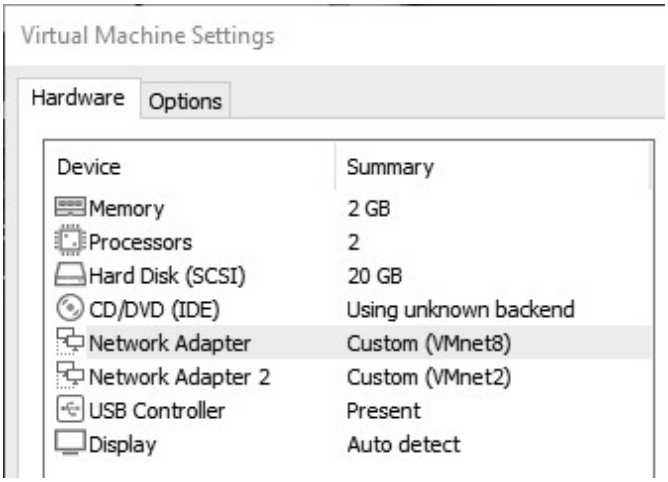
Week 3: Journal

Lab3a: Static Networking

Task 1 Query your Network Configuration

- Ensure both VMs have their Network Adapters set to VMnet8 and VMnet2 for connection to each other and to the internet.



- `sytemctl is-active NetworkManager` ensures the Network Manager Service is active before attempting any network configurations, otherwise it will do nothing.
- `systemctl enable NetworkManager` ensures the Network Manager Service will start automatically at boot up.
- Linux Network Configuration
    - `Ifconfig` shows all configuration for all network interfaces on the Linux Server. Ens33 should have an inet address since it connect to the NAT network adapter **(MAKE SURE ENS33 IS TURNED ON!!**)

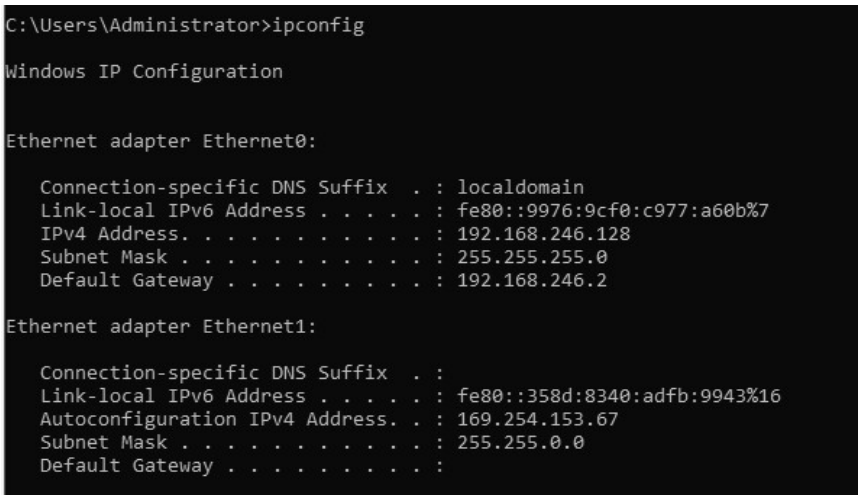
```
[root@localhost etc]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.246.129  netmask 255.255.255.0  broadcast 192.168.246.255
        inet6 fe80::dc4:b003:eda6:2840  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:8b:77:57  txqueuelen 1000  (Ethernet)
        RX packets 135121  bytes 200382453 (191.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 32629  bytes 2053153 (1.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:8b:77:61  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 3612 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

    - `route -n` shows routing table without DNS query revealing the IP address instead of the domain name.
    - `hostname or cat /etc/hostname.conf` shows hostname attached to a domain name. e.g. localhost.localdomain. The domain name is the DNS suffix
    - `cat /etc/resov.conf` is the DNS configuration that automatically resolves by the Network Manager.

cat /etc/sysconfig/network System wide network configuration

Windows

ipconfig Network configuration of IP address and default gateway



route print -4 shows routing table for IPv4 routes

Linux: ens33			Windows: Ethernet0	
DNS suffix	localdomain		DNS suffix	localdomain
Inet address	192.168.246.129		Inet address	192.168.246.128
Subnet mask	255.255.255.0		Subnet mask	255.255.255.0
Default route	192.168.246.2		Default Route	192.168.246.2

Task 2: Designing the network

Linux: ens37			Windows: Ethernet0	
Inet address	10.0.2.1		Inet address	10.0.2.2
Subnet mask	255.255.255.0		Subnet mask	255.255.255.0
Default route	10.0.2.1		Default Route	10.0.2.1

- The network between the two servers is 10.0.2.0/24.
- Inet address of each server is within the network
- Subnet mask is 255.255.255.0
- Default gateway should be the same for both servers.

Task 3: Command-line configuration

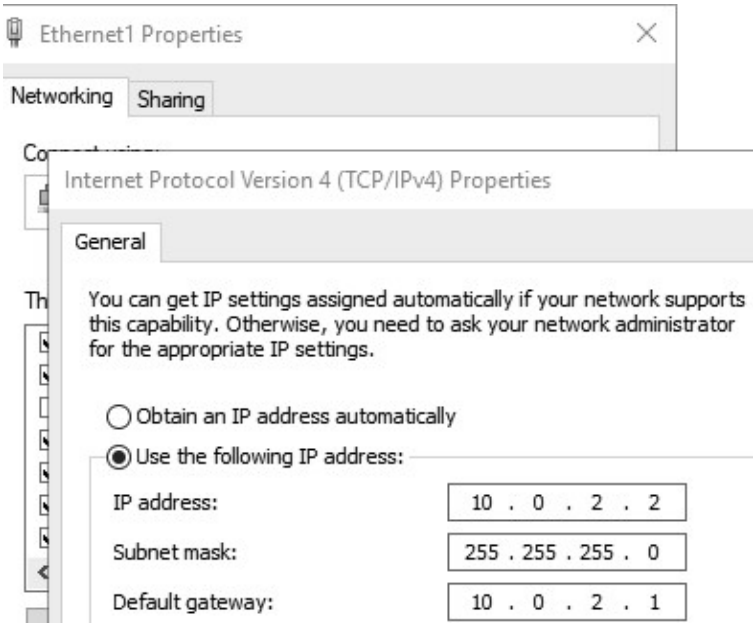
3a: Linux server

- ifconfig ens37 10.0.2.1 netmask 255.255.255.0 Configure the IP address manually for interface ens37 that forwards packets to the Windows Server.
- route add default gw 10.0.2.1 Adding a default route to the routing table with the IP address of the default gateway.
- netstat -r routing table command
- Changing default gateway alters the default route to the internet making ping requests to a dns server not reachable

- route del default gw 10.0.2.1 to remove the default route and use the original default route gateway.

3b: Windows server

- Configure the network configuration of the Windows Server using GUI
- Access Control Panel > Network and Internet > Network Connections > Interface (Ethernet1) to configure the IPv4 properties
- ipconfig shows the new network configuration has been reflected from the IPv4 property changes.
- Windows Server can ping Linux Server's IP address but not the other way around. Windows Server's firewall is blocking ICMP requests from Linux Server.



Task 4: Setting up the firewall

4a: Windows server

1. **(easiest)**
   Click Start > Control Panel > Network and Internet > System and Security > Windows Defender Firewall > Allow an app through firewall > File and Print sharing
   a. **enable checkbox(es) (private and public)**
   b. **Press OK button.**
2. **(advanced)**
   Server manager > Tools > Windows Defender Firewall with Advanced Security > Inbound rules
   a. **Enable File and Printer sharing (Echo request ICMPv4 IN) rule**
   b. **Other Rules if needed**

After allowing the inbound traffic for Echo requests to the Windows Server, it is able to receive the request from the Linux Server and send a response back. Linux Server can now ping Windows Server's IP address (10.0.2.2) which it couldn't before.

4b: Linux

- **Firewalld is a firewall package capable of filtering the network traffic going in and out of the Linux device.**
- **To interact with the firewall, the firewall-config package needs to be installed.**
  - **systemctl status firewalld ensures that the firewalld service is running before it can be configured.**
  - **yum install firewall-config installs the firewall-config package used to change the firewall rules through GUI or CLI**
- **firewall-config to start the GUI to configure the rules**
  - **Zones > public > ICMP Filter To filter specific ICMP events when receiving traffic. In this example the echo reply wants to be blocked from incoming traffic.**
  - **Tick the echo-reply box. Ping requests from the Windows Server will be blocked.**
  - **However, the firewall was not successful to block as this feature sometimes work even when configured properly.**
- **CLI commands**
  - **firewall-cmd --add-icmp-block=echo-reply**
  - **firewall-cmd –remove-icmp-block=echo-reply**
  - **firewall-cmd --query-icmp-block=echo-reply**