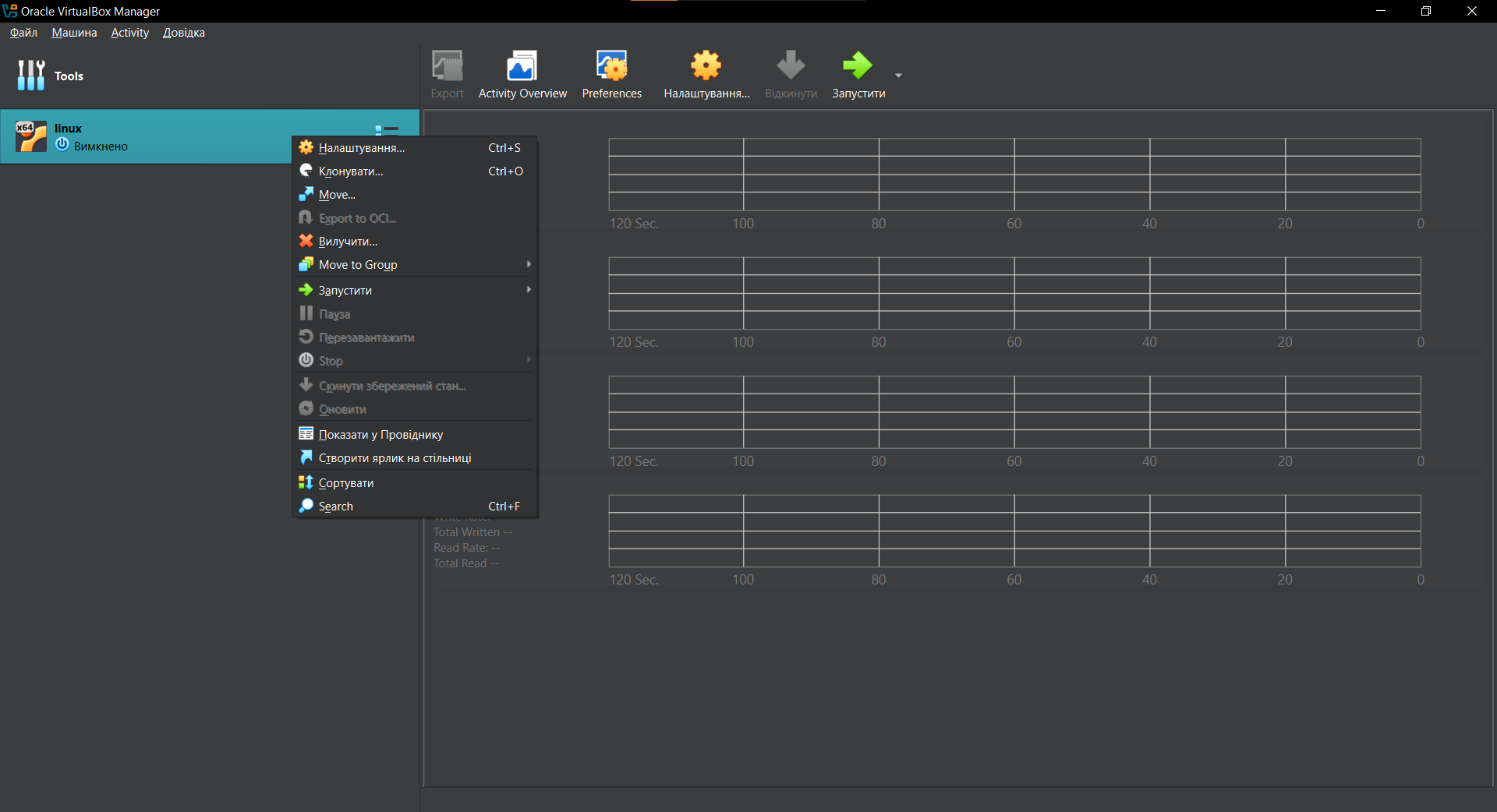
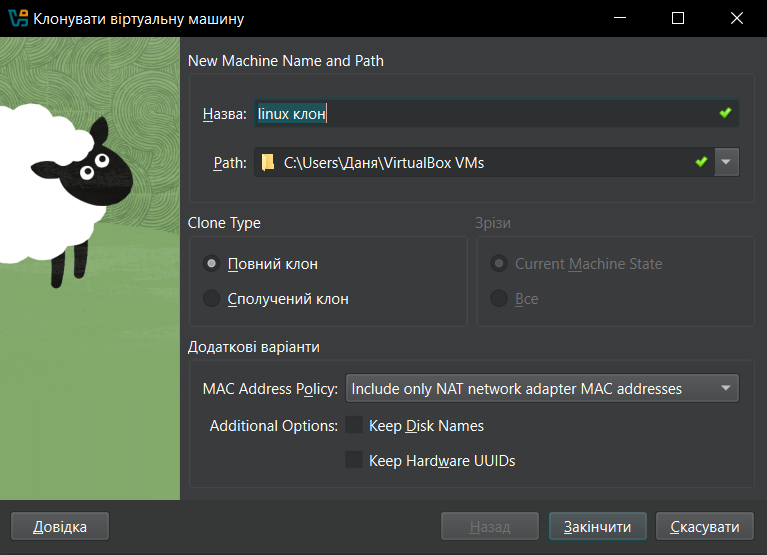
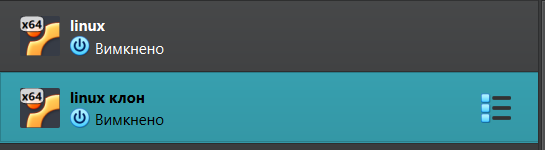
1. В робочому середовищі віртуальної машини Virtual Box, VMWare Workstation (або інший на Ваш вибір) необхідно виконати:  
- Клонування вашої віртуальної робочої ОС (Work-case 2). Яким чином це можна зробити? Продемонструйте всі етапи;  
- Може виникнути необхідність перенесення (клонування) ОС у інше віртуальне середовище. Які треба виконати дії для експорту вашої віртуальної робочої ОС? 

On an unstarted virtual machine, right-click, get a drop-down menu in which you select clone...

We get a modal window in which we specify the name, path, and type of clone.

* Full Clone: Creates a complete copy of the VM with its own files and settings.
* Composite Clone: Shares virtual disk files with the original VM (saves space but links the clone to the original).

I choose a full clone because I want them to be separate virtual mice, but with common settings.



After downloads, we get a clone.

**Exporting a Virtual Machine (if you need to transfer to another virtual environment):**

Exporting a VM allows you to transfer it to another virtual environment.

**In VirtualBox:**

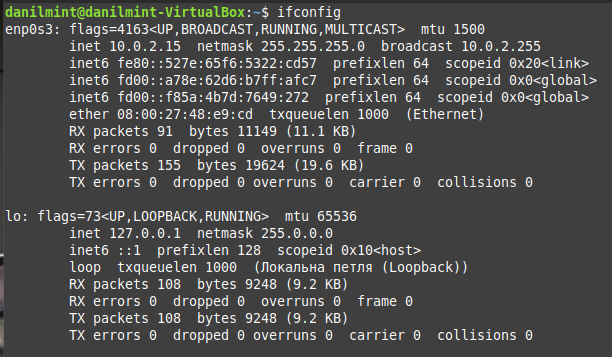
1. **Select the VM** in VirtualBox.
2. Go to **File > Export Appliance**.
3. Choose the VM you want to export and click **Next**.
4. Select the **export format** (usually .ova or .ovf).
5. Click **Export**.

2. В ході роботи одна робоча віртуальна машина може взаємодіяти з іншою. Для цього необхідно між ними розгорнути мережу. Опишіть які типи організації мережевих з’єднань підтримуються в середовищі віртуальних машин, в чому особливість кожного з них:  
- Трансляція мережевих адрес (NAT);  
- Мережевий міст (Bridged);  
- Віртуальний адаптер хоста (Host-only);  
- Внутрішня мережа (Internal Network).

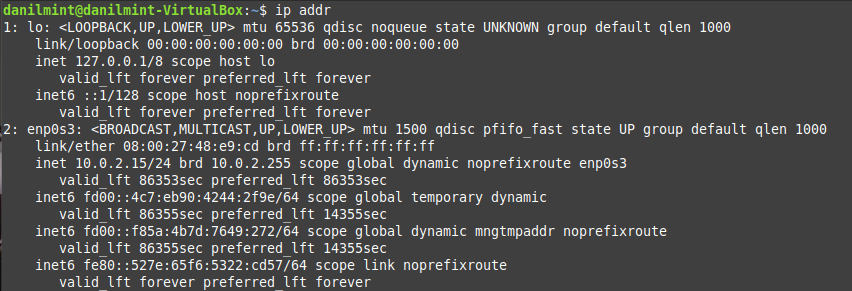
* **NAT (Network Address Translation)**:
  + The VM uses the host machine’s IP address to access external networks like the internet.
  + The guest OS is invisible to external networks and can only access the internet through the host.
  + **Use case**: Simple internet access for VMs without external exposure.
* **Bridged Network**:
  + The VM acts as if it is part of the same network as the host and gets its own IP from the physical network (router).
  + **Use case**: VM can interact with other devices on the same network and is accessible externally.
* **Host-Only Network**:
  + The VM can only communicate with the host machine, but not with external networks.
  + **Use case**: Secure communication between VMs and the host without outside access.
* **Internal Network**:
* VMs can communicate with each other, but neither the host nor external networks are accessible.
* **Use case**: Secure communication between VMs in isolated environments.

3. Розгорніть мережу між вашою робочою ОС та її клоном (завдання 1):  
- Продемонструйте базові команди для налаштування мережевих параметрів ОС, поясніть, що вони виконують.  
- Обидві ОС мають мати вихід у мережу Інтернет. Відкрийте браузер та перегляньте будь-яке відео в youtube  
- Налаштуйте та продемонструйте обмін повідомленнями між двома ОС по локальній мережі. Які команди в терміналі при цьому необхідно ввести?  
- Налаштуйте спільну мережеву папку для обох ОС. Спробуйте скопіювати файли з цієї директорії в домашній каталог користувача (віртуальна робоча ОС) та на робочій стіл (клон віртуальної робочої ОС).

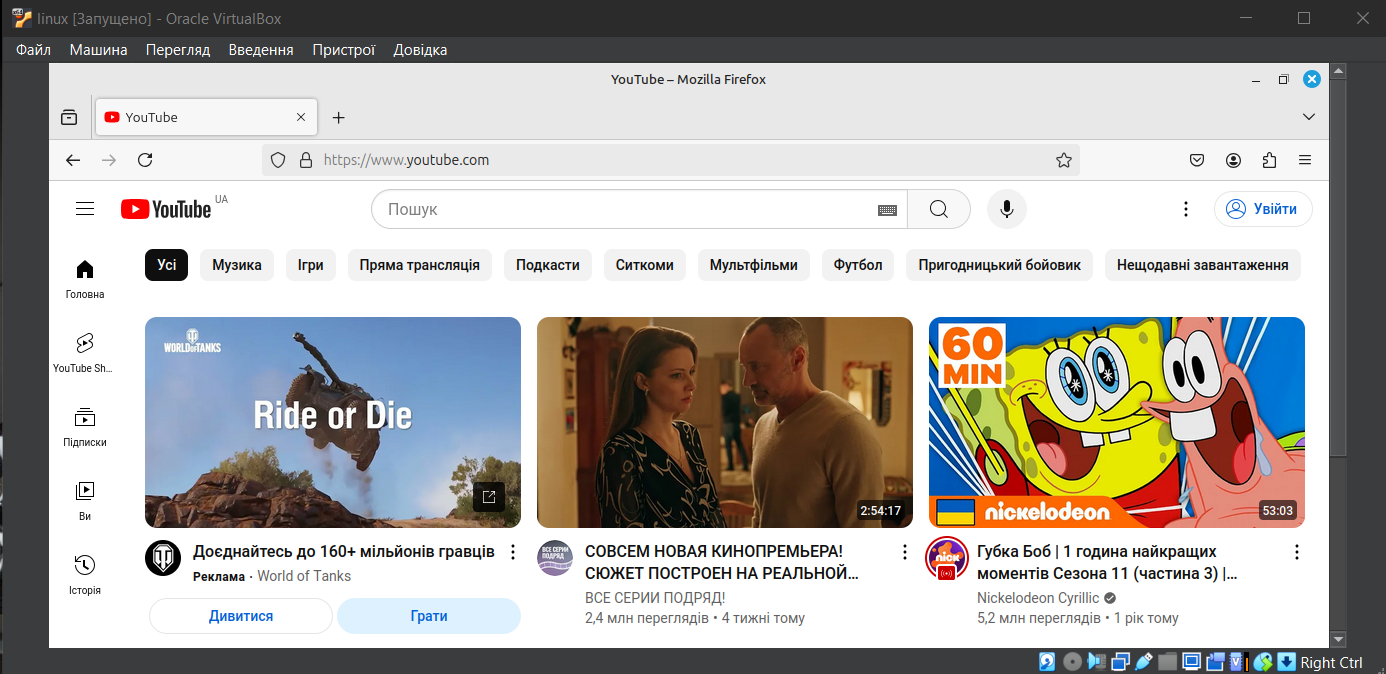
On the old



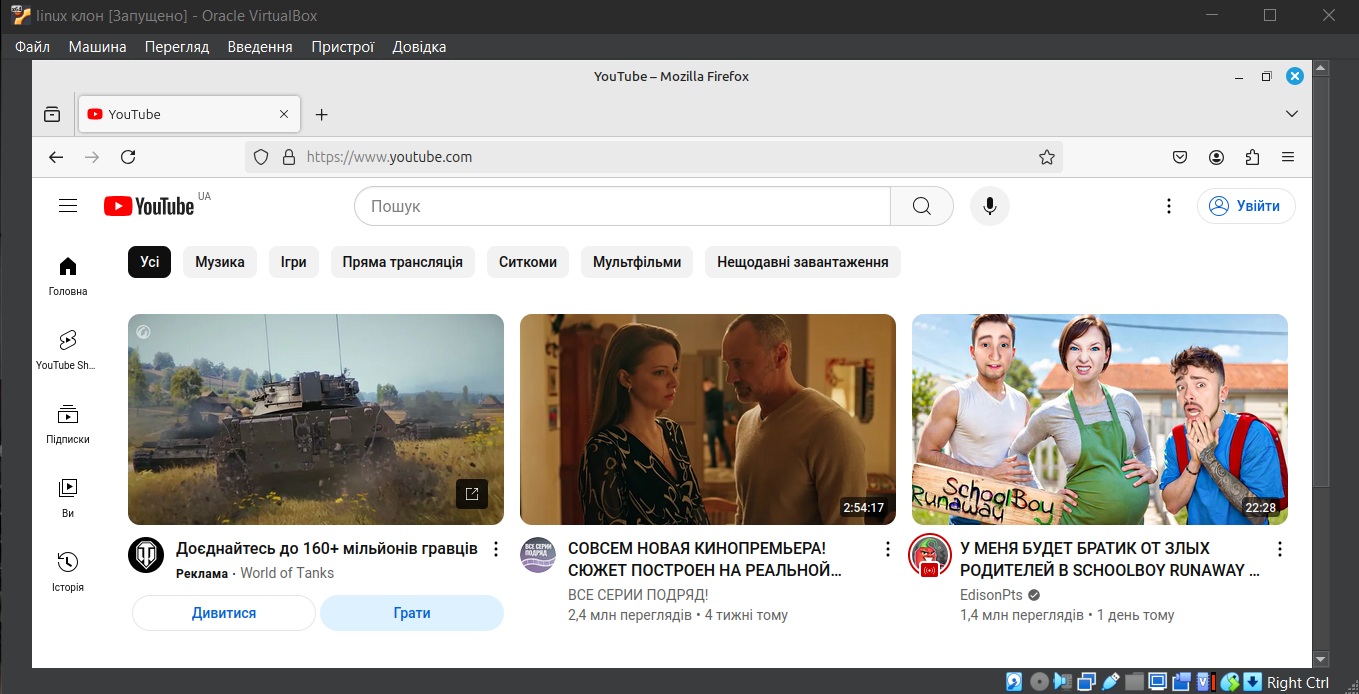
On a new (cloned)



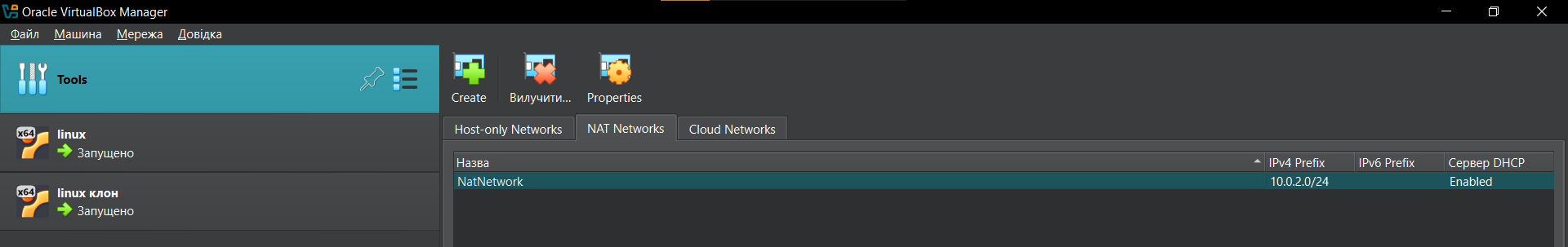
To check if the virtual machines are connected to the Internet, I went to YouTube, everything works.

First Machine

Second Machine

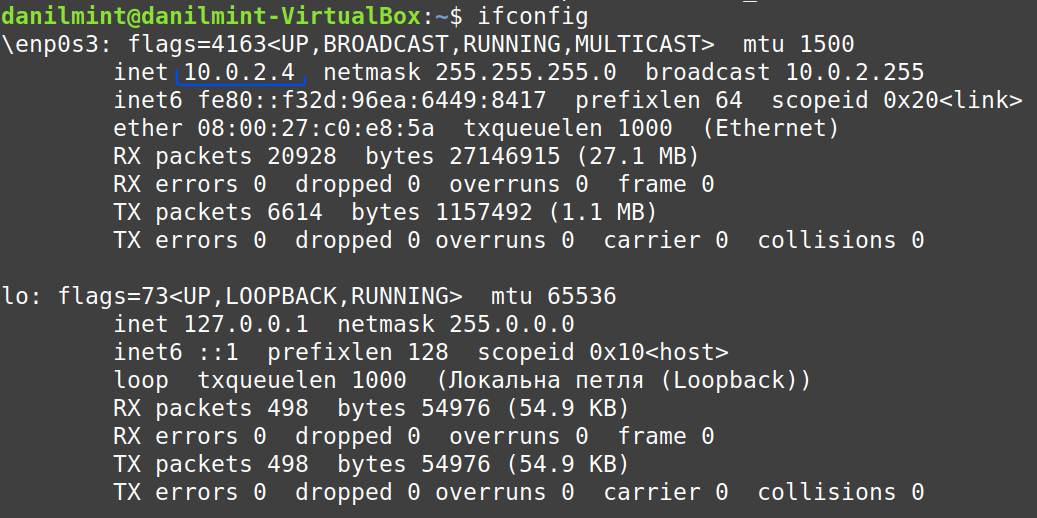


I encountered a problem that there was no message from one car to another. To do this, I created a separate network. Click File -> Tools -> Network Manager and tap create to create the new Network, before that choose Nat Networks and then create.

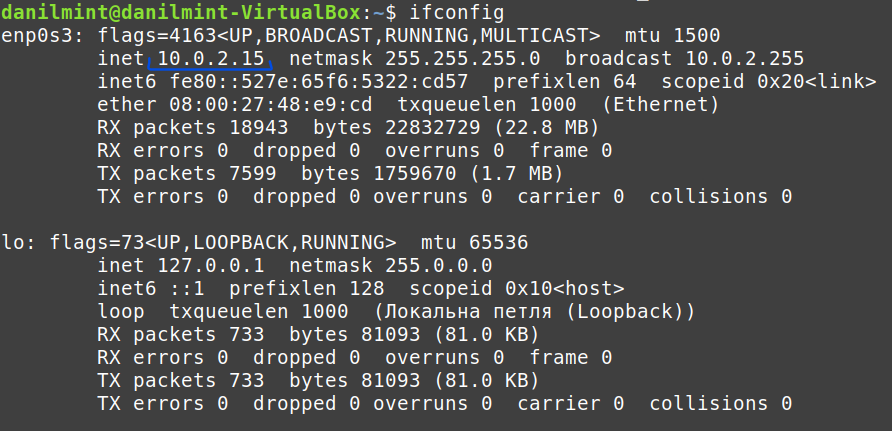


Check the IP in both OS.

First

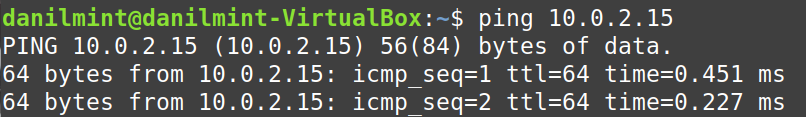


Cloned

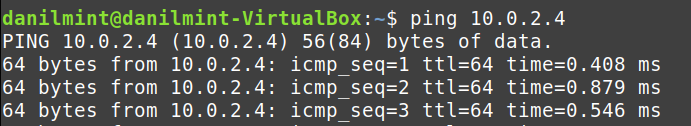


Let's check if virtual machines see each other's IP addresses:

First VM



Cloned



nc -l -p 12345 – on the virtual machine on which we want to see the message, where:

**- nc**: This is the command to run **netcat**. netcat is a tool for reading from and writing to network connections using TCP or UDP.

**- l**: This option tells netcat to **listen** for incoming connections. It puts netcat in server mode, meaning it waits for a connection from another machine.

**- p 12345**: This specifies the **port number** on which netcat will listen. In this case, 12345 is the port number where netcat will wait for incoming connections. You can use any valid port number that is not already in use.



echo "Hello from VM2" | nc IPfirstVM 12345 – Message to Second

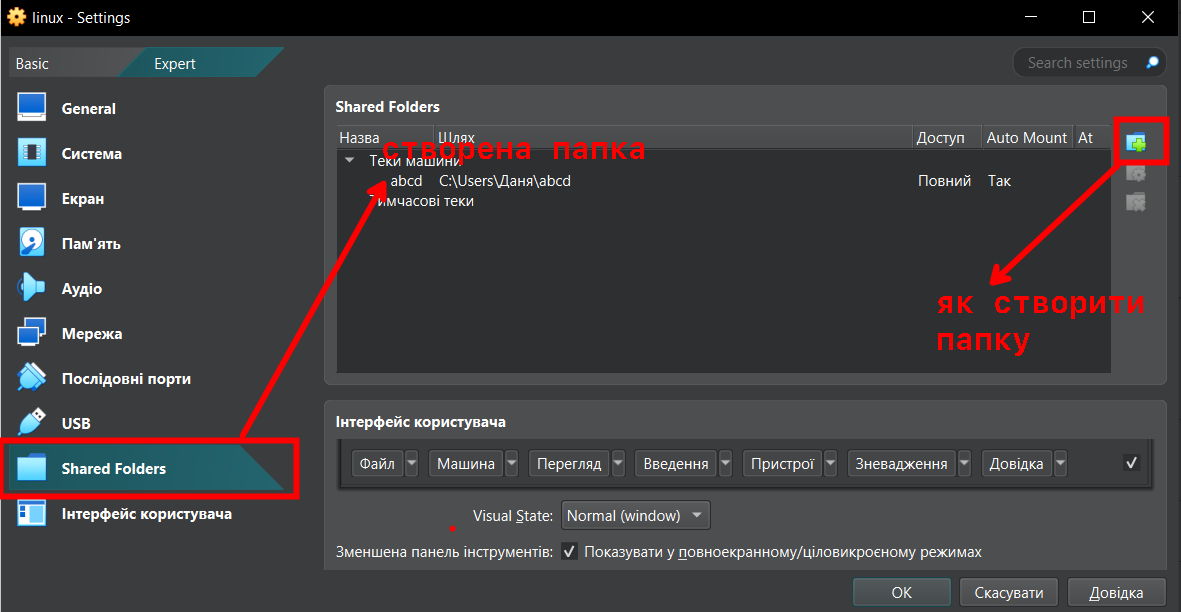
* **echo**: This is a command that prints the text following it to the standard output (terminal). In this case, the text "Hello from VM2" will be output.
* **"Hello from VM2"**: This is the message you want to send. You can replace it with any message you want to send to the other machine.
* This symbol takes the output of the command on the left (echo "Hello from VM2") and **passes** it as input to the command on the right (nc 10.0.2.4 12345).
* In other words, it sends the output of echo to the nc (netcat) command.

**nc**: This is the **netcat** command, used for reading from and writing to network connections.

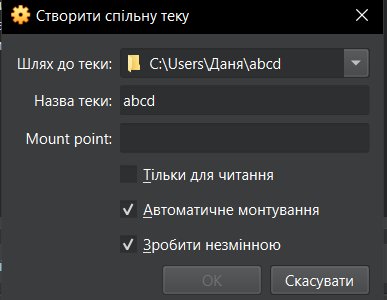
* **10.0.2.4**: This is the **IP address** of the machine (VM1) you want to send the message to. In this case, it’s the IP address of the listening machine.
* **12345**: This is the **port number** on which the destination machine (VM1) is listening for connections.



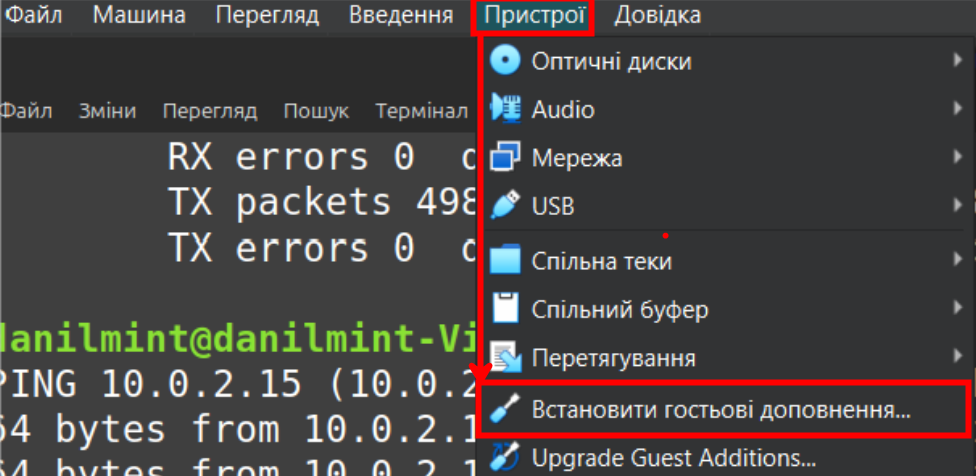
To set up a shared network folder, you need to create it for both virtual machines as a shared folder (I've already created one)



For the folder (on both OS), I have selected the following options:



To see the folder, manipulate it, and so on. We have to upload guest add-ons.

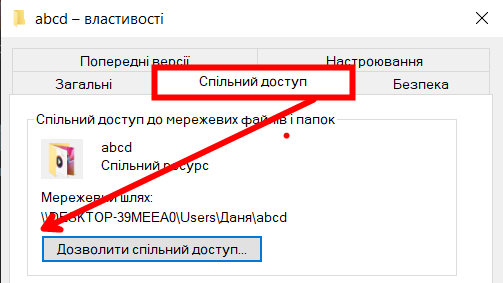


The main operating system I use on my PC is Windows, so we have to specify network access to it for our shared folder.

To do this, find the path of the folder (my path is indicated above in the screenshots) and select the properties

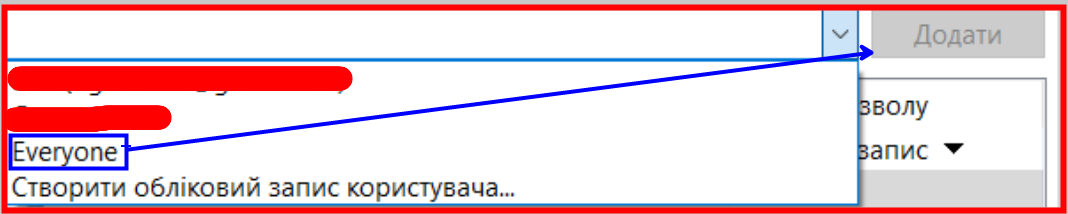


Sharing – Allow sharing



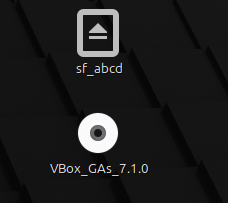
Allow reading and editing (we need this for the fourth point in the tasks)

Adding all users with the appropriate access



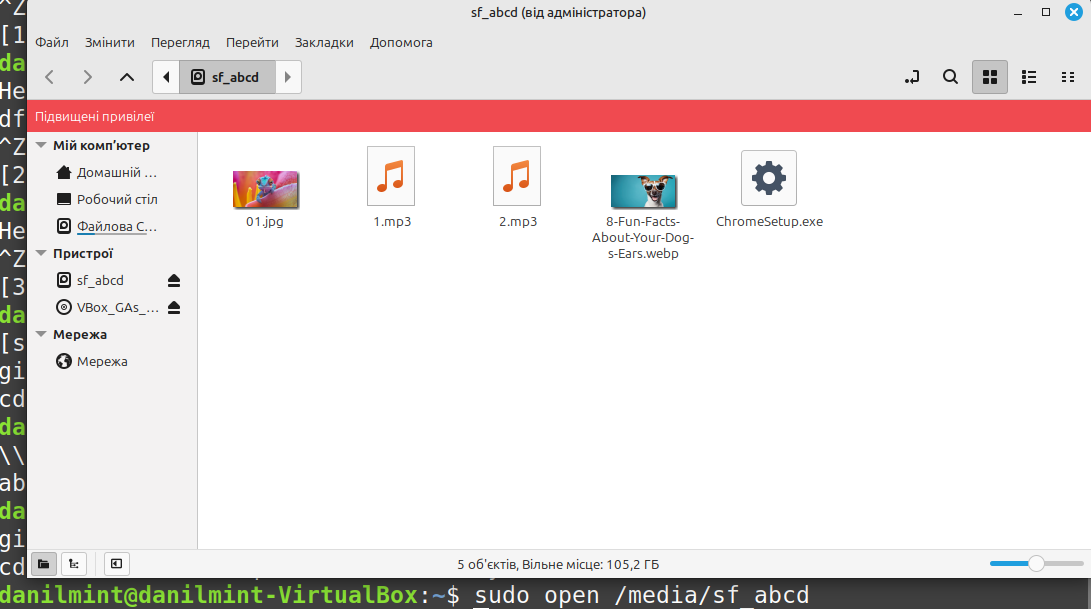


After rebooting, we get:



Our folder and guest additions.

Access to the folder is blocked due to the lack of rights, but we can fix this using the terminal



Since I chose automatic mounting, the sf\_abcd folder appeared in the /media directory.

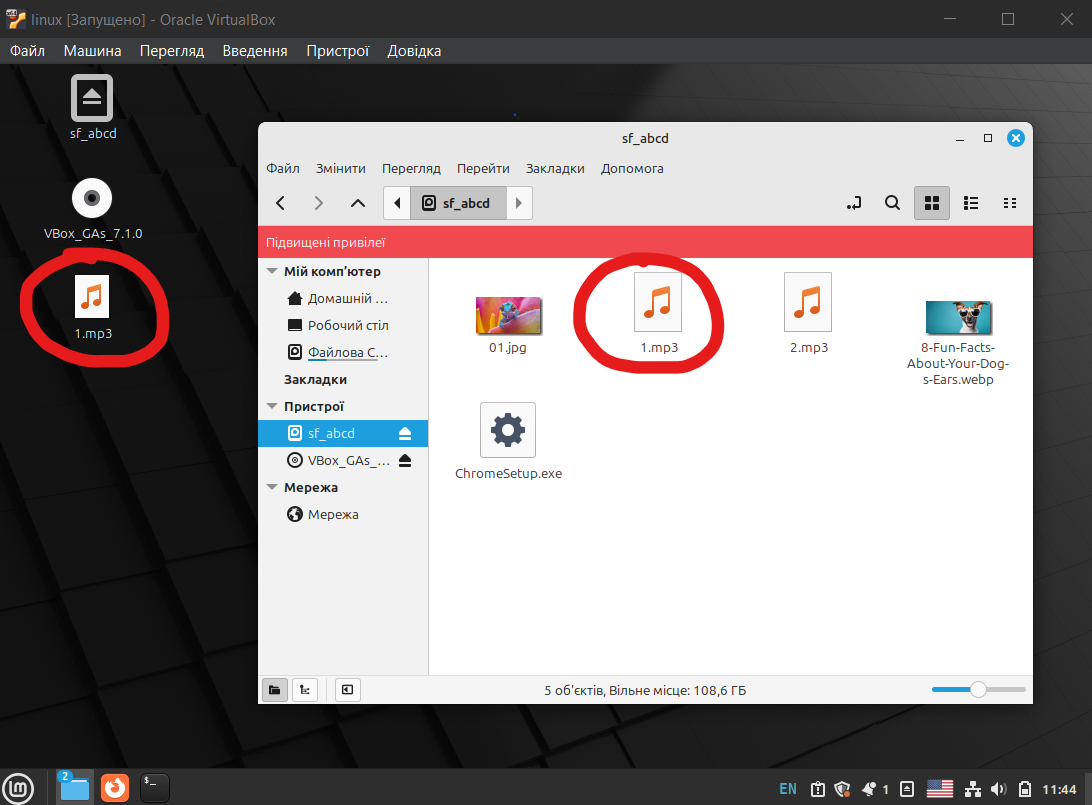
In the folder I uploaded some photos and music (which was dumped from my main OS)

4. Яким чином можна організувати обмін інформацією між вашою основною ОС (наприклад Windows) та віртуальними ОС? Скопіюйте довільний аудіо-файл з вашої основної ОС на робочий стіл віртуальної ОС та її клона. Як зробити зворотну дію, коли треба документ з робочого столу віртуальної ОС скопіювати до вашої основної робочої ОС?

Working with an audio file.

I downloaded the audio file from the Internet directly to the abcd folder, and from there I moved the items to the desktop of both VMs, since sf\_abcd has elevated privileges, the files we move can only be moved to /root. To avoid this situation, let's configure access rights using the command: 

Although all permissions were granted, I couldn't move files from the folder, the final solution was to remount the folder (reassign all access to the folder again) 

Now everything works. Files can be moved to the desktop, and from the desktop to the folder (actions are performed immediately in the screenshot)

**Додатково:** Які мережеві можливості доступні в інших гіпервізорах? Проведіть порівняння.

**Types of Network Connections in Hyper-V:** Hyper-V has three types of virtual switches: External, Internal, and Private. Briefly about each network:

* **External (external network):**  
  This type of connection allows virtual machines to directly interact with the host's physical network and the external network. Virtual machines gain access to the internet and can communicate with other devices in the network like physical machines.
* **Internal (internal network):**  
  This type allows virtual machines to communicate with each other and the host, but without access to the external network or the internet. It is useful for private connections between the host and virtual machines.
* **Private (private network):**  
  In this mode, virtual machines can only communicate with each other. The host and the external network cannot interact with machines in the private network.

**Types of Network Connections in VirtualBox:**

* **Network Address Translation (NAT):**  
  By default, the guest operating system connects to the network using Network Address Translation (NAT). In this case, your actual computer acts as a router, forwarding packets between the virtual machine and the internet. If the type of the virtual machine’s network interface connection is set to NAT, no additional configuration of the guest OS and the host is needed.  
  However, with this setup, the virtual machine will be invisible to the internet. Another downside of NAT is the limitation of supported protocols, as only UDP and TCP are fully supported. The lack of support for the GRE protocol will result in the inability to authenticate in a virtual private network (VPN) via PPTP from the virtual machine. In such cases, you will need to choose other connection types, such as "Bridged Adapter" or "Host-only Adapter," which will appear in the host system upon installing VirtualBox. You can find it in the list of network connections.

When the guest machine sends an IP packet to a remote machine, the VirtualBox NAT service intercepts the packet, extracts TCP/IP segments, changes the IP address to the host machine's IP, and sends it. The outside world sees only the IP of the host machine. The host machine receives the response and forwards it to the guest machine.

* **NAT Network:**  
  This type of connection has been available since VirtualBox version 4.3. It is mostly similar to the previous type, except that if you run multiple guest systems connected to the same NAT network, they can communicate with each other. In the global settings of VirtualBox, you can create several different NAT networks.
* **Bridged Adapter:**  
  In Bridged Adapter mode, virtual machines behave like any other computer connected to the same network as the host machine. The bridged adapter connects the real and virtual networks. The outside world can directly interact with the guest machine.  
  The network bridge connects through the host system to your network device, which is assigned an IP address from your physical network. VirtualBox connects to one of your installed network cards and exchanges packets directly, linking the physical and virtual networks. Normally, it will attempt to obtain a standard 192.168.x.x IP address from your router, so your virtual machine will appear as a physical device alongside other devices in the network.
* **Internal Network:**  
  If you need several guest machines to communicate with each other on one host and nothing else, you can use the internal network mode. Although you can use a bridged adapter for the same purpose, the internal network is more secure. When using a network bridge, all packets sent and received via the physical adapter on the host machine can be intercepted (e.g., by installing a sniffer on the host machine).  
  The internal network creates, according to the VirtualBox manual, "a software network visible to selected machines but not to applications running on the host or in the surrounding environment." This gives you a network where there are only the host and the virtual machines, without using physical adapters – they are entirely virtual, and VirtualBox acts as a virtual switch. You get a completely private LAN for your guest machines, with no external access, making it highly secure. Possible use cases include working on highly classified development servers, penetration testing, or creating a secure intranet for a team or organization. It's an ideal option for restricting the installation of unauthorized applications, downloads, or browsing social media during working hours.
* **Host-only Adapter:**  
  Under the host-only adapter, virtual machines can communicate with each other and with the host machine but not with the outside world. The host-only adapter uses a separate network device called vboxnet0 to set up a subnet and assign IP addresses to the guest machines. Guest machines cannot communicate with the outside world as they are not connected via a physical network interface. The host-only adapter provides limited services, useful for creating a local network under the VirtualBox host for guests.

**Conclusion:**

* Hyper-V is better suited for scenarios where high network performance, VLAN support, and work with large enterprise networks are required.
* VirtualBox offers more flexibility for users setting up home or testing environments where simplicity and quick configuration are essential.