**Work-case 3**

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?

1. 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).

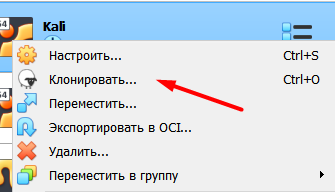
1. Розгорніть мережу між вашою робочою ОС та її клоном (завдання 1):

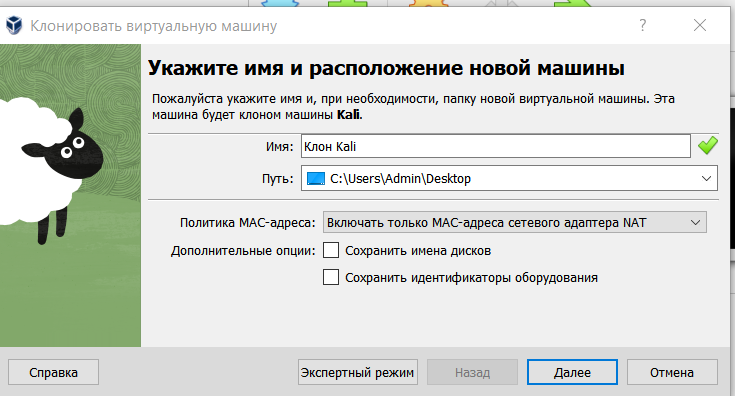
* Продемонструйте базові команди для налаштування мережевих параметрів ОС, поясніть, що вони виконують.
* Обидві ОС мають мати вихід у мережу Інтернет. Відкрийте браузер та перегляньте будь-яке відео в youtube
* Налаштуйте та продемонструйте обмін повідомленнями між двома ОС по локальній мережі. Які 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).

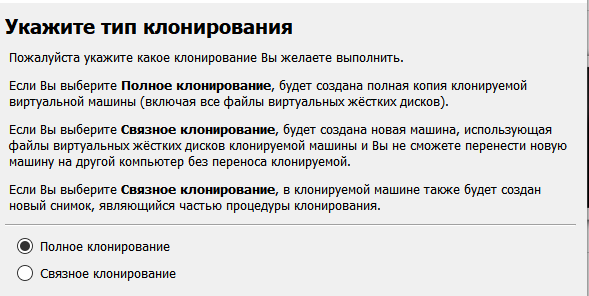
1. Яким чином можна організувати обмін інформацією між вашою основною ОС (наприклад Windows) та віртуальними ОС? Скопіюйте довільний аудіо-файл з вашої основної ОС на робочий стіл віртуальної ОС та її клона. Як зробити зворотну дію, коли треба документ з робочого столу віртуальної ОС скопіювати до вашої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

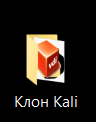
Prepared by: Malamuzh Volodymyr

1.

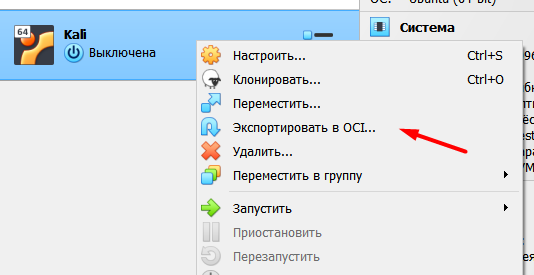


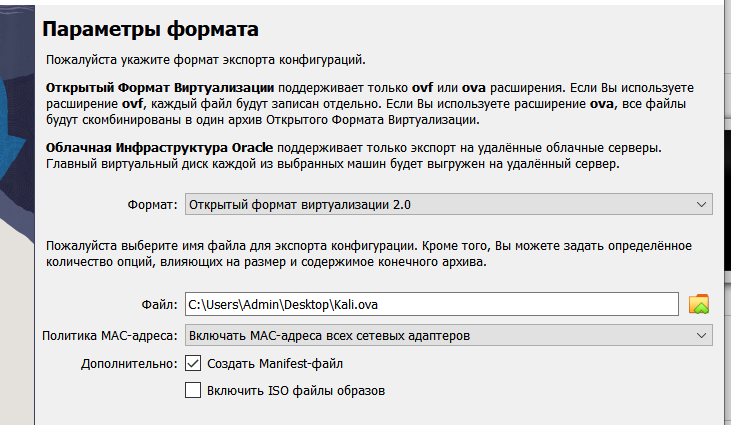


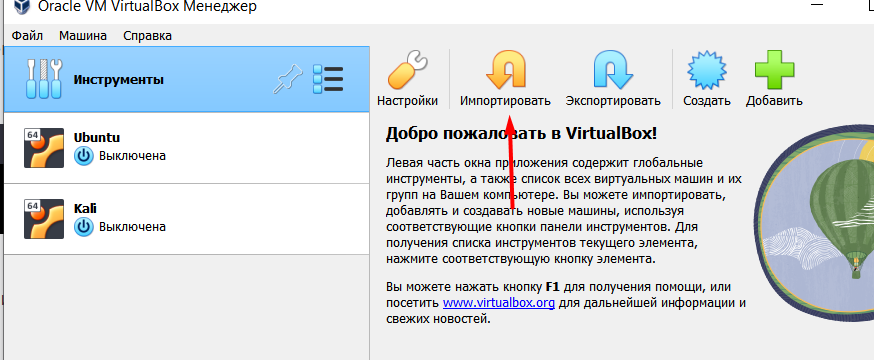


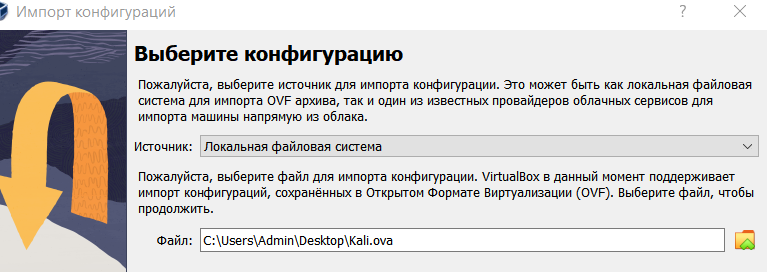


2.

. 







3.

1. Network Address Translation (NAT): NAT allows the guest OS to access the Internet using a private IP address that is not accessible from the outside network. This setting in the guest OS allows you to visit web pages, check email, and download files. But it is impossible to connect to this OS from the outside. The principle of NAT: when the guest OS sends packets to a certain address of a remote machine on the network, the NAT service intercepts these packets, extracts from them the segments containing the destination address (IP address of the guest OS) and replaces them with the IP address of the host machine. Then repackages them and sends them to the specified address.
2. Network bridge (Bridged): In a Network Bridge connection, the virtual machine works just like any other computer on the network. In the connection, the adapter acts as a bridge between the virtual and physical networks. From the side of the external network, it is possible to connect directly to the guest OS. The adapter in "Network bridge" mode is connected, bypassing the host, to the device that distributes IP addresses inside the local network to all physical network cards. VirtualBox connects to one of the installed network cards and forwards packets through it directly; the operation of the bridge that transmits data is obtained. And a virtual machine on the network looks like an ordinary physical device, no different from others.

Prepared by: Rumiantsev Hennadiy

1. Virtual Host Adapter (Host Only): With a "Virtual Host Adapter" type connection, guest OSes can interact with each other and with the host. All this happens inside the VirtualBox virtual machine itself. In this connection, the host adapter uses its own dedicated device (name - vboxnet0). Also, a subnet is created for them and IP addresses are assigned to network cards of guest OSes. The "Virtual host adapter" mode provides a limited set of services useful for creating private networks under VirtualBox for guest OSes.
2. Internal network (Internal Network): The "Internal network" mode configures the relationship between several guest OSes running on the same host and can only communicate with each other. It has good system protection (than "Network Bridge"). An internal network is a software network that may be visible to selectively installed virtual machines, but not to applications running on the host or on remote machines located externally. Such a network is a set of a host and several virtual machines. That is, a private local network is created only for guest OSes without Internet access (which is very safe).

The ifconfig command is used to assign a network interface address and to configure network interface parameters. If no options are specified, the ifconfig command outputs the current configuration of the network interface. If an address family is specified, the ifconfig command outputs only information related to the corresponding address family. Only the superuser can change the configuration of the network interface. If the options are specified in curly brackets ({}), one of them must be specified.

The ipconfig command is used to display all current TCP / IP network parameters. When calling the ipconfig command without parameters, only the IP address, subnet mask, and main gateway for each network adapter are displayed.

The netdiag command is an excellent tool for troubleshooting network problems on workstations. When launched from the command line, the utility performs several tests on the configuration of the TCP / IP protocol on the client side and reports all errors found. When the utility is launched without parameters, all possible tests are launched, otherwise, one or more selected tests can be launched.

The netstat command allows you to view information about system connections using UDP and TCP protocols. The command can be run to run every n seconds and allows you to get the following information in tabular format: - Protocol name (TCP or UDP) - Local IP address and port number used by the socket connection - Remote IP address and port number , which is used by the connection through the socket - State of the connection (listening, Established, etc.)

The pathping command allows you to detect certain problems that occur during the transmission of packets between the source and destination. To test routers between two points communication ,the pathping command sends several test echo packets to each router and displays the percentage of packets that were lost on each of the routers during the route. The pathping command allows you to detect certain problems that occur when transmitting packets between the source and destination. To test the routers between two communication points, the pathping command sends several test echo packets to each router and displays the percentage of packets that were lost at each router during the route.

With the help of the ping command, you can quickly make sure that: - There is a connection between two systems. - The DNS name resolution service is working. In addition, the ping command allows you to perform additional tests on the network environment between two systems.

The route command displays and modifies entries in the local IP routing table. Run with no parameters, the route command displays help.

Prepared by: Khomenko Anton:

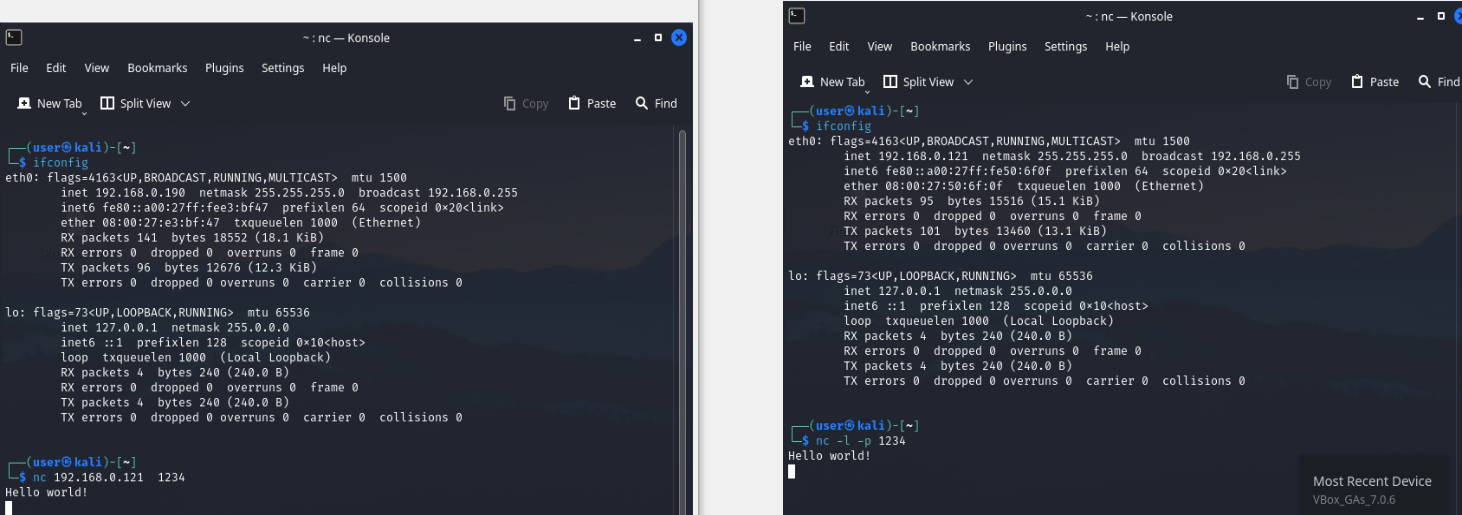
Tracert is a command designed to determine data transmission routes in TCP/IP networks. The tracert command sends data to the specified network node, displaying information about all intermediate routers through which the data passed on the way to the destination node. In the case of problems with data delivery to a node, the command allows you to determine exactly which part of the network has problems.

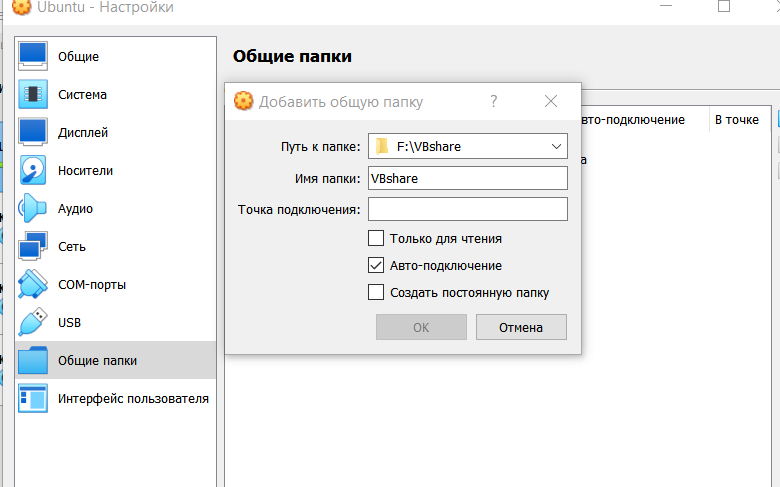
- Configure shared network folder for both OS. Try copying the files from this directory to the user's home directory (virtual desktop OS) and to the desktop (virtual desktop OS clone).

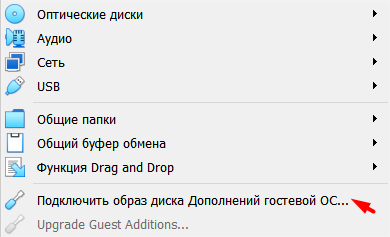
Netcat is a networking utility that allows its users to write and read data to and from computer networks. Commonly, it uses TCP or UDP for this function. Netcat makes it easy to send and receive messages on Linux and its back-ends-like nature, which allows it to be used by other scripts and programs. Furthermore, it is cross-platform and usually preinstalled on many popular Linux distros such as Debian, Ubuntu, and CentOS. It is a handy tool that makes information sharing, or more generally, computer networking, possible and easy.

Command to download it: sudo apt install netcat

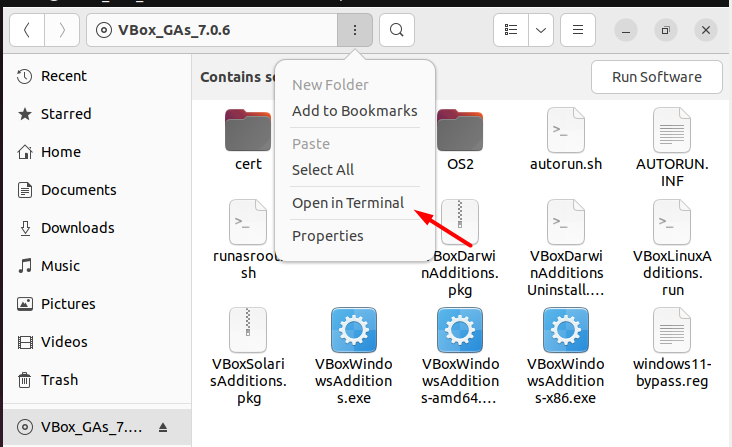
Using:

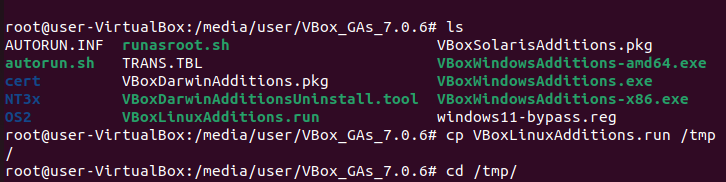






Going to files:

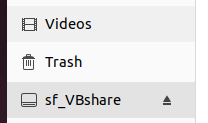




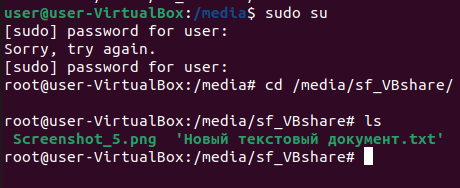


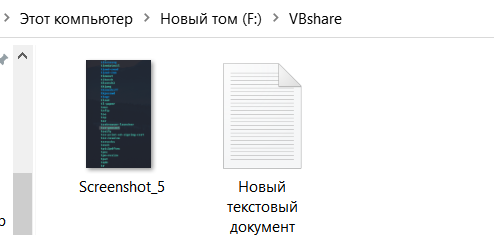
After that doing reboot

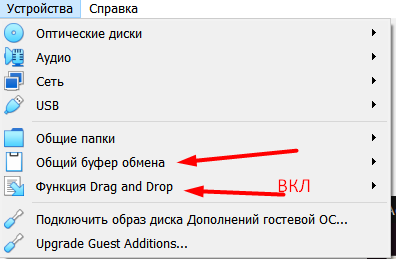
We see that in files 1 point more but we can`t enter there



We can entered there only with root privileges, doing sudo su:







On bidirectional!

