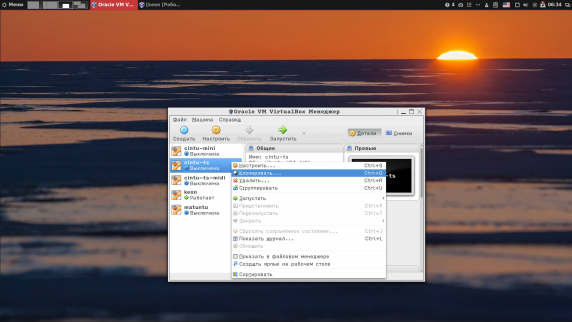
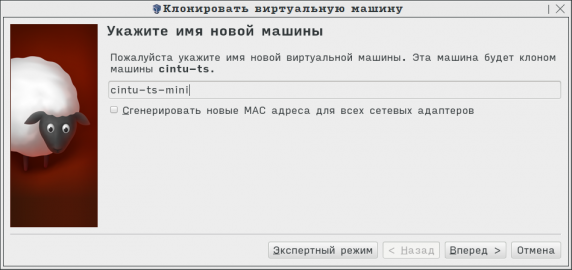
**1. Клонування вашої віртуальної робочої ОС (Work-case 2). Яким чином це можна зробити? Продемонструйте всі етапи;**

Клонування створених віртуальних машин - завдання, часта при створенні і тестуванні власних індивідуалізованих збірок. Благо, в Virtualbox'е вона виконується не просто, а дуже просто. Відповідна функція викликається або з головного меню: **Машина** -> **Клонувати** , або з контекстного меню по ПКМ:



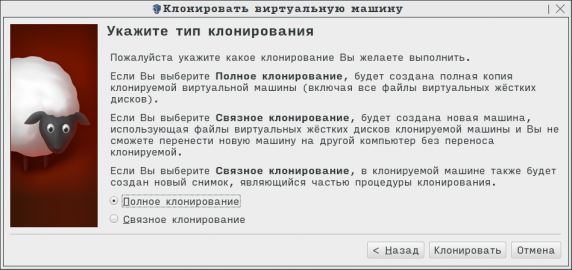
Очевидно, що в будь-якому випадку клонують машина повинна бути виключена - у працюючій машині вказаний пункт активізований не буде.

У вікні буде запропоновано задати ім'я нової машини - за замовчуванням це буде **Клон [orig-name]** , проте ясно, що воно може бути будь-яким, крім збігається з вихідним:

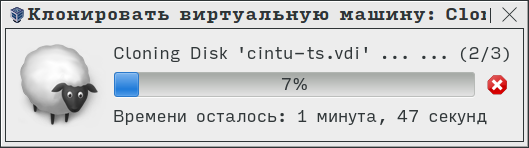
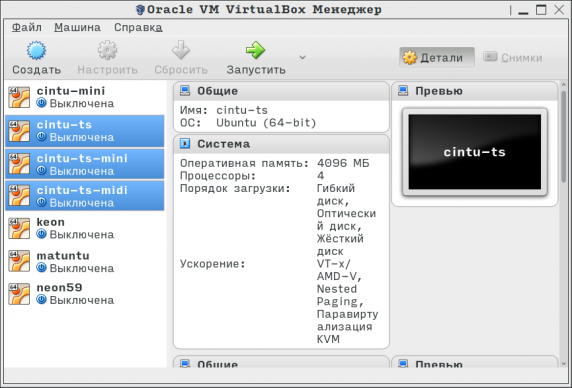
****

и потрібно генерувати нові MAC-адреси для мережевих пристроїв - залежить від завдання. Для тих цілей, в яких я використовую Virtualbox (тестування і модифікація власних образів) - не потрібно.

Далі пропонується визначити з типом клонування - повним або зв'язковим. Чим вони разлімчаются - очевидно з поясняющего тексту. Для моїх цілей підходить тільки повне клонування:

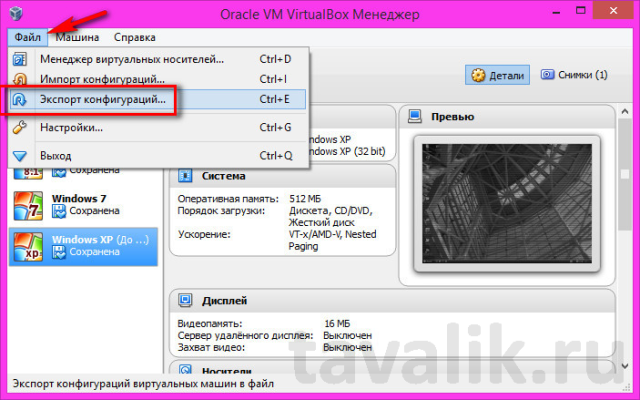


Далі починається процес клонування:

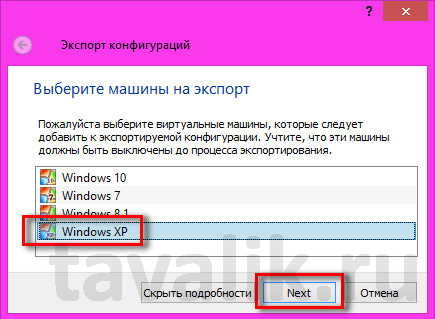
****

**Експорт віртуальної машини**

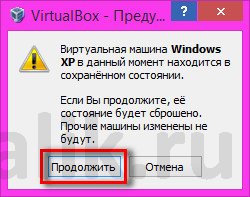
У вікні VirtualBox вибираємо конкретну віртуальну машину для експорту, тиснемо меню « Файл » і вибираємо « Експорт конфігурацій ».



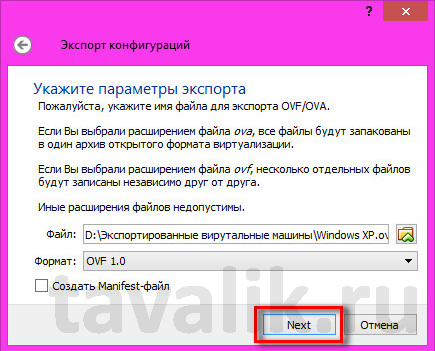
У наступному вікні тиснемо « Next ».



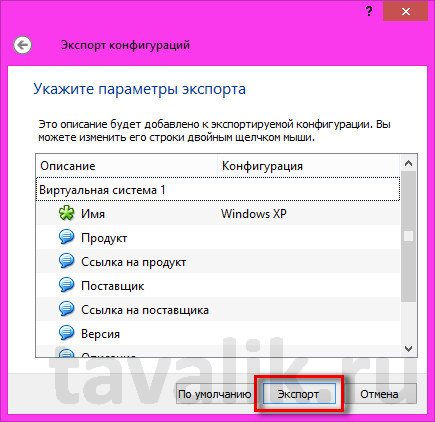
Експорт конфігурації можливий тільки при вимкненому стані віртуальної машини, і, якщо вона припинена, VirtualBox запропонує скинути збережене стан для продовження процесу.



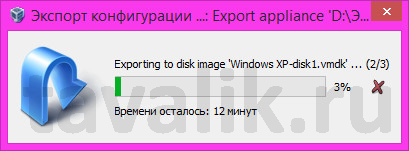
Далі з'явиться вікно параметрів експорту. Формат залишаємо встановлений, а ось папку файлу експорту «.ova», за замовчуванням розташовується на системному диску, міняємо на папку, наприклад, як в нашому випадку, спеціально створену на несистемно диску D.



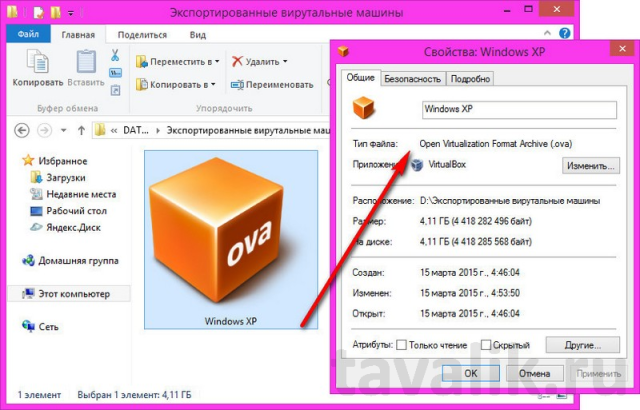
У наступному вікні тиснемо « Експорт ».



Чекаємо завершення процесу експорту.

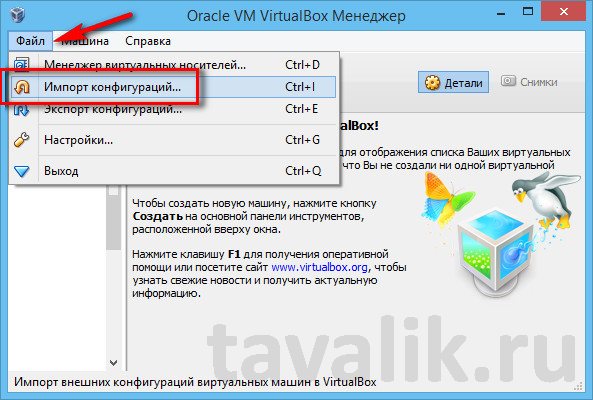


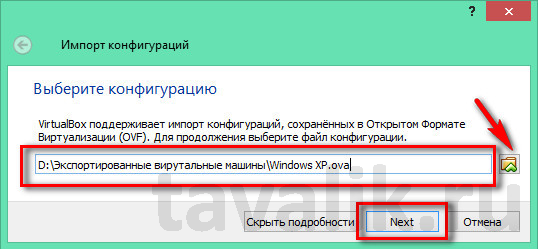
Експортована віртуальна машина в файлі «.ova» буде знаходитися в зазначеній папці, звідки її можна перемістити на інший комп'ютер, знімний носій, в хмарний сервіс. Або можна залишити, як в нашому випадку, на місці - на несистемно диску, де цей файл буде зберігатися під час установки Windows.

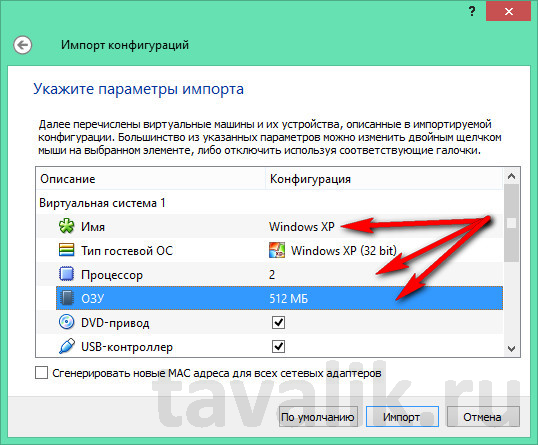


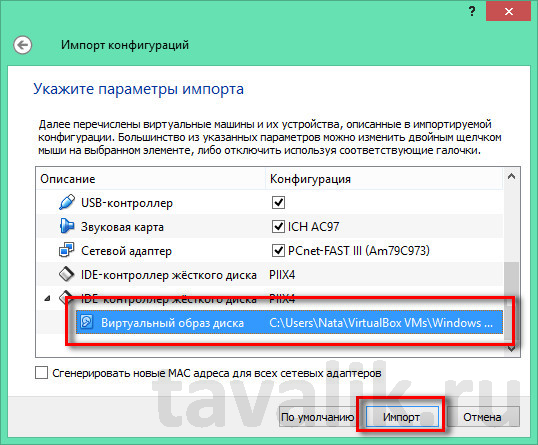
**Імпорт**

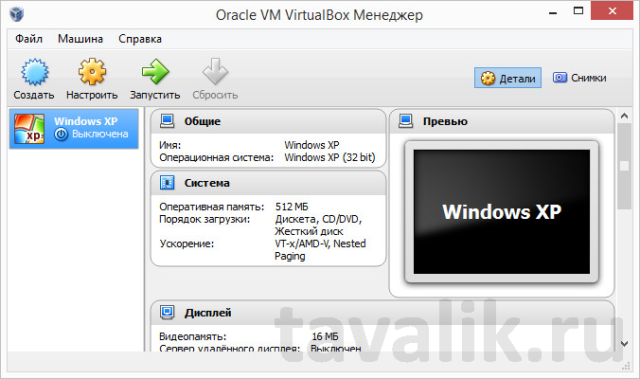
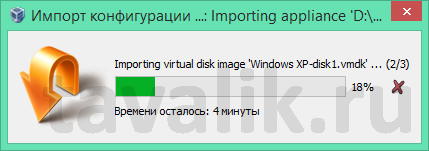
Після інсталяції VirtualBox на новій Windows або на іншому комп'ютері відкриваємо програму і в меню «Файл» вибираємо «Імпорт конфігурацій».



У наступному вікні вказуємо шлях до файлу «.ova» з експортованої віртуальною машиною. Тиснемо «Next».

man (від англ. manual - керівництво) - команда Unix, призначена для форматування і виведення довідкових сторінок. Поставляється майже з усіма UNIX-подібними збірками. Кожна сторінка довідки є самостійним документом і пишеться розробниками відповідного програмного забезпечення.

В самому кінці вікна буде вказано шлях, куди після імпорту буде поміщений файл жорсткого диска «.vdi». За замовчуванням це системний диск, і щоб не захаращувати його і запобігти втраті файлу «.vdi» в разі збою системи, можна змінити шлях, вказавши папку зберігання на несистемно диску. Тиснемо «Імпорт»

Далі буде процес імпорту

**2.1** Трансляція мережевих адрес (NAT) - це процес, в якому один або кілька приватних IP-адресів перетворюються в один або кілька публічних IP-адрес і навпаки, щоб забезпечити доступ в Інтернет для локальних вузлів.

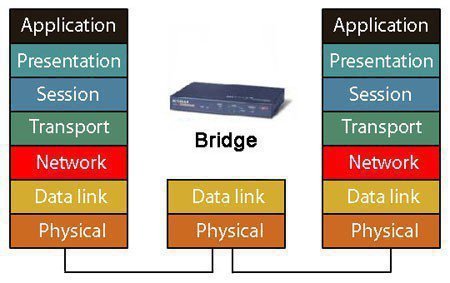
Крім того, NAT виконує перетворення номерів портів, тобто маскує номер порту хоста іншим номером порту в пакеті, який буде направлений до пункту призначення. При цьому NAT не тільки зберігає пул загальнодоступних IP-адресів, а й приховує схему адресації вашої мережі. Потім він вносить відповідні записи IP-адреси і номера порту в таблицю NAT.

Алгоритм роботи технології полягає в тому, що коли клієнт в мережі відправляє якийсь запит в Інтернет, маршрутизатор пересилає запит спеціального пристрою NAT. далі він перетворює адресу відправника в загальнодоступну IP-адресу пристрою перед пересиланням запиту в Інтернет і для подальшого отримання інформації з сервера. Коли відповідь отримана від зовнішнього джерела, NAT перетворює загальнодоступну IP-адресу в приватну IP-адресу перед самим пересиланням пакету клієнту. Для цього NAT створює зіставлення між парою PrivateSrcIP, PrivateSrcPort і парою PublicSrcIP, PublicSrcPort, щоб знати напевно, як перетворити IP-адресу і номер порту призначення. NAT зазвичай працює на маршрутизаторі або міжмережевому екрані.

2.2

# **Мережеві мости**

Міст являє собою мережеве обладнання, основним призначенням якого є об'єднання сегментів комп'ютерної мережі різних топологій та архітектури. Оскільки мости працюють на канальному рівні моделі OSI, їх використовують виключно в локальних мережах. Кожен вузол мережі, для якого визначено канальний рівень, має свою фізичну адресу, яка прошита в мережевому адаптері. Робота мостів полягає в тому, що вони виділяють фізичні адреси прийнятих кадрів і вибірково пропускають ці кадри в певні сегменти мережі. Дана фільтрація здійснюється відповідно до таблиці комутації, яка міститься в його пам'яті. У цій таблиці кожній фізичній адресі ставиться у відповідність порт пункту призначення або фрагмент мережі.



Міст збирає інформацію про сторону, де знаходиться конкретна MAC-адреса, і вирішує про пересилання даних на підставі відповідного списку MAC-адрес. Мости здійснюють фільтрацію потоків даних на основі тільки MAC-адрес вузлів.  
  
Передача даних на канальному рівні має широкомовний характер. Міст ігнорує кадри, які пересилаються між окремими вузлами, розташованими по одну сторону від нього. Наприклад, дані, відправлені вузлом A до вузла B, в інший сегмент мережі не потраплять, бо міст, розташований між сегментами не пропустить кадри даних. При обміні інформацією між вузлом A і H міст не буде перешкоджати передачі даних.  
  
Саме в цьому полягає головна перевага використання мостів - скорочення обсягу переданої інформації по всій мережі, за рахунок його локалізації на окремі фрагменти мережі.  
  
Локалізація трафіку також зменшує можливість несанкціонованого доступу до даних, оскільки кадри не виходять за межі свого сегмента і їх складніше перехопити зловмиснику.  
  
Міст являє собою накопичувально-передавальний пристрій, принцип роботи якого полягає в тому, що почавши отримувати кадр інформації на один зі своїх портів, він, перш ніж пересилати його через інший свій порт, отримує цей кадр повністю. Також міст визначає цілісність кадрів за допомогою наявності в них контрольної суми, що зменшує навантаження мережі, тому що погані кадри локалізуються і вилучаються в одному сегменті мережі, навіть якщо пересилаються в інший сегмент.  
  
Особливими функціями моста, які відрізняють його від іншого обладнання мережі, є фільтрація фреймів на канальному рівні і використовуваний при цьому спосіб обробки трафіку. Для фільтрації даних створюється таблиця всіх MAC-адрес, розташованих в мережі. Далі відбувається перетворення їх у відповідні номери портів.  
  
Основні етапи маніпуляції даними моста наступні:  
  
1. При пересиланні даних, міст виявляє MAC адресу пристрою відправника. Якщо фрейм даних вперше відправляється, тоді здійснюється запис фізичної адреси в таблицю адрес.  
  
2. При надходженні даних на порт моста, відбувається перевірка наявності в адресних таблицях MAC-адреси пункту призначення.  
  
3. Якщо MAC-адреси одержувача і відправника належать одному сегменту мережі, тоді міст блокує передачу в інші сегменти. Даний процес називається фільтрацією (filtering). Завдяки фільтрації відбувається значна оптимізація мережного обсягу переданих даних між сегментами.  
  
4. Якщо MAC-адресу одержувача і відправника знаходяться в різних сегментах, тоді міст направляє дані в сегмент одержувача.  
  
5. Якщо в таблиці адрес немає MAC-адреси одержувача, тоді міст розсилає дані в усі порти. Даний процес називається лавинною розсилкою (flooding).  
  
6. Міст створює таблицю комутації, вивчаючи MAC-адреси відправників у фреймах, і заносить в таблицю номера інтерфейсів і MAC-адреси.

2.3

Мережа лише для хостів налаштовується автоматично, якщо в майстрі створення нових віртуальних машин вибрано параметр **Використовувати мережу лише для хостів** . На хостах Linux цей вибір доступний лише у тому випадку, якщо під час встановлення робочої станції VMware ви ввімкнули параметр мережевої мережі, який використовується лише для хостів.

Мережа лише для хостів забезпечує мережеве з'єднання між віртуальною машиною та хост-комп'ютером, використовуючи віртуальний адаптер Ethernet, який видно операційній системі хоста. Цей підхід може бути корисним, якщо вам потрібно створити ізольовану віртуальну мережу.

Якщо ви використовуєте лише мережеву мережу, ваша віртуальна машина та хост-віртуальний адаптер підключені до приватної мережі Ethernet. Адреси в цій мережі надаються сервером DHCP VMware.

Якщо ви зробите якийсь інший вибір у майстрі нових віртуальних машин і пізніше вирішите, що хочете використовувати мережу лише для хостів, ви можете внести цю зміну в редакторі налаштувань віртуальної машини ( **VM> Налаштування** ). Докладніше див. У розділі Зміна конфігурації мережі .

### Маршрутизація та спільний доступ до з'єднання

Якщо ви встановите належне програмне забезпечення для маршрутизації або проксі на своєму хост-комп’ютері, ви можете встановити зв’язок між хост-віртуальним адаптером Ethernet та фізичним мережевим адаптером на хост-комп’ютері. Це дозволяє, наприклад, підключити віртуальну машину до Token Ring або до іншої мережі, що не є Ethernet.

На хост-комп'ютері під керуванням Windows 2000, Windows XP або Windows Server 2003 ви можете використовувати лише мережеві мережі в поєднанні з функцією спільного використання Інтернет-з'єднання в Windows, щоб дозволити віртуальній машині використовувати мережевий адаптер комутованої мережі або інше з'єднання з Інтернет. Докладніше про налаштування спільного доступу до Інтернету див. У документації Windows.

2.4

Внутрішня мережа подібна до мостової мережі тим, що ВМ може безпосередньо спілкуватися із зовнішнім світом. Однак зовнішній світ обмежений іншими віртуальними машинами на одному хості, які підключаються до тієї самої внутрішньої мережі.

Незважаючи на те, що технічно все, що можна зробити за допомогою внутрішніх мереж, також можна зробити за допомогою мостових мереж, внутрішні мережі мають переваги у безпеці. У режимі мережевого з'єднання весь трафік проходить через фізичний інтерфейс головної системи. Тому до інтерфейсу хоста можна приєднати sniffer пакетів, такий як Wireshark, і реєструвати весь трафік, що надходить через нього. Якщо з якихось причин ви віддаєте перевагу двом або більше віртуальним машинам на одній машині для приватного спілкування, приховуючи свої дані як від хост-системи, так і від користувача, мережеві мережі не є варіантом.

Внутрішні мережі створюються автоматично за потреби. Центральної конфігурації немає. Кожна внутрішня мережа ідентифікується просто за її назвою. Як тільки є більше однієї активної віртуальної мережевої карти з однаковим внутрішнім ідентифікатором мережі, драйвер підтримки Oracle VM VirtualBox автоматично *під’єднає* карти і буде діяти як мережевий комутатор. Драйвер підтримки Oracle VM VirtualBox реалізує повний комутатор Ethernet і підтримує як широкомовні / багатоадресні кадри, так і безладний режим.

Для того, щоб приєднати мережеву карту віртуальної машини до внутрішньої мережі, встановіть її режим мережі на Внутрішня мережа. Є два шляхи досягнення цього:

* Використовуйте діалогове вікно **налаштування** віртуальної машини в графічному інтерфейсі користувача Oracle VM VirtualBox. У категорії « **Мережа** » діалогового вікна налаштувань виберіть « **Внутрішні мережі»** зі спадного списку режимів роботи мережі. Виберіть назву існуючої внутрішньої мережі зі спадного списку нижче або введіть нову назву в поле **Ім'я** .
* Використовуйте командний рядок, наприклад:

VBoxManage modifyvm "ім'я віртуальної машини" --nic <x> intnet

За бажанням ви можете вказати ім’я мережі за допомогою команди:

VBoxManage modifyvm "ім'я віртуальної машини" --intnet <x> "ім'я мережі"

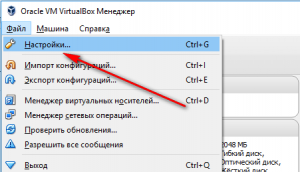
Якщо ви не вказали назву мережі, мережева карта буде приєднана до мережі intnetза замовчуванням.

Якщо ви не налаштуєте віртуальні мережеві карти в гостьових операційних системах, які беруть участь у внутрішній мережі, на використання статичних IP-адрес, можливо, вам доведеться використовувати DHCP-сервер, вбудований у Oracle VM VirtualBox, для управління IP-адресами внутрішньої мережі.

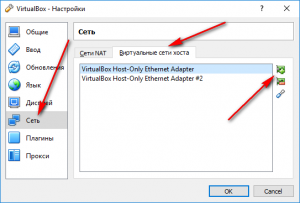
Як засіб безпеки, за замовчуванням, реалізація внутрішньої мережі Linux дозволяє лише ВМ, що працюють під тим самим ідентифікатором користувача, встановлювати внутрішню мережу. Однак можна створити спільний внутрішній мережевий інтерфейс, доступний для користувачів з різними ідентифікаторами користувачів.

3.1

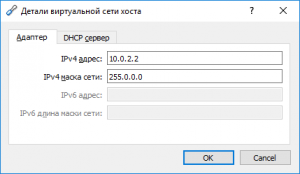
Нам необхідно додати ще один віртуальний адаптер (один уже є і використовується для виходу в інтернет гостьових ОС)

Для цього відкриваємо налаштування VirtualBox

Далі переходимо в «Мережа» і у вкладку «Віртуальні мережі хоста». Тиснемо додати новий адаптер.



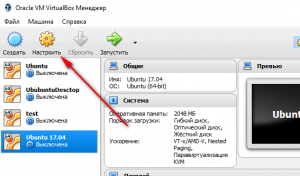
Далі налаштовуємо адаптер, прописуємо ip адресу, я прописав статичний. 10.0.2.2

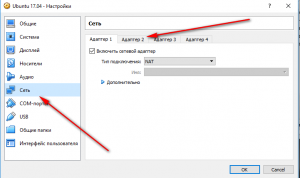


Также можно настроить и DHCP сервер.

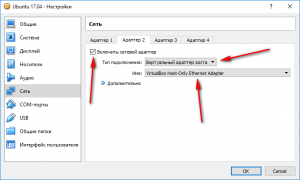
Жмем «Ок». Теперь переходим к настройке виртуальной машины.

Налаштування мережі в віртуальній машині.

Відкриваємо налаштування нашої віртуальної машини.

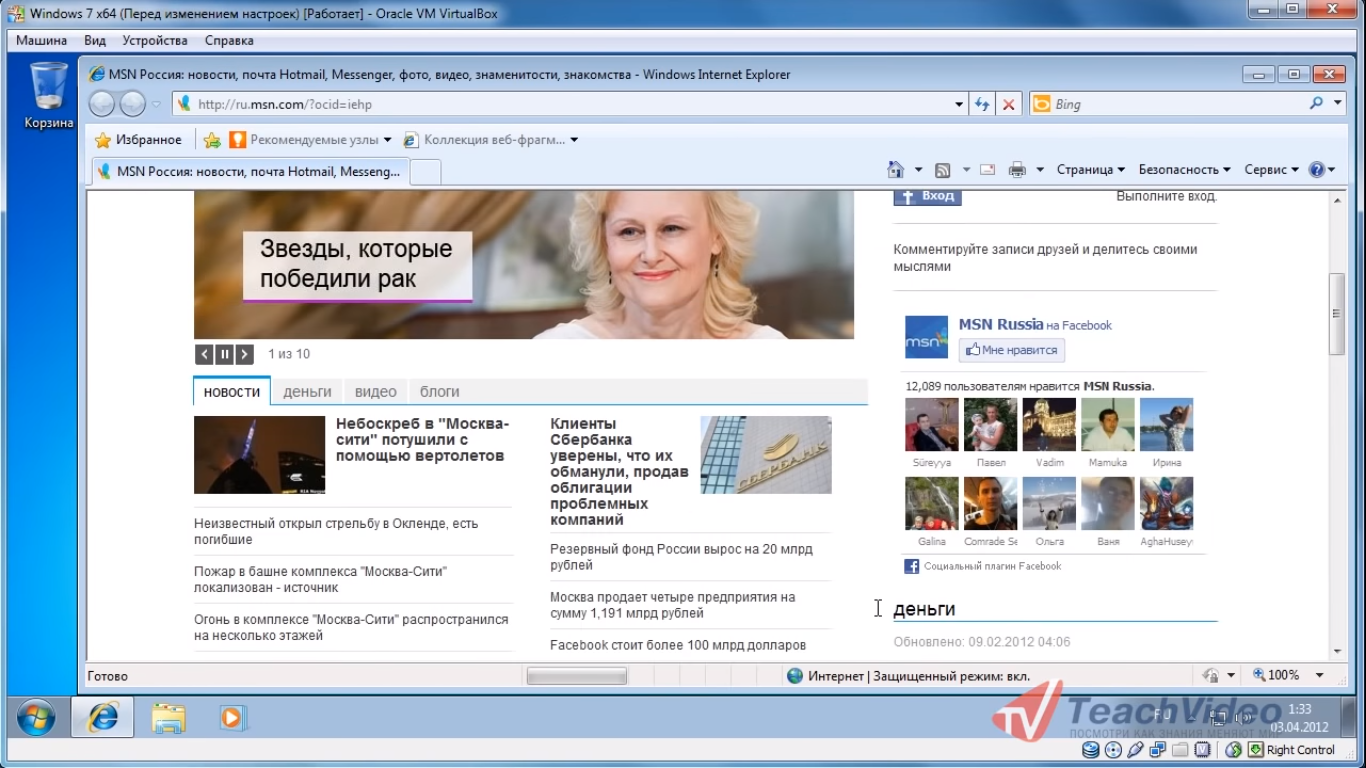
Вибираємо «Мережа» і переходимо у вкладку «Адаптер 2»

Включаємо мережевий адаптер. Потім вибираємо тип підключення «Віртуальний адаптер» і зі списку вибираємо ім'я. Тиснемо «Ок»



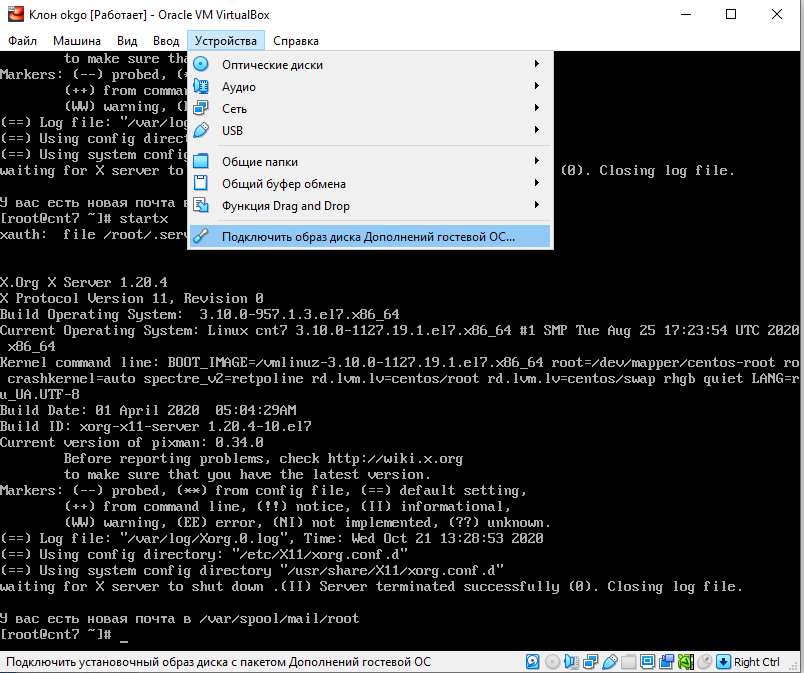
На цьому настройка віртуальної машини завершена. Запускаємо машину.

3.2



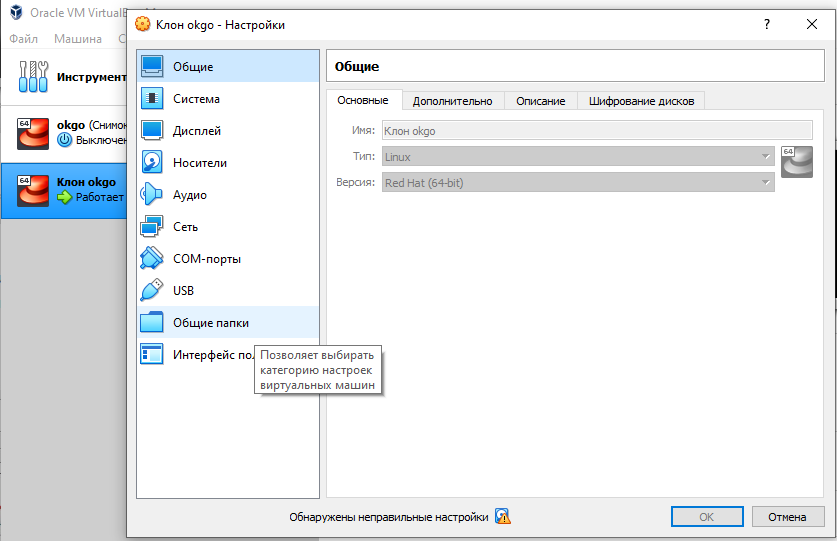
3.4

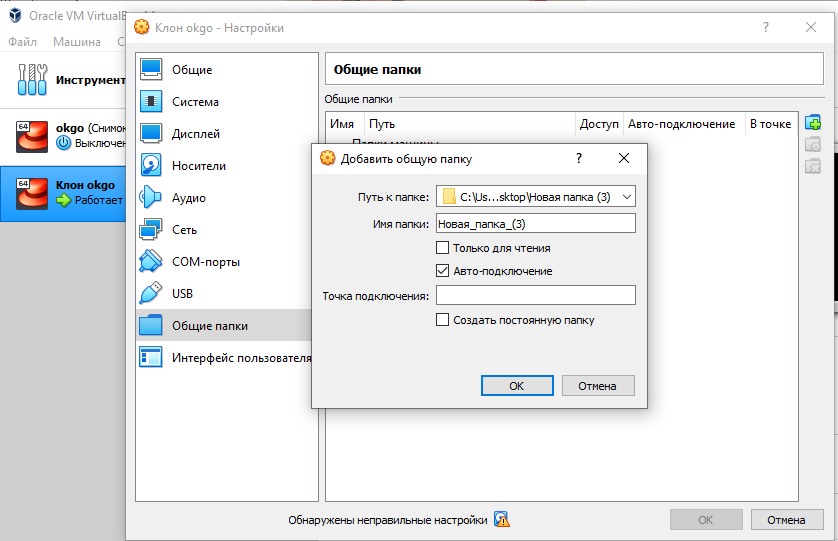
Перш за все потрібно встановити Гостьові доповнення VirtualBox. Без них ви не зможете працювати з загальними папками. Запустіть виртуалку, в меню виберіть "Пристрої", "Підключити образ диска Додатків гостьовий ОС".



Запустіть VirtualBox, виберіть потрібну віртуальну машину і натисніть "Налаштувати"

Перейдіть у вкладку "Загальні папки". Натисніть на значок створити нову папку, вкажіть її назву і місце розташування. Також не забудьте поставити галочку навпроти "Авто-підключення", щоб гостьова ОС автоматично включала цю папку.





Запустіть віртуальну ОС. У провіднику Windows XP з'явився мережевий диск, який є спільною папкою, якою можна користуватися як з гостьової ОС так і з реальною. Тепер можна спокійно **перенести потрібні файли на віртуальну машину VirtualBox і навпаки.**