventing meaningful insights into the VMs' capabilities and potential security enhancements.

VII. Conclusion

We embarked on a journey through the intricate landscape of virtual networking within VMware Workstation, with the primary goals of optimizing performance and bolstering security within a virtual network environment. However, as revealed through the challenges and limitations encountered, the project faced formidable hurdles that ultimately led to incomplete results. The endeavour was marred by the constrained resources of the host system, a Surface Pro 6, which struggled to accommodate the demands of multiple VMs running under standard settings. Network configuration issues, compounded by the use of NAT, introduced performance bottlenecks, while tools such as Wireshark, PassMark Performance Test, and Prime95, though powerful in their own right, strained the limited hardware resources further. These challenges highlighted the critical importance of aligning our project objectives with the available hardware capabilities, ultimately serving as valuable lessons for future endeavours in the realm of virtual networking optimization and security enhancement within VMware Workstation.

Acknowledgment

This research has been supported by the grant: DOE Title V P031S200139

References

[1] IBM, “What is Virtualization? | IBM,” www.ibm.com. https://www.ibm.com/topics/virtualization

[2] “What is a Virtual Network?,” Server and Cloud Blog, https://www.parallels.com/blogs/ras/what-is-a-virtual-network/

[3] WhatServerVirtualization?,” CDW.com https://www.cdw.com/content/cdw/en/as/datacenter/what-is-server-virtualization.html

[4] C. Ayuya, “Virtualization: Benefits, drawbacks and defining features,” TechRepublic, https://www.techrepublic.com/article/virtualization-benefits-drawbacks-defining-features/

[5] “VMwareWorkstation,”Wikipedia,https://en.wikipedia.org/wiki/VMware_WorkstationVMware

[6] CompTIA, “What Is Wireshark and How to Use It,” CompTIA, 2020. https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

[7] “Passmark PerformanceTest,” TechSpot, https://www.techspot.com/downloads/1110-passmark-performance test.html

[8] “What is Network segmentation? Why Is It Important?,” www.celona.io. https://www.celona.io/network-architecture/network-segmentation#benefits-of-network-segmentation