**Лекція 6. Віртуалізація та віддалена робота в комп’ютерних системах**

**1. Віддалене керування комп’ютерною системою.**

1.1. **Види віддаленого керування.**

Віддалене керування комп'ютером через Інтернет – це можливість використовувати комп'ютер з будь-якої точки світу так, як працювати безпосередньо за ним. Скрізь, де є Інтернет, з'являється можливість підключатися до офісного або домашнього комп'ютера і використовувати всі його можливості для вирішення різних завдань.

Застосування віддаленого керування

- **Для отримання доступу до офісного комп'ютера** або файл-серверу з дому, або з іншого офісу. Ви зможете користуватися повним набором програм на своєму робочому комп'ютері з будь-якого місця, мати доступ до своїх документів і вести офісну роботу навіть з кафе. Подібний тип віддаленого керування комп'ютером через Інтернет активно використовується бізнесменами, що часто мають відрядження. Просто не вимикайте офісний комп'ютер – і він буде «з вами» скрізь, де є вихід в Інтернет.

- **Для керування критичними комп'ютерами,** що працюють в складних мережах, наприклад, серверами. Віддалене керування комп'ютером через Інтернет дозволяє системному адміністратору постійно мати доступ до ресурсу, на збої в роботі якого повинна слідувати негайна реакція.

- **Для роботи з віддаленими комп'ютерами і мережами через віддалений робочий стіл.** Завдяки можливості керування через Інтернет, технічні фахівці мають можливість обслуговувати будь-які системи, що знаходяться в різних точках світу. Один системний адміністратор, наприклад, може налаштувати комп'ютери відразу в кількох містах: це дуже зручно для компаній, що мають велику мережу філій або складну інформаційну інфраструктуру.

- **Для проведення веб-семінарів або дистанційного навчання.** Можливість безпосередньо працювати на комп'ютері викладача або ж можливість викладача бачити всі дії учня і допомагати йому.

-За допомогою мобільного комп'ютера (ноутбука, нетбука, планшета IPad) з виходом в Інтернет можна **здійснювати віддалене керування домашнім комп'ютером,** перевіряти пошту, планувати завдання і користуватися документами та програмами.

**Організація віддаленого керування**

Практично всі сучасні операційні системи мають вбудовані функції керування віддаленим робочим столом. Проте, скористатися ними вдається далеко не завжди. Адже для того, щоб ці функції запрацювали, необхідно заздалегідь налаштувати комп'ютер. Не кожен користувач зможе це зробити самостійно. Крім того, в багатьох користувачів на це елементарно немає прав, а з системним адміністратором домовитися вдається не завжди.

**Для організації віддаленого доступу та керування слід:**

1.Встановити спеціальну програму на комп'ютер, який буде керованим. Ця програма дозволяє захистити дані, забезпечити конфіденційність обміну інформацією, а також правильність і надійність авторизації. Керувати своїм комп'ютером може лише власник, а інформація буде надійно захищена.

2. Залишити керований комп'ютер включеним і під'єднаним до мережі для віддаленого керування комп'ютером. Це цілком нормальний стан для сервера, але психологічно незвичний для домашнього комп'ютера. Згодом, його можна вимкнути в любий час, використовуючи віддалене керування *(remote dekstop).*

3. Використати програму або мережний сервіс на комп'ютері, з якого буде здійснено доступ. Технічно можливим є під'єднання з Інтернет-клубу, з нетбука або з мобільного телефону.

**Дистанційне керування**

Режим «дистанційного керування» дозволяє віддаленим клієнтам керувати роботою сервера або робочої станції, включеної в локальну мережу. Робота в режимі «дистанційного керування» відповідає клієнт-серверній моделі «сервер терміналів».

*Віддалений комп'ютер (віддалений хост) – сервер, фізично розміщений на деякій відстані від клієнта і доступ до якого (для клієнтів) можливий тільки через мережу.*

**Термінальний режим**

З середини 1970-х до середини 1980-х років вся робота за комп'ютером виконувалася через спеціальні пристрої введення-виведення – термінали. З поширенням персональних ЕОМ термінальний доступ став використовуватися в основному для вирішення завдань віддаленого адміністрування.

**Термінальний режим роботи** – організація мережевої роботи інформаційної системи шляхом розміщення усіх користувацьких програм і даних на центральному сервері (серверах), доступ до яких відбувається з машин-терміналів виготовлених в спрощеному виконанні і, як наслідок, більш дешевих, які займають мінімум місця, безшумні і практично не вимагають обслуговування.

**Термінал** – кінцевий мережевий пристрій, підключений до обчислювальної системи і призначений для введення і виведення даних. Команди, які приймає з пристрою вводу терміналу (клавіатури), передаються на головний комп'ютер (сервер, віддалений хост), де і виконуються. Результати опрацювання повертаються і виводяться на дисплеї терміналу.

*Фізичний* або *реальний термінал* – як правило мається на увазі пристрій, обчислювальні можливості якого обмежені можливістю відображати те, що йому передано з мережі (як максимум – повноекранну графіку).

*Віртуальний термінал – це програма, що виконує функції реального терміналу. З боку віддаленого хоста така програма, емулятор терміналу, нічим не відрізняється від реального терміналу.*

**Типи терміналів**

**Текстові термінали**

**Текстовий термінал** – це пристрій (або програма) введення/виведення, які працюють в дуплексному режимі і використовують символьно-орієнтовані протоколи передачі даних, такі як telnet (рис. 6.1). Потоки даних між терміналом і сервером представляють ASCII-символи. Спеціальні символи (або послідовність символів) представляють команди керування сервером і відповіді сервера. Існують і службові команди, які керують виводом (переведення рядка, напівжирний/похилий текст, звуковий сигнал тощо) і сеансом зв'язку (узгодження версій протоколу тощо).

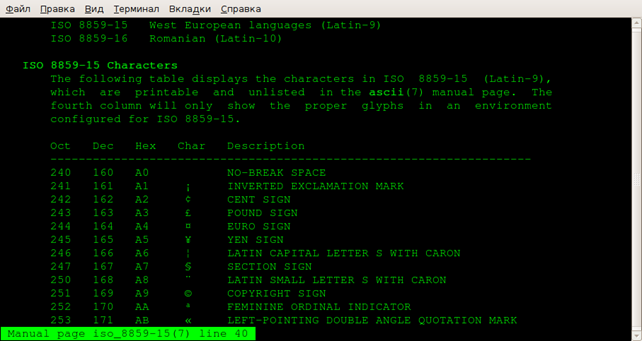


Рис. 6.1 – Вигляд текстового терміналу

Текстові термінали UNIX-подібних систем зазвичай підключаються до мейнфрейму або серверу через послідовний порт (RS-232C). Це дозволяє керувати фізично віддаленими серверами (наприклад, в Інтернеті), використовуючи повільні комутовані з'єднання.

Графічні можливості текстових терміналів обмежені спеціальними символами ASCII, які можуть бути використані для малювання рамок таблиць, стрілок, горизонтальних і вертикальних ліній, заливок різної щільності тощо. Використання VGA палітри дозволяє задавати колір фону і тексту. Але все це зводиться до псевдографіки, оскільки текстові термінали не керують виводом на рівні окремих пікселів.

**Графічні термінали**

**Графічні термінали,** на відміну від текстових, надають можливості роботи з повноколірною растровою і векторною графікою як при вводі даних, так і при їх відображенні. Графічні термінали застосовуються в системах, які підтримують графічний користувацький інтерфейс (GUI, Graphic User Interface).

Вимоги до пропускної здатності лінії зв'язку при використанні графічних терміналів, в загальному, значно більше в порівнянні з текстовими, оскільки передавати приходиться не коди символів, а, фактично, скріншоти. Для зиження навантаження на мережу використовуються різні способи: компресія, обмеження на глибину кольору і роздільної здатності екрану, передача лише областей, які змінилися тощо.

Текстовий режим роботи також підтримуються графічними терміналами, але реалізований інакше – всередині основного протоколу.



Рис. 6.2 – Вигляд графічного терміналу

Інтелектуальний термінал

**Інтелектуальний термінал** – під цим терміном вважають апаратно- програмний комплекс, комп'ютер, ресурсів якого достатньо не лише для виводу повноекранної графіки, але і для виконання деяких обчислень. Принциповою відмінністю інтелектуального терміналу від звичайного ПК є те, що виконуючі програми повинні завантажуватися з сервера (наприклад - *бездискова робоча станція).*

**1.2. Протоколи віддаленого керування**

**Сервіс telnet**

Служба віддаленого керування telnet (Teletype Network) – одна з найстаріших мережевих технологій Internet. Протокол telnet з початку розроблявся для використання в гетерогенних мережах. В його основі — концепція мережевого віртуального терміналу (Network Virtual Terminal, NVT) – механізму абстрагування від специфіки введення/виведення різних апаратних і програмних платформ. Так, в UNIX в якості символу переходу на інший рядок використовується LF (код 13), в той же час як в MS-DOS і Windows – пара символів CR-LF (коди 10 і 13). Мережевий віртуальний термінал NVT пропонує використання уніфікованого набору символів: telnet-клієнт відповідає за перетворення власних кодів в коди NVT, а сервер робить зворотне перетворення.

**Протокол rlogin**

**Протокол rlogin** (англ. *remote login* – віддалений вхід в систему, RFC 1282, порт сервера – 513) дозволяє користувачам робочих станцій UNIX підключатися до віддалених серверів UNIX через Internet і працювати так же, як при прямому підключенні терміналу до машини. Попри rlogin існує ще декілька подібних протоколів: rsh (remote shell), rcp (remote copy). Утиліти rlogin, rsh и rcp часто об'єднують під загальною назвою r-команд.

**SSH (Secure Shell)**

**SSH** (англ. Secure SHell – безпечна оболонка) – безпечний протокол віддаленого керування комп'ютером і передачі файлів. Схожий за призначенням з протоколом telnet і rlogin, але використовує алгоритми шифрування передаваючої інформації. Основна специфікація – RFC 4251. The Secure Shell (SSH) Protocol Architecture

SSH представляє істотно більші можливості, ніж telnet, і дозволяє не лише використовувати захищену оболонку на віддаленому хості, але і тунелювати графічний інтерфейс – X11 forwarding (для ОС і програм, які використовують X-Window System). SSH також може (при вдалому налаштуванні) передавати через безпечний канал будь-який інший мережевий протокол – port forwarding. Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування.

**Remote Desktop Protocol**

**RDP** (англ. *Remote Desktop Protocol,* протокол віддаленого робочого столу) – відкритий протокол прикладного рівня, розроблений Microsoft і з самого початку призначений для підключення графічних терміналів до Windows Terminal Server. Клиєнти існують практично для всіх версій Windows (включаючи Windows CE і Mobile), Linux, Free BSD, Mac OS X. Типово використовується порт TCP 3389. Офіційна назва Майкрософт для клієнтського ПЗ - Remote Desktop Connection або Terminal Services Client (TSC), зокрема, клієнт в Windows XP/2003/vista називається mstsc.exe.

RDP-клієнт, – Remote Desktop – дозволяє вам, перебуваючи на одному комп'ютері, віддалено керувати іншим.

Remote Desktop підтримує роботу в двох режимах:

-Remote Desktop (Віддалений робочий стіл) – підходить для використання в локальній мережі і вимагає встановлення програмного забезпечення на комп'ютері-клієнті.

-Remote Desktop Web Connection (Інтернет-підключення до віддаленого робочого столу) – потребує на клієнтській машині лише наявність браузера, але на сервері для неї необхідно встановити і налаштувати велику кількість програм.

Remote Desktop підтримує 24-бітні кольори – це дозволяє варіювати кількість картинки в широких межах.

Remote Desktop-сервер і Remote Desktop-клієнт користуються загальним буфером. Це дозволяє їм вільно обмінюватися інформацією.

**1.3. Веб-технології віддаленого керування**

**VNC-системи (Virtual Network Computing)**

VNC система – це система віддаленого доступу до іншого комп'ютера, що використовує протокол RFB (*Remote FrameBuffer).* Керування здійснюється шляхом ретрансляції вмісту екрану через комп'ютерну мережу.

Системи VNC є платформо незалежними: VNC-клієнт (VNC viewer), що запущений на одній операційній системі, може підключатися до VNC-сервера, що діє на іншій операційній системі. Реалізація клієнтської і серверної частини існує майже для всіх операційних систем.

До одного VNC-сервера синхронно можуть під'єднуватися кілька клієнтів. Найчастіше VNC системи використовують для технічної підтримки і доступу з дому до комп'ютера на роботі.

Популярними VNC системами є TeamViewer, TightVNC, Logmein, CrossLoop, AMMYY Admin, ShowMyPC, Radmin та інші.

**VPN** (**Віртуальна приватна мережа**, [англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Virtual Private Network*) – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

LogMeIn Hamachi – це хост-служба VPN, що дозволяє безпечно організовувати віртуальні ЛОМ для розподілених команд, мобільних співробітників і друзів з відеоігор - в лічені хвилини.

**2. Системи віртуалізації**

Термін віртуалізація останнім часом став дуже популярним. Віртуальні рішення в тій чи іншій мірі застосовуються в переважній більшості інформаційних систем. Фахівці використовують їх з метою тестування, для виконання додаткових завдань на існуючому обладнанні, для навчання і т. д. Віртуалізують сервери, робочі станції, системи зберігання, мережеву інфраструктуру.

Наприкінці 80-х майже всі думали, що ІТ-інфраструктура буде виглядати як досить малопотужні, легко замінні термінали і суперкомп'ютери, до яких ідуть підключення. Все повільно йшло до цього (і це було логічно), але в кінцевому підсумку перемогла парадигма зберігання даних на локальних вузлах. У чому чимала заслуга Microsoft, до речі. У довіртуальній інфраструктурі у кожного є системний блок і жорсткий диск всередині. Там обробляються дані, і тільки результати відправляються на сервер.

Економічні аспекти віртуалізації

Перш ніж приступати до впровадження віртуальних систем, слід ретельно продумати, що ми хочемо отримати в результаті і скільки це буде коштувати. Незважаючи на те, що практично в кожній презентації ми чуємо про економічну ефективність технології, на практиці впровадження віртуалізації супроводжується витратами, причому досить значними.

По-перше, віртуалізація вимагає наявності інфраструктури, наприклад, системи зберігання даних, підключеної до декількох серверів. По-друге, програмне забезпечення, що дозволяє використовувати переваги віртуальних середовищ: мігрувати віртуальні машини з одного фізичного сервера на інший в реальному режимі часу, балансувати навантаження на фізичних серверах, вимикаючи обладнання, яке не використовується і т. д., – є комерційним і порівняно недешевим продуктом.

У результаті економічний ефект переходу у віртуальні середовища досягається, починаючи з деякого числа серверів. Якщо вам і не потрібно відразу встановити 10 нових серверів, то купувати нове обладнання доведеться відразу і в розрахунку на розміщення всіх майбутніх систем.

Ефективність керування комплексом віртуальних машин в наших умовах рідко можна оцінити в цифрах, оскільки штатних змін серед ІТ-спеціалістів підприємства (наприклад, скорочення числа системних адміністраторів) після впроваджень рішень з віртуалізації не відбувається, а витрати на електропостачання серверних кімнат підприємства зазвичай не враховуються окремим рядком.

У підсумку впровадження віртуалізації часто призводить тільки до додаткових витрат на утримання ІТ-інфраструктури.

Основні терміни

**Гіпервізором (hypervisor)** називають програмне забезпечення, що забезпечує віртуалізацію ресурсів і дозволяє декільком операційним системам працювати одночасно на одному фізичному пристрої, який прийнято називати *хост-системою* або просто хостом. Назва гіпервізор збереглася історично, більш зрозумілим міг би бути термін «менеджер віртуальних машин».

Операційну систему, що працює під керуванням гіпервізора, прийнято називати *гостьовою операційною системою*.

Жорсткі диски гостьових операційних систем є файлами на рівні гіпервізора. Їх прийнято називати віртуальними жорсткими дисками. Відповідно мережеві адаптери, пам'ять в гостьових системах називають віртуальними адаптерами, віртуальною пам'яттю і т. д.

На рівні гіпервізора можна створити різні віртуальні мережі: з підключенням до реального мережного адаптера в режимі моста, в режимі трансляції мережевих адрес, сегмент мережі без доступу до реального адаптера (внутрішня мережа) і т. д.

Комерційні рішення віртуалізації включають в себе віртуальні комутатори, які ви можете налаштувати на необхідні правила пересилання і фільтрації пакетів з однієї мережі в іншу.

Як правило, розробники гіпервізорів підготовлюють спеціальні пакети оновлень, що оптимізують роботу гостьових операційних систем. Наприклад, в гостьові ОС додаються мережеві адаптери, що працюють на швидкості внутрішньої шини гіпервізора. При цьому з'являється можливість обмінюватися даними між гостьовими ОС через буфер пам'яті, підключати папки хоста як мережевих папок в гостьові ОС і т. д. Таке ПЗ прийнято називати *розширеннями віртуальних машин* (virtual machine additions). Якщо немає спеціальних вимог, то для підвищення продуктивності систем розширення повинні бути встановлені в гостьовій ОС (зазвичай команди встановлення розширень присутні в меню вікна віртуальної машини).

*VDI* (Virtual Desktop Infrastructure, інфраструктура віртуальних робочих столів) – так називають ПЗ, що дозволяє керувати великою кількістю віртуальних робочих станцій (рис. 3.3).

Клієнти (ПК, ноутбуки, тонкі клієнти, мобільні пристрої)

Рис. 3.3 – Представлення інфраструктури VDI

**Розробники віртуальних рішень**

Існує декілька технологій віртуалізації, розроблених різними вендорами. Ми наведемо лише короткий список систем, які найбільш активно, використовуються на практиці.

Лідером ринку віртуалізації сьогодні є продукти компанії *VMware* (www.vmware.com). Рішення від VMware забезпечують віртуалізацію практично всієї лінійки операційних систем (Windows, Linux, Apple Macintosh і т. д.), ПЗ компанії тісно інтегровано з апаратними можливостями багатьох платформ, реалізовані технології відмовостійких рішень і т. д. Лінійка ПЗ представлена ​​як вільно поширюваними, так і комерційними продуктами гіпервізор ESXi (рис. 3.4).

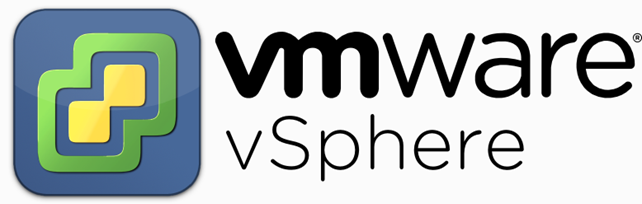


Рис. 3.4 – Логотип компанії VMware

*XEN* (www.xensource.com, www.virtualiron.com, http://www.xen.org/) багатоплатформовий гіпервізор, розроблений в комп'ютерній лабораторії Кембриджського університету і поширюваний на умовах ліцензії GPL (рис. 3.5).



Рис. 3.4 – Логотип гіпервізора Xen

На базі цього гіпервізора компанією Citrix створені сервери XenServer, які також є безкоштовними рішеннями. Правда, ПЗ централізованого керування серверами XenServer є комерційним продуктом.

Компанією Sun (нині Oracle) випущена віртуальна машина *VirtualBox*. Це рішення безкоштовне і може бути завантажене з сайту Oracle. У компанії Oracle є і рішення VDI – Oracle Virtual Desktop Infrastructure (VDI), причому у варіанті до 10 віртуальних робочих столів воно може безкоштовно тестуватися напротязі необмеженого часу.



У складі серверних операційних систем починаючи з Windows 2008 присутній гіпервізор – *HyperV*, який може бути завантажений з сайту Microsoft і в якості окремого продукту і може бути використаний повністю безкоштовно.

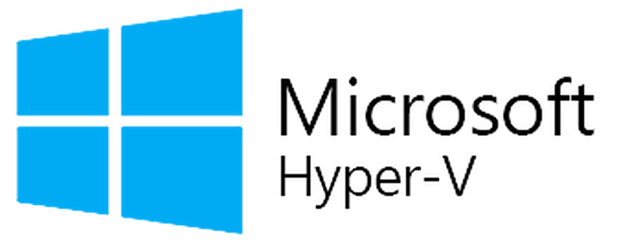


Рис. 3.4 – Логотип гіпервізора Microsooft Hyper-V

Продукти відкритого коду останнім часом активно починають використовувати рішення з віртуалізації з назвою *KVM* (Kernel-based Virtual Machine) (наприклад, цей гіпервізор включений до складу Ubuntu, RedHat і т. д.). Гіпервізор KVM реалізує віртуалізацію на Linux-системах і доступний як у складі відповідних дистрибутивів, так і через пакети установки.



