Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.11, No.4, 2020
www.iiste.org

Simulating Cloud Environment in Single Host Machine by Applying Virtual Switches in VMware

Elias Bassa Badacho
(M.Tech in Computer Science and Engineering)
Department of Computer Science (Lecturer)
Wolaita Sodo University, Ethiopia
P.O. Box 138, Wolaita Sodo, Ethiopia

Abstract
Computer virtualization in its simplest form is where one physical Server simulates being several separate servers and it allows one server to handle various functions or processes. It enables a single system to concurrently run multiple isolated virtual machines (VMs), operating systems or multiple instances of a single operating system and It minimizes resource requirements of hardware and software, minimizes power consumption, increases utilizations, maximizes hardware processing power, minimizes the work costs in the data center and maximizes the usage of available resources. Virtualization is a partitioning of single physical server into multiple logical servers. This paper work highly focuses on the configuration of virtual switch, Virtual Bridge, Virtual Host adapters and NAT devices. This paper work is implemented by using one host computer, one virtual bridge, two virtual Ethernet switches and three virtual machines.
Keywords: VMware, Virtualization, Public cloud, Private cloud, Virtual cloud, community cloud, Hyper-V, VMNet, Virtual switch
DOI: 10.7176/CEIS/11-4-02
Publication date: June 30th 2020

1. Introduction

Cloud Computing is defined by the United States National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network accesses to a shared pool of configurable computing resources such as networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. It is having characteristics of on-demand self-service, broad network access, resource pooling, rapid elasticity and payment per usage of various business models. [1] It may have different definitions according to different scholars, expertise and system user for instance it can be defined as the newly emerging computing technology that can deliver the hosted services such as Virtual machines, storage devices,.. etc to its users such as customers, data owners, Trusted Third Party auditors and cloud service providers through intranet or internet as an utility. Cloud computing has a number of standardized service and deployment models. Again it allows the users and enterprises with various capabilities to store and process their data in either privately owned cloud or on a third-party server in order to make data accessing mechanisms much more easy and reliable. And it relies on sharing of resources to achieve coherence and economy of scale.

Computer virtualization in its simplest form is where one physical Server simulates being several separate servers and it allows one server to handle various functions or processes. One of these simulated servers is known as a virtual machine [2]. It enables a single system to concurrently run multiple isolated virtual machines (VMs), operating systems or multiple instances of a single operating system [3]. It minimizes requirements of hardware and software, minimizes power consumption, increases utilizations, maximizes hardware processing power, minimizes the work costs in the data center and maximizes the usage of available resources. Virtualization is a partitioning of single physical server into multiple logical servers. Once the physical server is divided, each logical server behaves like a physical server and can run an operating system and applications independently. Many popular companies like VMware and Microsoft provide virtualization services, where instead of using your personal PC for storage and computation, you use their virtual server. They are fast, cost-effective and less time consuming.

2. Purposes of Virtualization

There are several uses for virtualization in the areas of cloud computing technologies. It is mainly used for three main purposes:

A. Network Virtualization

It is a method of combining the available resources in a network by splitting up the available bandwidth into channels, each of which is independent from the others and each channel is independent of others and can be assigned to a specific server or device in real time.

B. Storage Virtualization

It is the pooling of physical storage from multiple network storage devices into what appears to be a single storage device that is managed from a central console. Storage virtualization is commonly used in storage area networks (SANs).

C. Server Virtualization

It is the masking of server resources like processors, RAM, operating system so on, from server users. The intention of server virtualization is to increase the resource sharing and reduce the burden and complexity of computation from users. **Multi-tenancy** refers to the ability of a cloud provider to deliver software as a service solution to multiple client organizations or tenants from a simply shared instance of software. The cloud user's information is virtual, not physically, separated from other users. The major benefit of this model is cost-effectiveness for cloud providers. Some issues or risks with the model within the cloud users include the potential for one user to be able to access data which belonging to other users and it is difficult to backup and restore data in this model.

3. Cloud computing Architecture

Cloud computing is currently the buzzword in IT industry, and many are curious to know what cloud computing is and how it works. More so because the term CLOUD is intriguing and some people even wonder how do clouds that rain can even remotely be used in Computing. The generally accepted definition of Cloud Computing comes from the National Institute of Standards and Technology (NIST), essentially says that; Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [4, 5, 6].

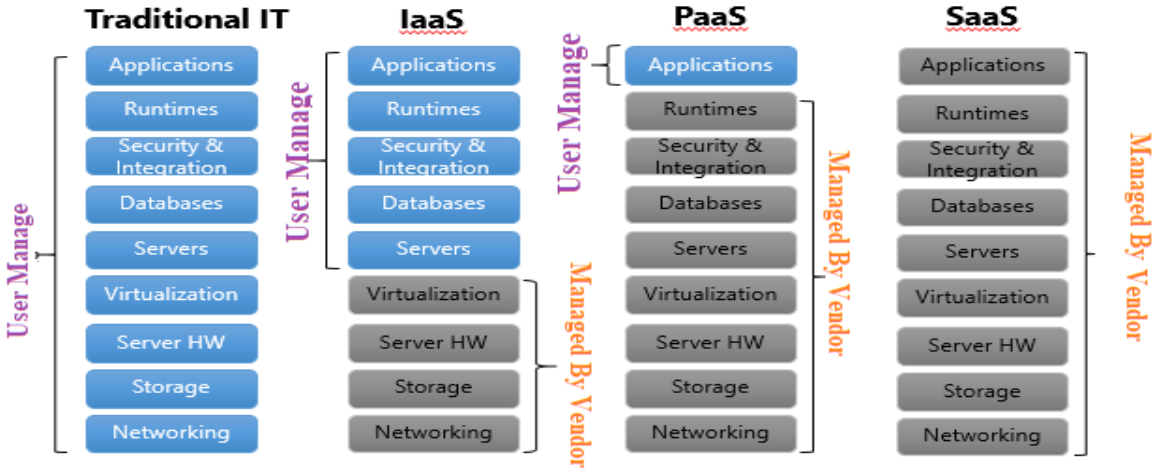


Figure 1 Cloud Architecture

Cloud computing characteristics, NIST [4, 5] has made effort to provide a unified way to define cloud computing and its main functionality.

4. Cloud Computing Service Deployment Models and its architecture

Cloud infrastructure and services may be operated or deployed in different ways depending on customer needs and requirements, as some cloud customers have security and privacy concerns over their sensitive data. They would rather not share cloud resources with other customers for security concerns which might cost more money, or other customers are interested in less expensive solutions. There are five main architectural deployments of the cloud computing services for cloud clients, those are mentioned and explained as below:

4.1 Cloud as a Service (CaaS)

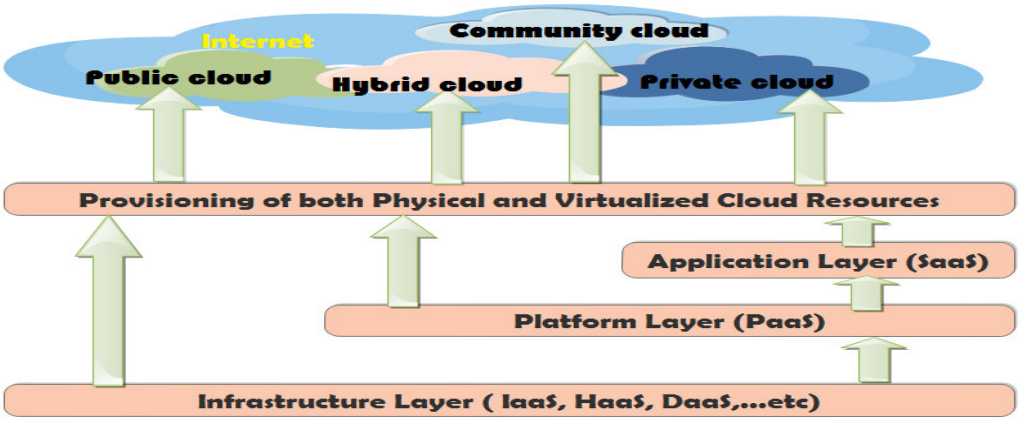


Figure 2 cloud as a service

A. Public Cloud

It is the cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization or some combination of them and it exists on the premises of the cloud provider. This type of deployment provides cloud services to the public under some sort of service level agreement. This model is considered one of the most recognizable models of cloud computing for many consumers, where cloud services are provided in a virtualized environment, and physical resources are shared among many users and are accessible over the public network. Public clouds usually provide services to multiple clients using the same shared infrastructure. Public cloud services may be free. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Public cloud model has the following features and benefits in the cloud system [7]. These are highly scalable resources because cloud resources are available on demand, high availability of cloud services and resources; reduces cost, flexible services and location-independent access to services.

B. Private Cloud

This type of deployment basically gives organizations the ability to create a remote data center. This model often gives the highest level of control from a security perspective. A private cloud is a type of cloud computing architecture that delivers services similar to the public cloud model such as scalability and flexibility, but unlike public clouds, which deliver services to multiple organizations, a private cloud is dedicated to a single organization. Public and private cloud deployment models are different, as public cloud shares a computing infrastructure across many users or businesses. However, these shared resources are not suitable for every business, such as businesses with mission-critical operations, security concerns, availability, or management requirements. Instead, these businesses can provision a portion of their existing data center as an on-premises or private cloud [8].

C. Virtual Private Cloud

A private cloud classified as virtual cloud consists of on demand shared computing resources which can be allocated to customers within a public cloud environment. There is a certain level of isolation between different organizations and customers using the resources. This type of deployment utilizes virtual private networks (VPNs), to establish a secure connection with the cloud provider's network. Virtual private networks provide a secure data transfer over the Internet and they also ensure that each customer's data is kept isolated from other customers' data both in transit and in the cloud provider's network. This is accomplished by the use of security policies and some or all of the following processes. Those processes are highly capable for encrypting, tunneling, or possibly allocating dedicated virtual local area networks (VLANs) or private IP addresses for each customer [9].

D. Community Cloud

This type of cloud deployment model provides a cloud computing solution to a limited number of organizations' that are managed and secured commonly by all the participating parties or a third-party managed service provider. Usually, this type of deployment includes certain organizations with similar requirements and/or policies that can benefit those organizations from the same infrastructure, or organizations that are working on joint projects, researches, or applications that require a central computing facility [10].

E. Hybrid Cloud

The hybrid cloud model consists of a combination of public and private cloud resources, where the public and private cloud infrastructures operate independently and usually communicate over an encrypted connection as shown Figure 2. It is important to understand that the public and private clouds are distinct and independent

elements. Usually, organizations store critical or important data in the private cloud, and the public cloud can use the private cloud to get computational resources that applications rely on, which enhances security and decreases the data exposure to an accepted minimum. Hybrid clouds have many benefits and bring many solutions, as this deployment model is suitable for creating a backup when failover situations occur, balance heavy workloads, and can be much more cost effective than private clouds [11].

Benefits of Cloud Computing

The potential for cost saving is the major reason of cloud services adoption by many organizations. Cloud computing gives the freedom to use services as per the requirement and pay only for what you use. Due to cloud computing it has become possible to run IT operations as an outsourced unit without much in-house resources. Following are the benefits of cloud computing:

- Lower IT infrastructure and computer costs for users
- Improved performance
- Fewer Maintenance issues
- Instant software updates
- Improved compatibility between Operating systems
- Backup and recovery
- Performance and Scalability
- Increased storage capacity
- Increase data safety

5. Literature Reviews and Related Works

In essence, system virtualization is the use of an encapsulating software layer that surrounds or underlies an operating system and provides the same inputs, outputs, and behavior that would be expected from physical hardware. The software that performs this is called a Hypervisor, or Virtual Machine Monitor (VMM) [12]. System virtualization is widely used for a variety of applications, such as, among other things, the consolidation of physical servers [Scott et al. 2010], isolation of guest OSs, and software debugging [Bratus et al. 2008]. By utilizing a VMM to mediate between the OS and the hardware, virtualization changes the one-to-one mapping of OSs to hardware to many-to-many. Virtualization is the basic concept behind the Cloud. We no longer refer to the physical machine but rather to the virtual machine [13]. Virtualization can be considered IT asset optimization. It is gaining popularity in enterprise environments as Infrastructure as a Service i.e IaaS. For Data Centers, SMB and larger enterprises virtualization offers a solution for resource management (e.g., servers, storage devices, network devices, desktops and applications) which helps to achieve greater system utilization, lowering total cost and ease of management. Many experts agree that the current generation of enterprise information systems configured using dedicated resources and high ongoing support costs. Virtualization is the technology that allows multiple operating system images running all at once by using only one piece of hardware [14, 15].

6. Implementation of Virtualization and VMware Workstation and Techniques

Virtualization is the key to unlock the Cloud system, what makes virtualization so important for the cloud is that it decouples the software from the hardware. For example, PC's can use virtual memory to borrow extra memory from the hard disk. Usually hard disk has a lot more space than memory. Although virtual disks are slower than real memory, if managed properly the substitution works perfectly. Likewise, there is software which can imitate an entire computer, which means one computer can perform the functions equals to N computers.

- VMware Workstation and its internal architecture

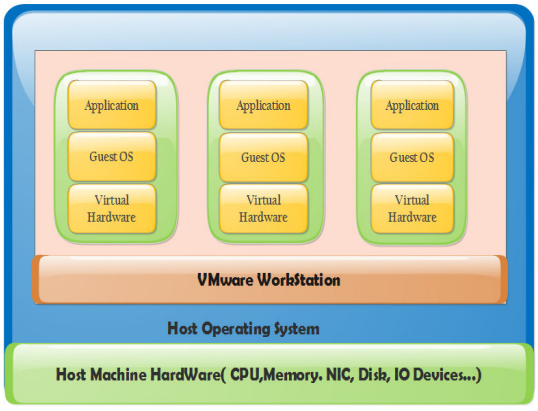


Figure 3 VMware Workstation

Logical Devices in Virtual Network and Configurations

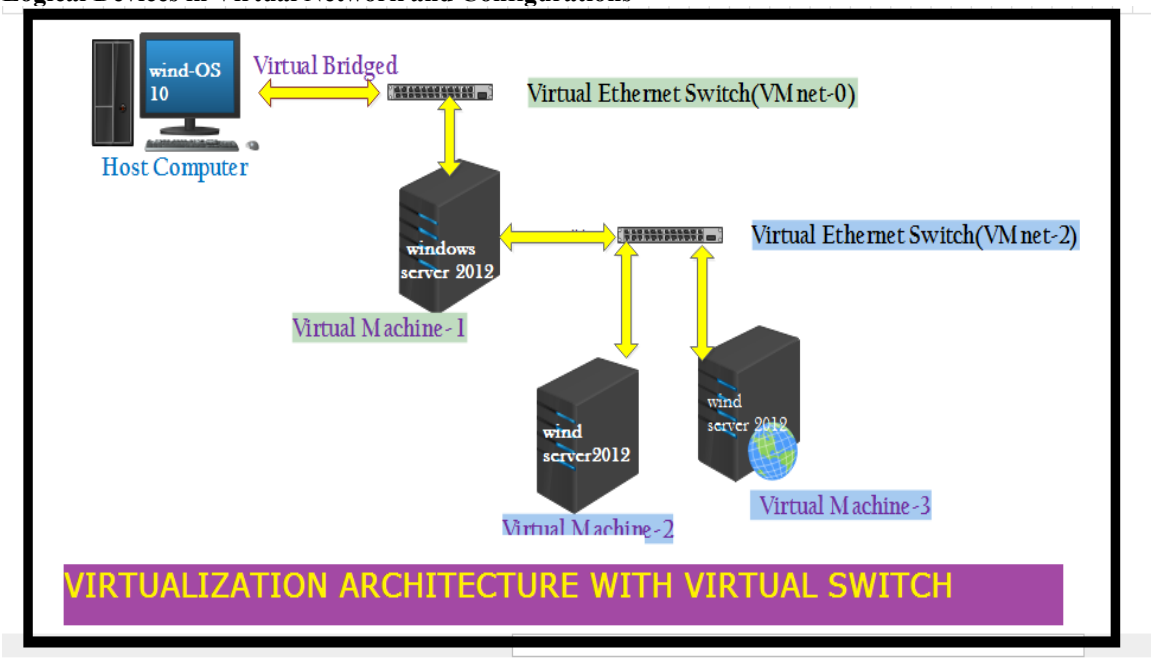


Figure 4 Architecture of Virtual machine with Virtual Switch

A. Virtual switch

The virtual switch is similar to the physical switch that means it also used to connect different virtual network components together within the virtual machines or virtual software. This device lets the users to connect up to nine different virtual switches in VMware Workstation and VMware has capability to connect one or more virtual machines to a single logical switch.

- Some of switches and networks in VMware have named configurations
  - Bridged network uses VMnet0.
  - Host-only network uses VMnet1.
  - NAT network uses VMnet8.
- The remaining named networks are VMnet2, VMnet3, VMnet4, VMnet5 and so on.

B. Bridge

It is also a logical virtual network device that lets to connect virtual machine to the LAN that is used by the host computer that means this device connects the virtual network adapter in virtual machine to the physical Ethernet adapter in physical host machine or computer. While we create a new virtual machine using bridged networking, the bridge is set up automatically and additionally, user can set up additional virtual bridges for custom configurations that require connections to more than one physical Ethernet adapter on the host computer.

C. Host Virtual Adapter

It is a virtual Ethernet adapter that is visible to the host Operating System as a VMware virtual Ethernet adapter on a windows host and it is known as a host-only interface on the Linux host. Most of the host virtual adapters let to make communication between the physical host computer and the virtual machines on the host computer. The host virtual adapter is used in host-only and NAT configurations but it is not connected to any external network unless we set up special software on the host computer for example to proxy server which used to connect host-only adapter to physical network adapter.

D. NAT Device

It is a device that used to connect virtual machines to the external network when for the system has only single IP Network Address on the physical network in host computer. And it is also used to connect virtual machines to the Internet through a dial-up connection on the host computer by using host computer's Ethernet Adapter or WiFi Ethernet Adapter. In the same way it is again used to connect Non-Ethernet networks such as Token Ring or ATM (Asynchronous Transfer Mode). NAT provides the ways for virtual machines to use all Client Applications those are available to any type of network connection in which connection that support TCP/IP. NAT network performs the following tasks:

- It translates the address of virtual machine in a private VMnet network to that of the host computer/machine.
- It uses the host's own network resources to connect to the external network.
- Any TCP/IP network resource to which the host has access should be available through the NAT connection.
- It provides a transparent, easy to configure way for virtual machines to gain access to network resources.

7. Components of Host Computer and Its Connection

A. Host Computer

It has an adapter on the NAT network (identical to the host-only adapter on the host-only network). And it allows the host and the virtual machines to communicate with each other for such purposes as file sharing.

B. NAT Network

The NAT network, never forwards traffic from the host adapter.

C. DHCP on the NAT Network

It provides easy way to configure network and DHCP server installed automatically from VMware Workstation. Virtual machines running on the network with the NAT device can dynamically obtain their IP addresses by sending out a DHCP request. In addition to the IP address, the DHCP server on the NAT network also sends out additional configuration information that enables the virtual machine to operate automatically. This information includes the default gateway and the DNS server**.** This causes all IP packets destined for the external network and DNS requests to be forwarded to the NAT device.

D. DNS on the NAT Network

The NAT device acts as a DNS server for the virtual machines on the NAT network. Actually, the NAT device is a DNS proxy and merely forwards DNS requests from the virtual machines to a DNS server that is known by the host. Responses come back to the NAT device, which then forwards them to the virtual machines. If they get their configuration information from DHCP, the virtual machines on the NAT network automatically uses the NAT device as the DNS server. However, the virtual machines can be statically configured to use another DNS server.

E. External Access from the NAT Network

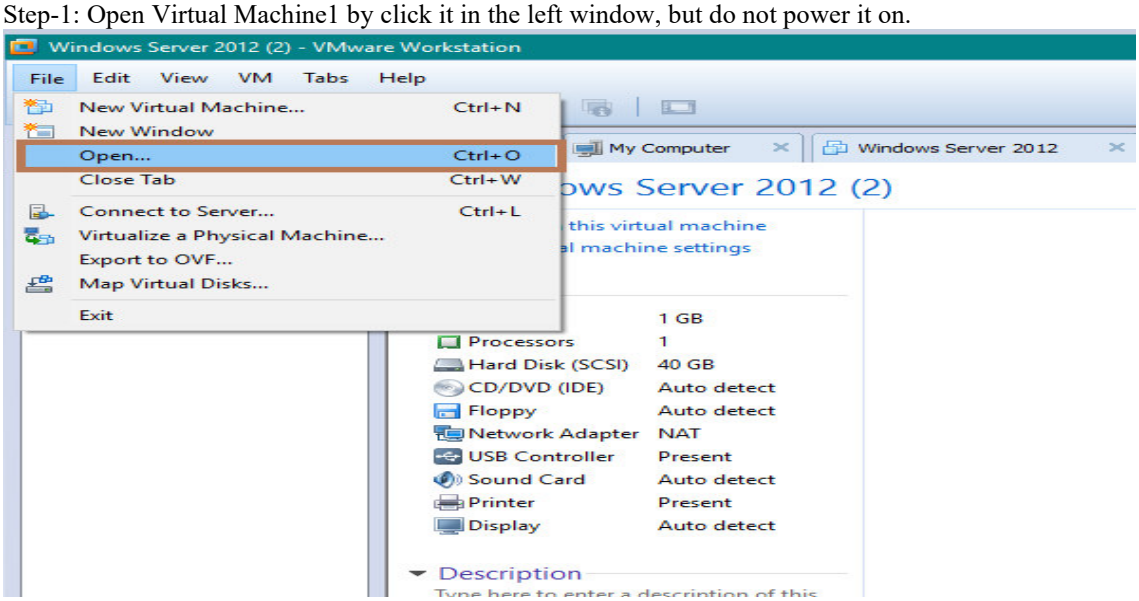
In general, any protocol using TCP or UDP can be used automatically by a virtual machine on the NAT network so long as the virtual machine initiates the network connection. This is true for most client applications such as Web browsing, Telnet, passive-mode FTP and downloading streaming video. Additional protocol support has been built into the NAT device to allow FTP and ICMP echo (ping) to work completely transparently through the NAT. On the external network to which the host is connected, any virtual machine on the NAT network appears to be the host itself, because its network traffic uses the host's IP address. It is able to send and receive data using TCP/IP to any machine that is accessible from the host. Before any such communication can occur, the NAT device must set up a mapping between the virtual machine's address on the private NAT network and the host's network address on the external network. When a virtual machine initiates a network connection with another network resource, this mapping is created automatically. The operation is perfectly transparent to the user of the virtual machine on the NAT network. No additional work needs to be done to let the virtual machine access the external network.

F. DHCP Server

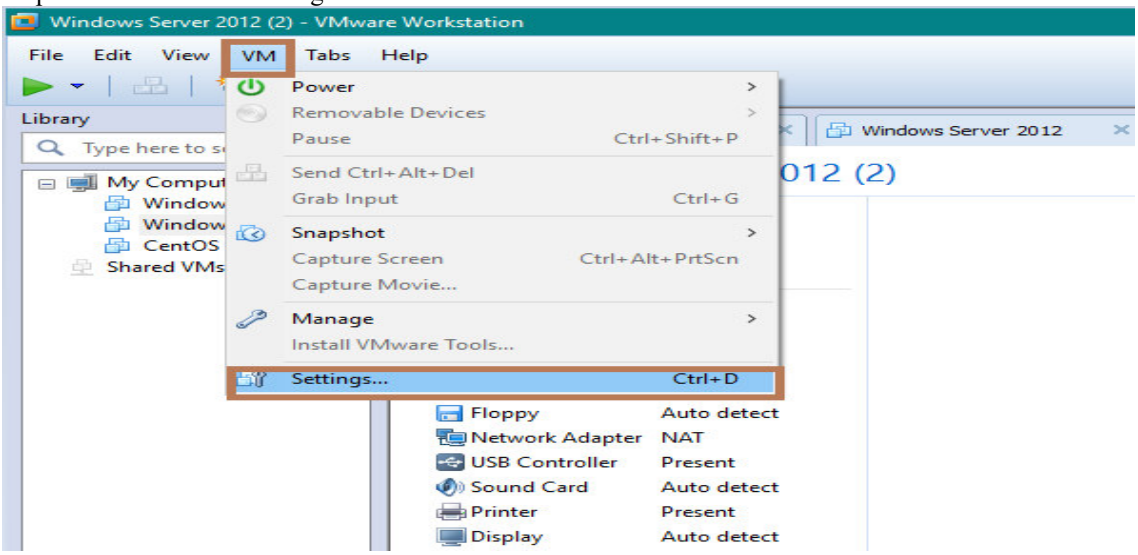
The DHCP (dynamic host configuration protocol) server provides IP network addresses to virtual machines in configurations that are not bridged to an external network for example, host-only and NAT configurations. VMware Workstation virtualization software that is very useful to develop and test the system that runs in the real world network. It is used to test database server system connection through a firewall to an external network. And also the administrators' computer database server connected through second firewall. In this project work includes three virtual machines within a single host computer with three guest windows server 2012 operating system in a the single windows 10 host operating system. The virtual machines are created by using virtual machine settings editor in VMware Workstation to connect and adjust their virtual network adapters. In the VMware Workstation, the Bridged Adapter makes virtual machine 1 which is worked as the bridged networking and through this network the virtual machine one connected to the host computer's network adapter. The second one is Custom Adapter that creates connection between virtual machine1 and VMnet2. This adapter again used to make connection between virtual machine1 and virtual machine2. The last one is Virtual machine3 which has two Custom Network Adapters from these two adapters one is used to connect virtual machine 3 with VMnet2 and the second is used to connect virtual machine3 with VMnet3. Eventually this work configured IP Addresses for these adapters to make real communication between devices.

8. Implementation of Virtualization and steps

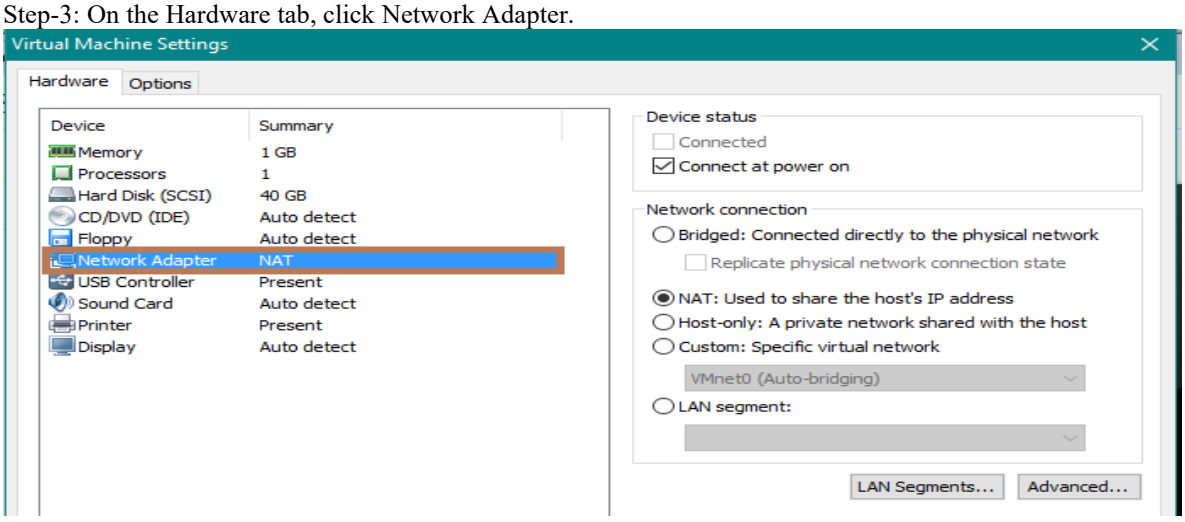
Step-1: Open Virtual Machine1 by click it in the left window, but do not power it on.



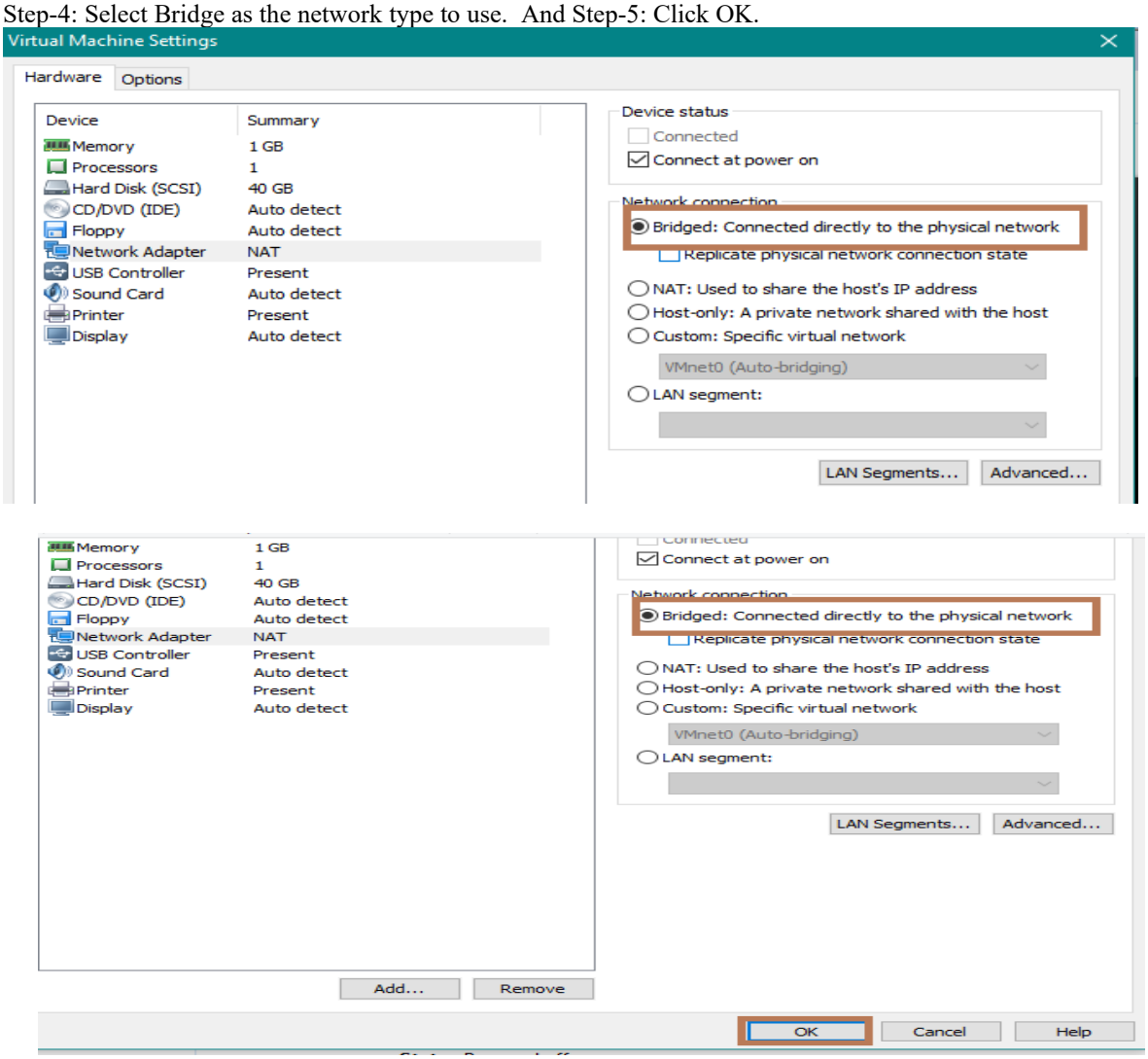
Step-2: Choose VM →Settings.



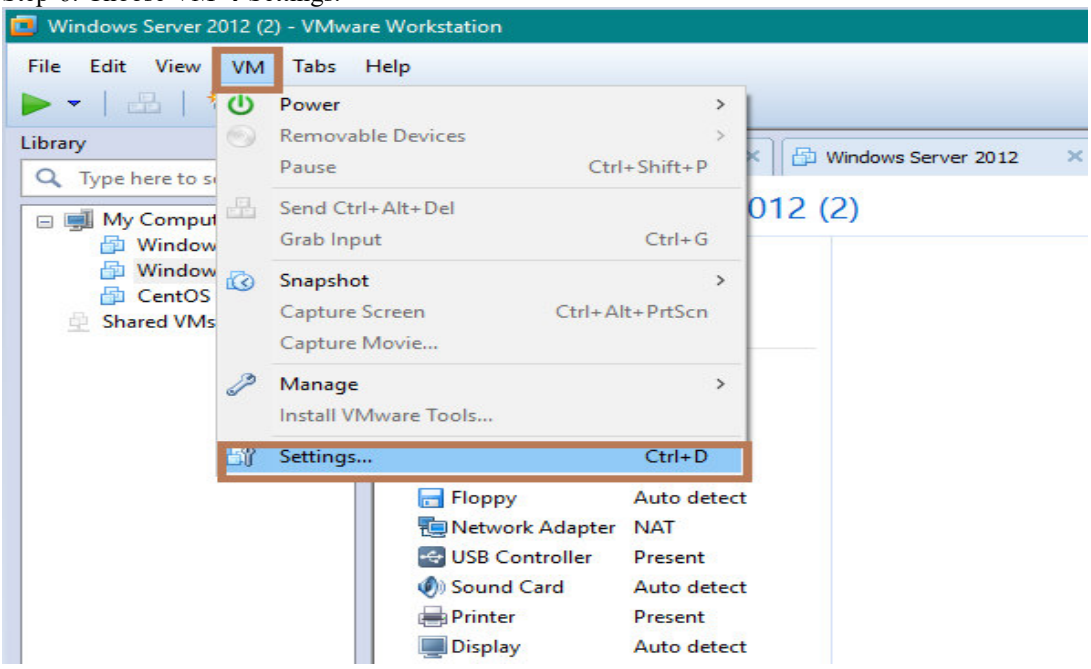
Step-3: On the Hardware tab, click Network Adapter.



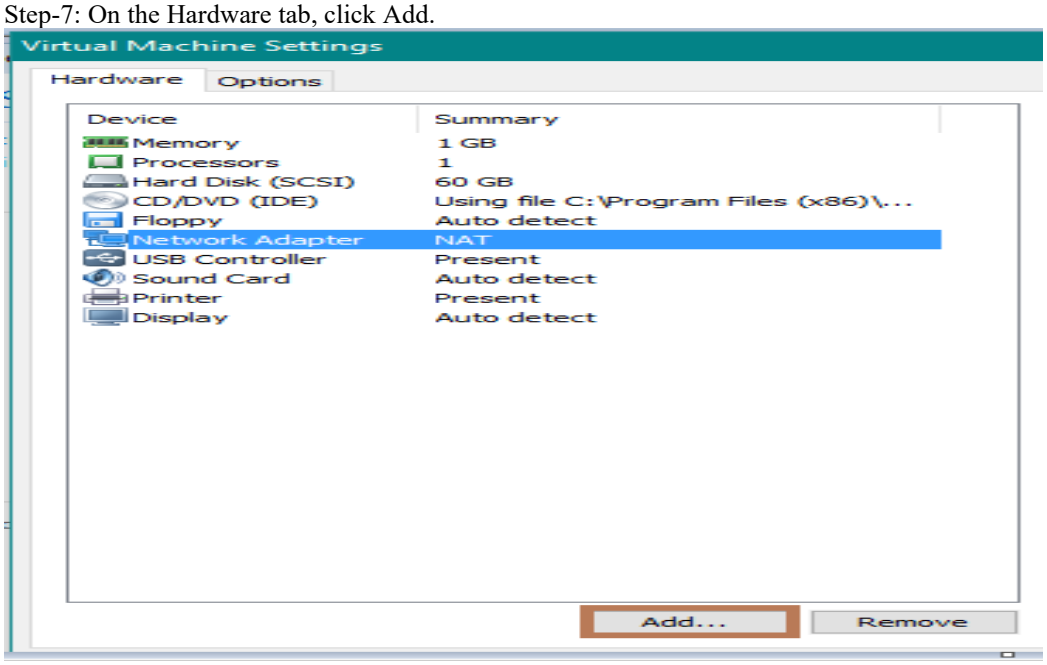
Step-4: Select Bridge as the network type to use. And Step-5: Click OK.



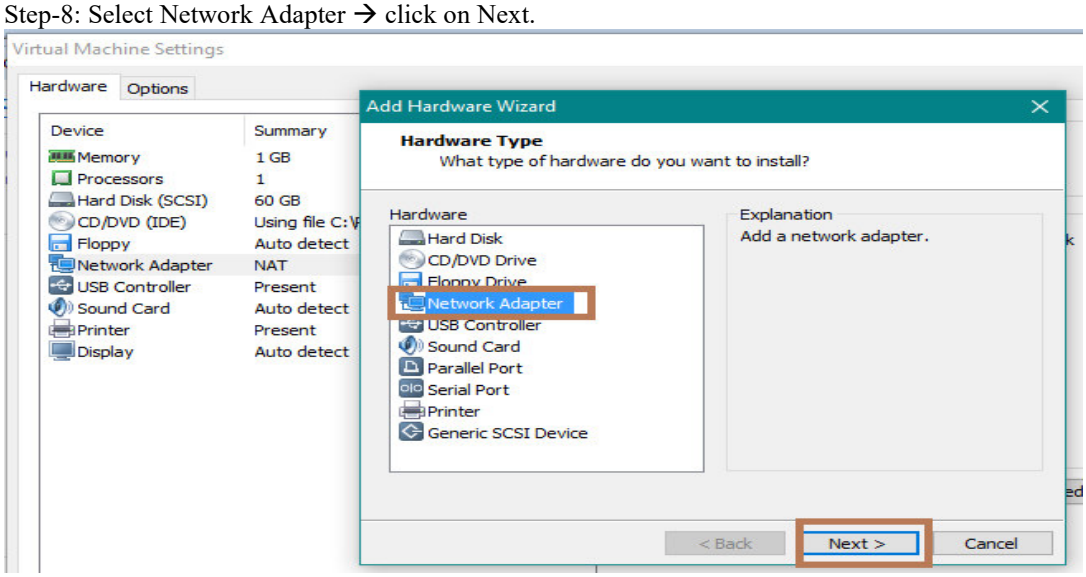
Step-6: Choose VM →Settings.



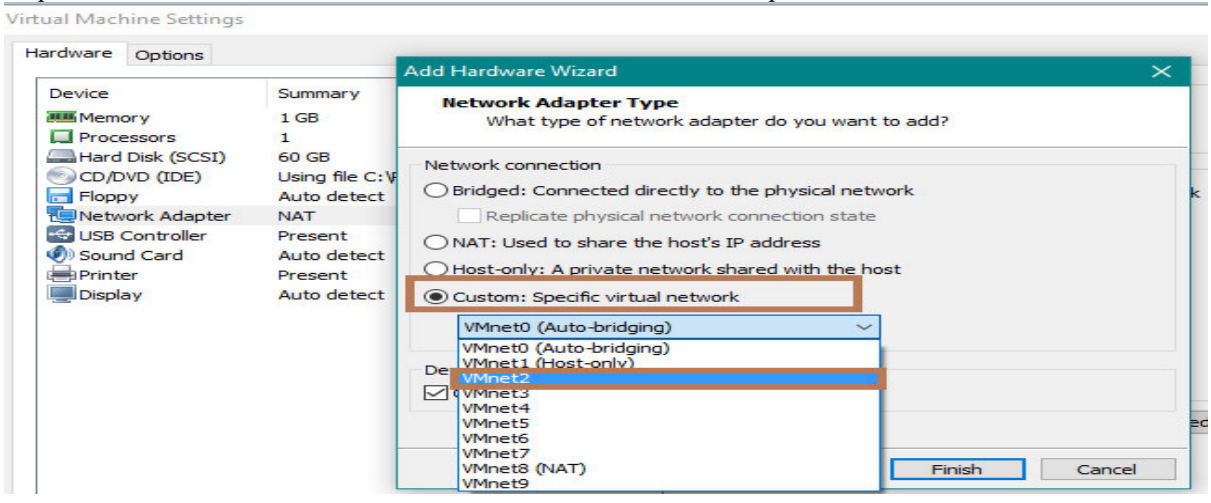
Step-7: On the Hardware tab, click Add.



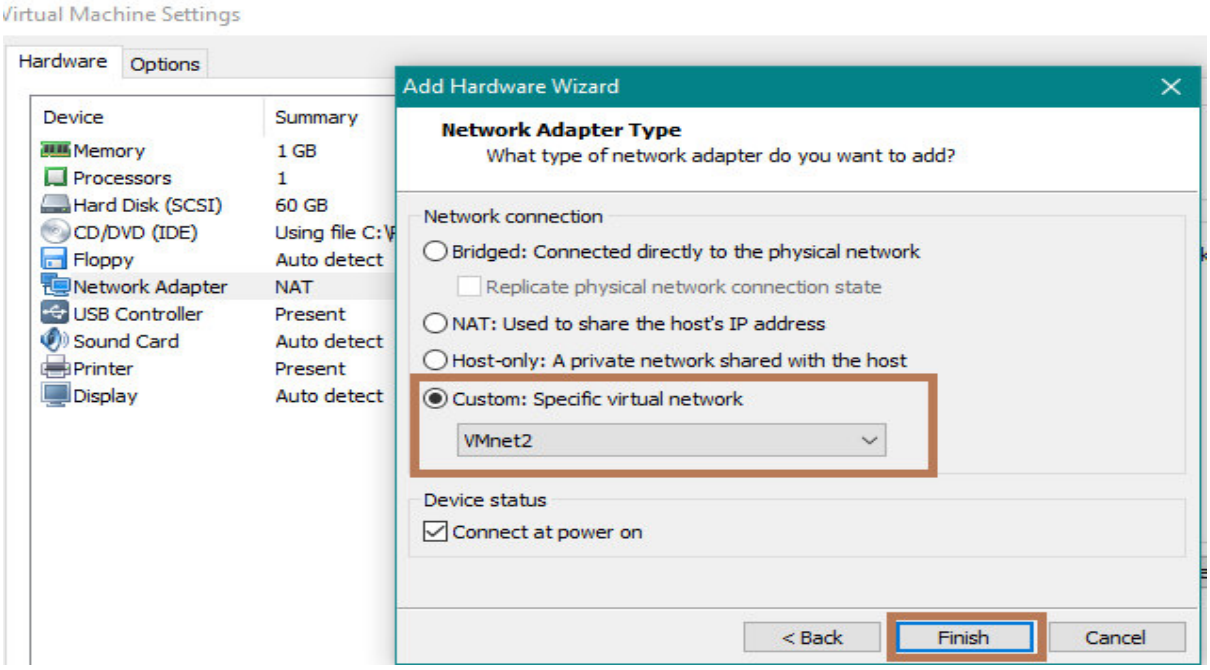
Step-8: Select Network Adapter → click on Next.



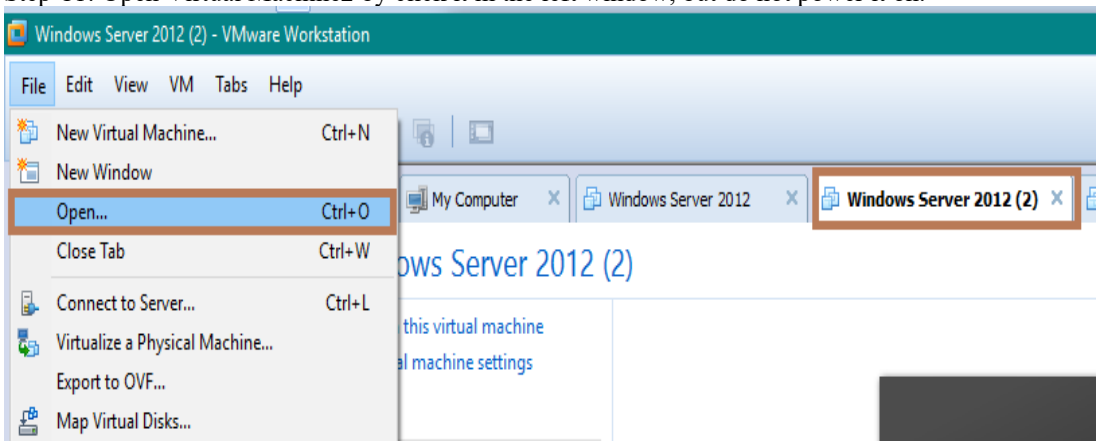
Step-9: Select Custom, choose the VMnet2 network to use from the drop-down menu.



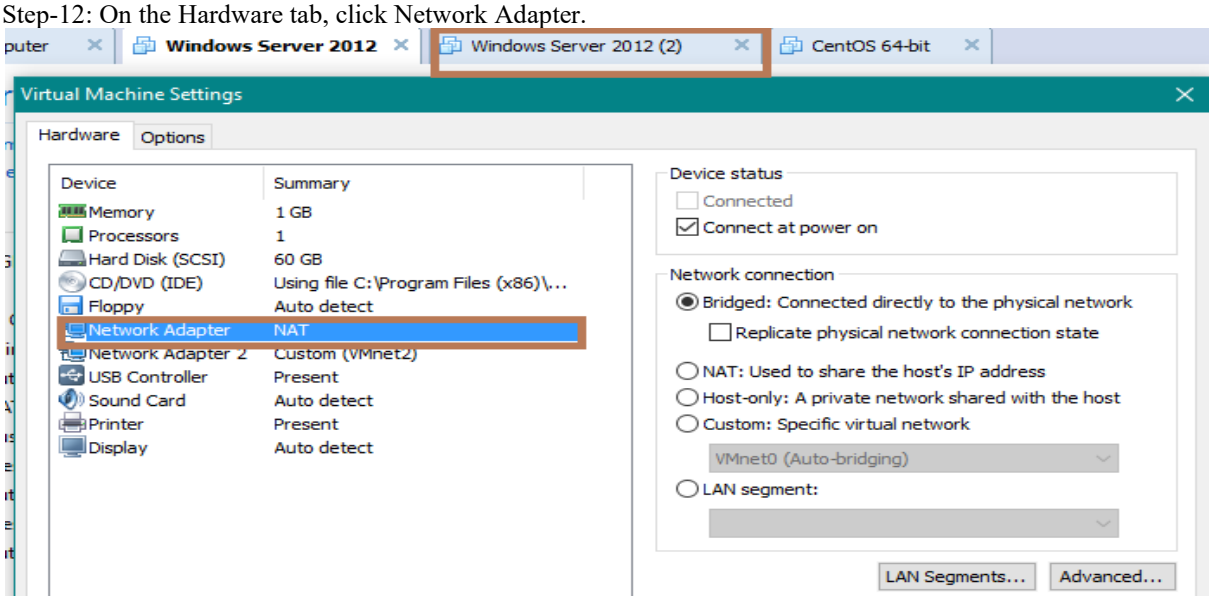
Step-10: Click Finish.



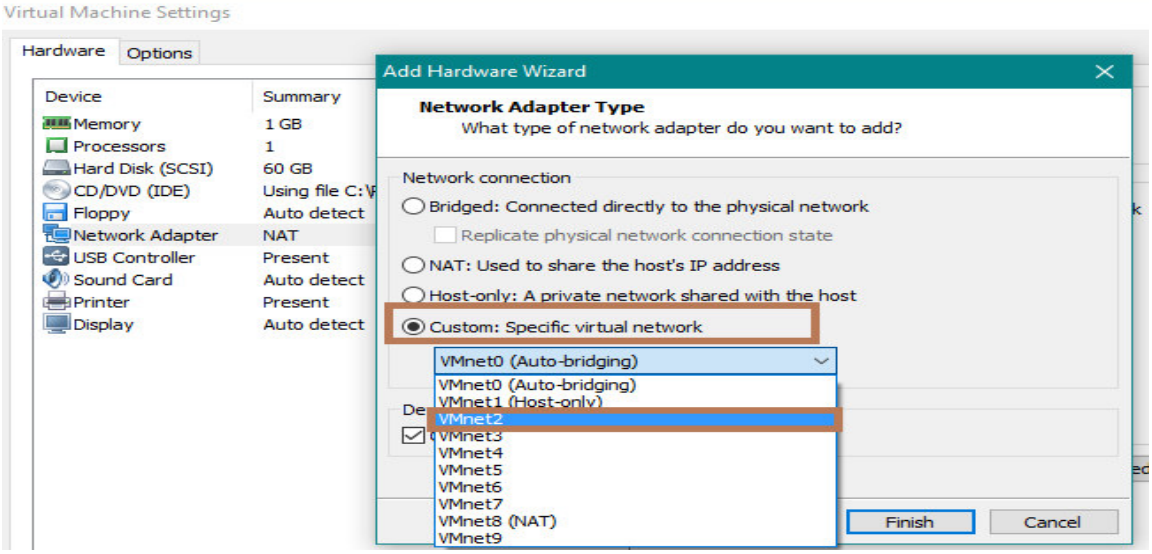
Step-11: Open Virtual Machine2 by click it in the left window, but do not power it on.



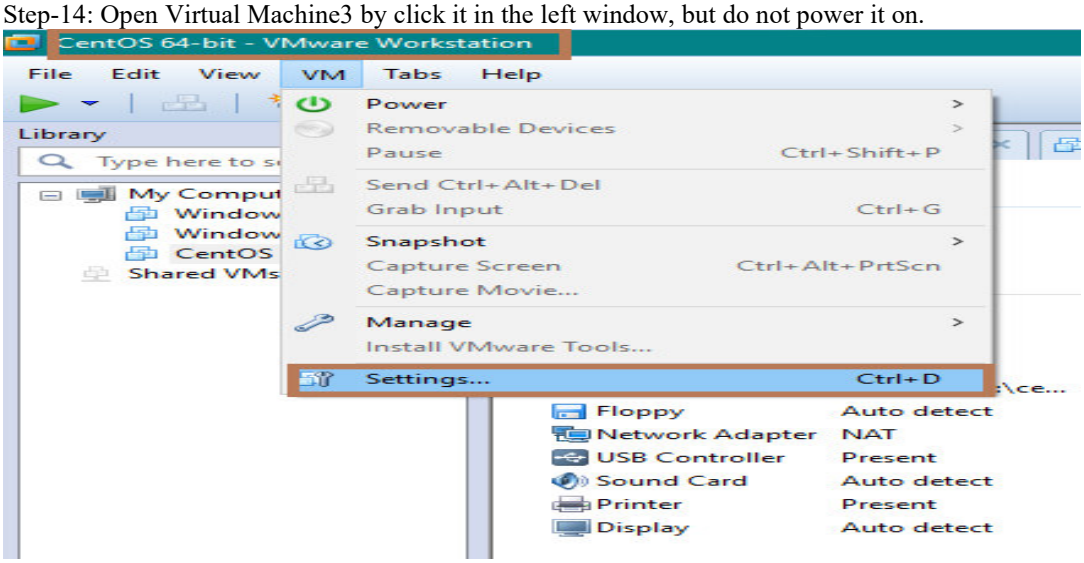
Step-12: On the Hardware tab, click Network Adapter.



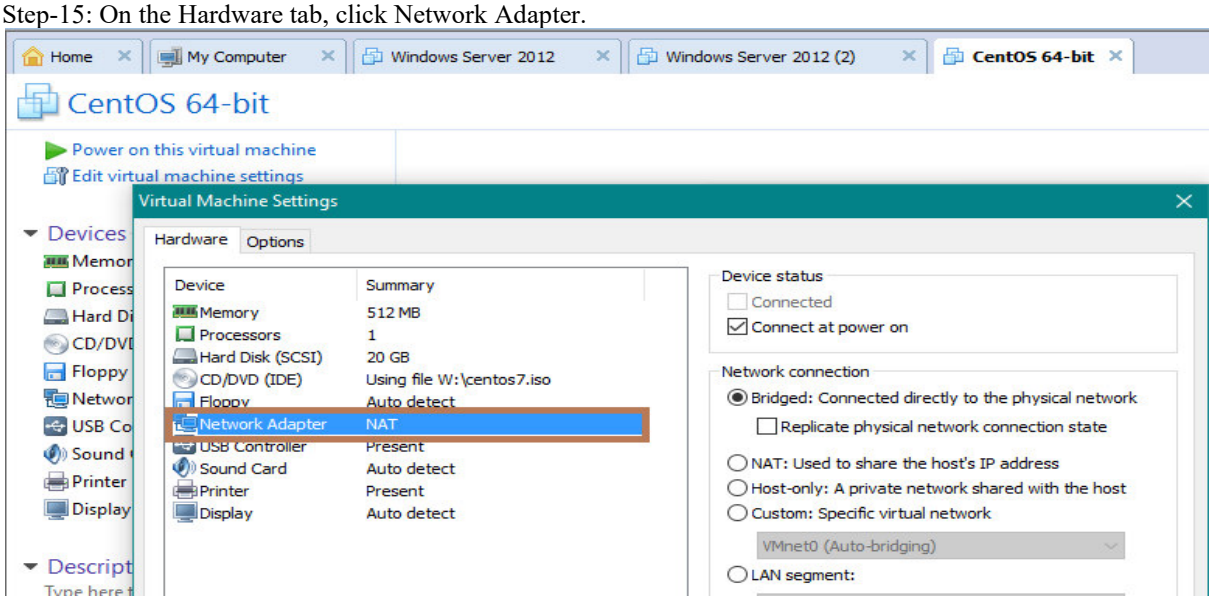
Step-13: In the right windows, select Custom and choose the VMnet2 network to use from the drop-down menu.



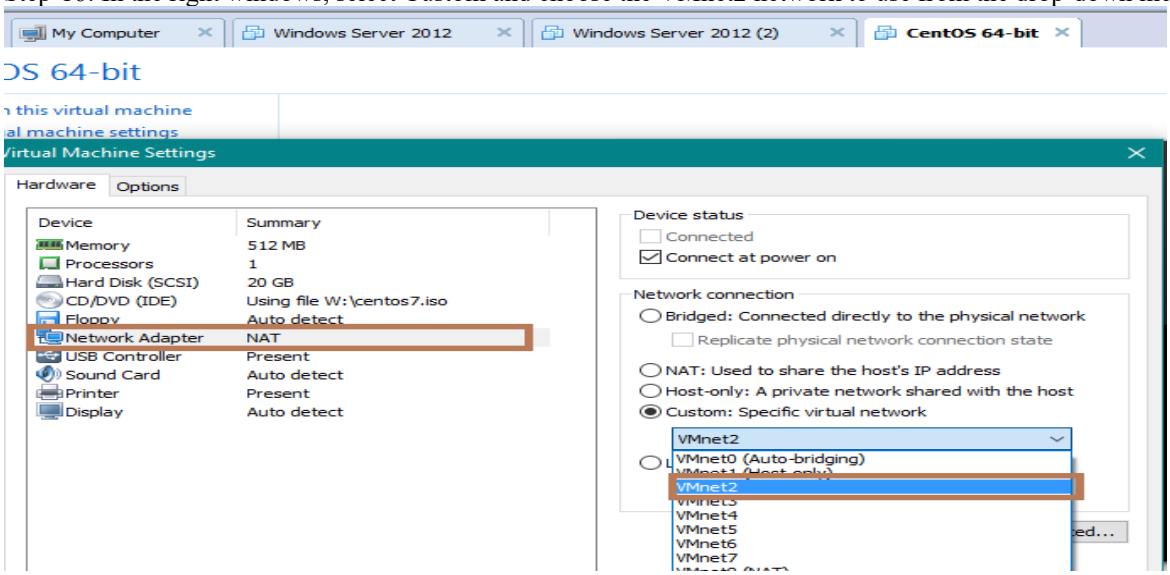
Step-14: Open Virtual Machine3 by click it in the left window, but do not power it on.



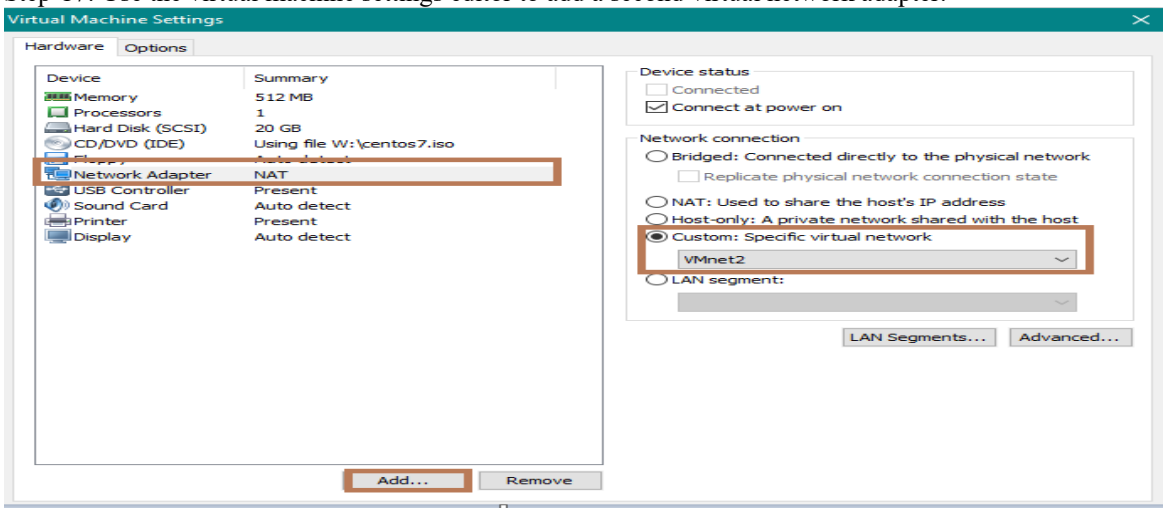
Step-15: On the Hardware tab, click Network Adapter.



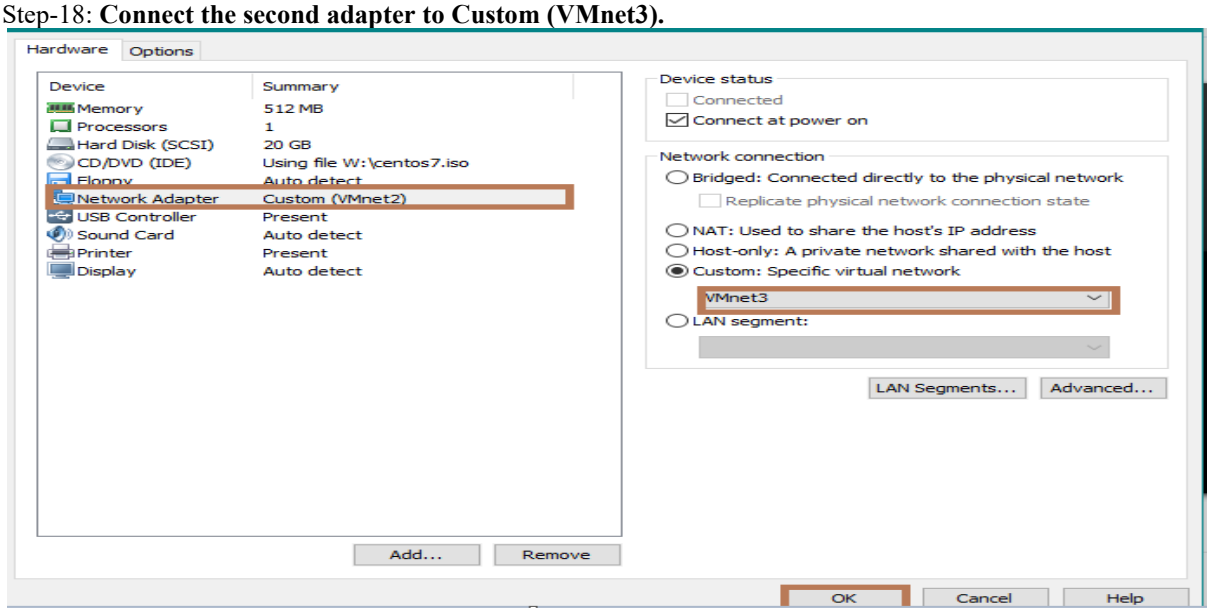
Step-16: In the right windows, select Custom and choose the VMnet2 network to use from the drop-down menu.



Step-17: Use the virtual machine settings editor to add a second virtual network adapter.



Step-18: **Connect the second adapter to Custom (VMnet3).**



9. Conclusion and Future Work

The cloud computing technology without virtualization, it is inconsiderable and impracticable. There are different virtualization techniques in the cloud computing such as software based such as VMware, Virtual Box, so on and Hyper-V or bare metal based virtualizations. But, this paper work is executed by using software based virtualization to simulate cloud based system by applying virtual Ethernet switches, virtual bridged devices and NAT devices in the single host computer by using VMware workstation. In the future work, anyone can address this work by applying different host and virtual machines.

10. References

[1]. NIST Cloud Computing Standards Roadmap, NIST Special Publication 500-291,Version2 (Supersedes Version 1.0, July 2011).
[2]. John Wiley and Sons, cloud computing principles and paradigms Book, 2015.
[3]. "Security Aspects of Virtualization in Cloud Computing", by Muhammad Kazim, Rahat Masood, Muhammad Shibli and Abdul Abbasi.
[4]. "Virtualization: Current Benefits and future potential technology concepts and business considerations", January 2011.
[5]. The NIST Definition of Cloud Computing Peter Mell Timothy Grance, september2011.
[6]. https://www.vmware.com/support/ws55/doc/ws_net_component_vswitch.html.
[7]."http://collaborate.nist.gov/twiki/cloudcomputing/bin/view/CloudComputing/CloudSecurity".
[8]. "Cloud computing Implementation, and security", by John W.RittingHouse and James F.Ransome.
[9]. "Cloud security and privacy", by Tim Mather, Subra Kumaraswamy and Shahed Latif.
[10]. "NIST cloud reference architecture, US, department of commerce"or online:"https://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf".
[11]. "Privacy-EnhancingAggregationTechniquesforSmartGridCommunications", by Rongxing Lu.
[12]. "Virtualization: issues, security threats, and solutions" by michael pearce, sherali zeadally and ray hunt (acm computing surveys, vol. 45, no. 2, article 17, publication date: february 2013).
[13]. "An Overview on Data Security in Cloud Computing", by Lynda Kacha and Abdelhafid Zitouni.
[14]. Best Practices for Mitigating Risks in virtualized Environment, April 2015.
[15]. S. De Capitani di Vimercati, S. Jaljodia, S. Paraboschi, G. Pelosi, and P. Samarati, "Encryption-Based Policy Enforcement for Cloud Storage", in Distributed Computing System workshops (ICDCSW), 2010 IEEE 30th international conference on, 2010, pp. 42-51.